POLÍTICAS Y REGULACIÓN PARA LA EXPLOTACIÓN LEGÍTIMA DE LOS DATOS Y LA PRIVACIDAD

Dr. Christian James Aguilar Armenta[1]

Instituto Federal de Telecomunicaciones

Centro de Estudios
james.aguilar@ift.org.mx

[1]Ingeniero en Telecomunicaciones por la Facultad de Ingeniería de la UNAM y Doctor en Electrónica con especialización en Telecomunicaciones por la Universidad de York, Reino Unido. Se desempeñó como asesor de la entonces Comisionada Adriana Labardini Inzunza por más de tres años y cuenta con amplia experiencia en Telecomunicaciones en los sectores privado, público y académico con más de seis años en el sector. También cuenta con tres artículos de investigación científica, entre los que destaca el journal paper “Cantilever RF-MEMS for Monolithic Integration with Phased Array Antennas on a PCB”.

Contenido

Introducción

La evolución de las tecnologías digitales ha permitido que en la actualidad las comunicaciones entre las personas sean más rápidas, sencillas y que trasciendan fronteras, facilitando, entre otros muchos sectores, la economía digital.

Vivimos en un mundo en el que todos los ámbitos del ecosistema digital crecen de manera acelerada. De acuerdo con algunas estadísticas,[1,2] sabemos que hay cerca de 4,176 millones de usuarios activos de Internet en todo el mundo (71.3 millones en México),[3] de los cuales 250 millones son nuevos usuarios que surgieron en 2017. Además, cerca de 3,800 millones de esos usuarios son móviles, haciendo que el uso diario promedio de Internet sea de 6 horas para lo que va del año 2018. Respecto a las redes sociales sabemos que hay alrededor de 3,000 millones de usuarios, de los cuales 2,243 millones son de Facebook, con un uso diario promedio de 135min, según lo registrado en 2017.

El uso del teléfono móvil también presenta un aumento notable. En la actualidad alrededor de 5,000 millones de personas cuentan con un celular, de las cuales más de 200 millones obtuvieron su primer teléfono en 2017, y más de la mitad de los celulares que se usan hoy son *smartphone*. Además, hoy hay más de 3.8 millones de *apps* disponibles para dispositivos Android y más de 2 millones para iOS, con un número acumulado de 180 billones de *apps* descargadas desde la tienda de Apple.

Por otra parte, en 2017 hubo aproximadamente 1,660 millones de compradores *online* en todo el mundo y se pronostica que para 2020 habrá cerca de 2,050 millones. Asimismo, diariamente se realizan más de 4,400 millones de búsquedas en Google. Como puede verse la tendencia actual es hacia la conectividad global, con un crecimiento exponencial de usuarios de Internet que buscan información de toda índole y que utilizan los diversos servicios y aplicaciones *online* que surgen día a día, principalmente a través de dispositivos móviles.

La conectividad digital de la que hoy gozamos permea prácticamente todos los aspectos de nuestra vida (por ejemplo, comunicación instantánea, redes sociales, compras y servicios *online*, entre otros) y la cantidad de información que generamos y transmitimos es impresionante. De acuerdo con algunas estadísticas[2] el promedio mundial de datos móviles consumidos por mes en los *smartphones* fue de 3 GB en 2017, lo que generó un tráfico de alrededor de 12 EB (billones de GB) a finales de 2017. La mayor parte de este tráfico proviene del uso de aplicaciones y de los sitios web que visitamos. Dentro de él están incluidos nuestros datos personales, los cuales representan una fuente de ingreso para muchas empresas, redes y organizaciones que se dedican a su recolección y análisis para obtener información valiosa o simplemente para venderlos a los interesados (por ejemplo, empresas de publicidad y marketing). Desafortunadamente la mayoría de las personas no tiene conocimiento de que sus datos personales son recolectados sin su consentimiento (por ejemplo, datos de geolocalización, nombre, edad, logs de

[1] https://www.statista.com/
[2] https://wearesocial.com/blog/2018/01/global-digital-report-2018
[3]http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-713-millones-de-usuarios-de-internet-y-174-millones-de-hogares-con-conexion-este-servicio

mensajes, contactos, historial del navegador, datos sensibles, etc.), no sabe que inclusive sus perfiles digitales son vendidos.

Está claro que el papel que desempeñan nuestros datos personales en la economía digital es fundamental y que su aprovechamiento está cambiando de forma radical. Uno de los grandes retos al que se enfrentan las autoridades y reguladores del mundo es garantizar el derecho a la privacidad sin mermar la innovación y el desarrollo del ecosistema digital. Este desafío es cada vez mayor si consideramos que el ecosistema actual presenta cambios constantes, particularmente en el volumen de datos personales que se recolectan, en la gran variedad de procesamientos analíticos que existen para obtener información valiosa, en el valor comercial que representan los datos personales para generar y crear nuevos servicios, en cuanto al alcance de las actuales amenazas cibernéticas, en el número y variedad de actores que ponen en riesgo la protección y privacidad de los datos, en la frecuencia y complejidad de las interacciones entre personas, sistemas y dispositivos, en cuanto a la disponibilidad global de datos personales en las redes de los operadores, entre otros.

El objetivo principal de este estudio es analizar iniciativas internacionales de política pública y regulación respecto a la protección de datos personales, con el fin de identificar desafíos regulatorios que sirvan de insumo para formular posibles soluciones en México, particularmente en beneficio del desarrollo del sector de telecomunicaciones. Para tal fin, primero presentamos algunas definiciones importantes del tema, seguidas de un análisis del valor de los datos personales en la economía digital, en el que mostramos la viabilidad de cuantificar su valor monetario. También identificamos quiénes son los interesados en obtener nuestros datos personales. Posteriormente analizamos en qué momento y de qué manera nuestros datos personales son recolectados y transmitidos, mediante la investigación de los métodos de rastreo más comunes que existen actualmente en Internet y sobre los actores involucrados en la recolección de los datos (desarrolladores de *apps*, fabricantes de dispositivos y sistemas operativos, operadores de telecomunicaciones, etc.), en especial en el ecosistema de las aplicaciones y servicios *online* móviles. En seguida, presentamos un análisis de las políticas y regulaciones internacionales que existen respecto a la protección de datos personales, particularmente un análisis del reglamento europeo (i.e. GDPR por sus siglas en inglés) y su similitud con las regulaciones de algunos países de América, resaltando la situación específica de México y su marco jurídico vigente. Finalmente, presentamos un análisis del posible impacto que tendrá el cumplimiento del GDPR para el sector de telecomunicaciones, así como los retos que esto representa para las tecnologías emergentes (e.g. *Big Data*, IoT, 5G, etc.) de las cuales son parte los operadores de telecomunicaciones.

Definiciones importantes

Los datos, y en particular los datos personales, son el activo fundamental para la economía digital. Tener muy en claro el significado de datos personales es indispensable para delimitar el objeto de estudio del presente documento. A nivel internacional existen diversas definiciones del término datos personales; sin embargo, a continuación, presentamos las definiciones que consideramos son las más claras y precisas para cumplir con los principales objetivos del presente estudio. Asimismo, incluimos las definiciones de otros términos tales como datos, información y datos no personales con el fin de diferenciarlos del término de interés.

Datos personales:

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) define datos personales como:[4]

> *toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

La Organización para la Cooperación y el Desarrollo Económico (OECD por sus siglas en inglés) los define como:[5]

"cualquier información relativa a una persona identificada o identificable".

De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) los datos personales son:[6]

"cualquier información concerniente a una persona física identificada o identificable".

Otros conceptos importantes son:

Datos: *es la materia prima que se procesa y depura para generar información* (Rumbold & Pierscionek, 2017). *Son la representación primaria de variables cualitativas y cuantitativas que son almacenables, transferibles y que pueden ser visualizadas, controladas y entendidas.*[7]

Datos no personales: *datos que no permiten identificar a una persona o que no tienen ninguna conexión con algún individuo o grupo de individuos* (Rumbold & Pierscionek, 2017)

Información: *son los datos que han sido procesados de manera que sean significativos para el receptor* (Rumbold & Pierscionek, 2017).

De las definiciones de datos personales antes citadas podemos observar que los términos clave, y en común entre ellas, son "información", "identificada" e "identificable". En muchas ocasiones los términos "información" y "datos" son usados como sinónimos; sin embargo, para este estudio es fundamental resaltar que son términos diferentes y que sólo a través del procesamiento o análisis adecuado de los datos se puede generar información valiosa, o de interés, para alguien. Más adelante explicaremos cómo a través de un conjunto de datos personales se puede obtener información personal.

Es cierto que todas las definiciones de datos personales que citamos utilizan el término "información" como sinónimo de "datos"; sin embargo, creemos que se emplean así con el fin de evitar caer en la falacia denominada "definición circular" en la que el término de interés forma parte de su definición. La aclaración

[4] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
[5] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[6] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
[7] Política Nacional de Explotación de Datos (*Big Data*), Colombia, 2018.

de estos dos términos es importante en el ámbito de protección de datos personales puesto que nos permite delimitar cuáles son los datos que la ley debe proteger para garantizar el derecho de privacidad de las personas.

Las definiciones de datos personales citadas arriba también incluyen los términos “identificada” e “identificable”. El primer término se refiere a la determinación inequívoca de la identidad de una persona. El segundo término, de acuerdo con la definición del GDPR, se refiere a la posibilidad de determinar la identidad de una persona de manera directa o indirecta, a través de un identificador, el cual puede ser un identificador *online*, o a través de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Esto permite que el horizonte de todos los elementos que puedan asociarse para identificar a una persona sea muy amplio, además de que la definición considera los elementos de la vida de una persona en diversos aspectos desde físicos hasta sociales, incluyendo identificadores *online*.

Las actuales tecnologías que permiten la existencia de la economía digital, y las emergentes que favorecerán su desarrollo, tienen la capacidad de relacionar o asociar varios elementos *online* de una persona con el fin de determinar la identidad o perfil de dicho individuo. El así llamado *Big Data* es justo una tecnología que puede analizar un gran volumen de una gran variedad de datos para obtener información de interés y potencialmente procesar datos personales con fines comerciales. Lo anterior supone un gran reto para las autoridades y reguladores respecto a la protección de datos personales, considerando que tienen entre sus objetivos principales garantizar los derechos fundamentales de las personas, en particular el derecho a la privacidad, y al mismo tiempo propiciar la innovación y el desarrollo del entorno digital.

En el siguiente apartado presentamos un análisis sobre el valor comercial que tienen los datos personales y su posible impacto de competencia en el sector de telecomunicaciones.

El valor comercial de los datos personales en la economía digital

En la actualidad varias veces hemos escuchado que nuestros datos personales son la moneda de cambio para todas aquellas aplicaciones y servicios *online* que se ofrecen “gratuitamente”. Sin embargo, ¿sabemos realmente cuánto valen nuestros datos personales?, si tienen un precio ¿a quiénes les interesa adquirirlos? y, finalmente, ¿qué importancia tiene para nosotros conocer todo esto?

El objetivo de este apartado es contestar estas preguntas con el fin de comprender la importancia y el trato que reciben nuestros datos personales en la economía digital.

A pesar de que la Unión Europea (UE), a través de una de sus propuestas de Directiva sobre el suministro de contenidos digitales, reconoce que los datos personales pueden ser usados como forma de pago para recibir contenidos digitales,[8] en la actualidad aún no existe un método que permita conocer con precisión el valor monetario o precio de nuestros datos personales. Es verdad que existen diversos estudios que han

[8] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD))

tratado de estimar su valor (e.g. OCDE);[9] sin embargo, debido a la complejidad que esto representa, son estudios unilaterales o que simplemente no contemplan todos los aspectos necesarios para definir un método estándar. Nuestra intención en este capítulo no es determinar con exactitud el precio de los datos personales sino mostrar que sí es viable cuantificar su valor monetario.

En Internet podemos encontrar diversas calculadoras que estiman el precio de los datos personales a partir de la información que se proporciona de una cierta persona. Para nosotros la calculadora que presenta el *Financial Times*[10] es una buena herramienta de referencia que nos permite cuantificar el valor monetario aproximado de los datos personales ligados a diferentes perfiles. Con ese fin, y a manera de ejercicio, decidimos presentar un esquema que muestre el precio (en dólares) de los datos personales para diferentes tipos de personas, con base en algunos de los perfiles que se presentan en el documento sobre la "Adopción de las TIC y usos de Internet en México",[11] tal como se observa en la figura 1.

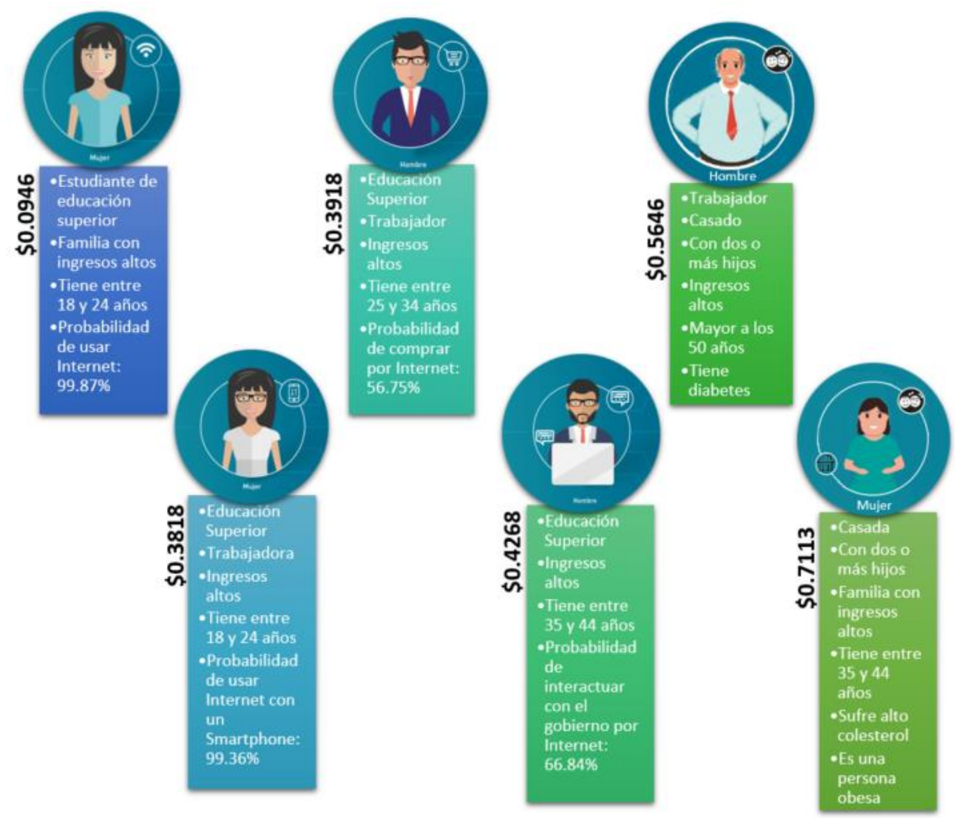

Figura 1. Valor monetario de los datos personales de diferentes personas

Del esquema de la figura 1 podemos observar que el valor monetario de los datos personales aumenta significativamente cuando sabemos que la persona tiene alguna enfermedad, considerando que son

[9] OECD*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, (2013, OECD Publishing).
[10] https://ig.ft.com/how-much-is-your-personal-data-worth/
[11] http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/adopciondelasticyusosdeinternetenmexico.pdf

personas con mayor probabilidad de adquirir medicamentos y productos que mejoren su estado de salud. Esta condición los convierte en blanco de empresas que vendan o promocionen dichos productos, entre otros servicios; sin embargo, y a pesar de lo anterior, estos valores no rebasan un dólar. Es decir, pareciera que el precio de nuestros datos es insignificante para cualquier interesado. No obstante, como lo sugiere un estudio reciente (Malgieri & Custers, 2018), para poder estimar el valor monetario real de los datos personales en la economía digital es necesario tomar en conjunto los siguientes factores:

1. que los datos personales se actualizan de manera constante;
2. que exista la posibilidad de reutilizarlos en cualquier momento y sin costo;
3. que los datos personales son un producto dinámico y no estático, por lo que su valor monetario debe expresarse en euros o dólares por mes;
4. que la combinación de los datos personales genera mayor valor que los datos aislados;
5. que entre más detallados, precisos y completos sean los datos recolectados mayor será su valor.

De acuerdo con los estos factores, el valor monetario real de los datos personales está mejor estimado cuando éstos están actualizados, son completos y precisos, se presentan en conjunto, pueden utilizarse en cualquier momento y tienen el potencial de crear una identidad o perfil digital. Como lo sugiere el mismo estudio (Malgieri & Custers, 2018), el acceso a perfiles digitales evita mayores esfuerzos, tiempo y dinero para las empresas publicitarias a diferencia del acceso a datos personales aislados. Para ejemplificar lo anterior, el mismo estudio menciona que las compañías cobran hasta 10 veces más por publicidad personalizada que por publicidad estándar. Facebook, por ejemplo, cobra $0.0005 de dólar por cada publicidad personalizada en su versión móvil. Si se considera que un usuario estándar ve 20 anuncios de publicidad al día, el ingreso es de $0.01 de dólar por día, lo que a su vez significan $0.3 de dólar por mes aproximadamente. Esto aún pareciera ser insignificante; sin embargo, este precio no considera ninguna subsiguiente venta, renta o suscripción de los mismos datos personales. Si lo anterior se incluyera, es probable que el precio de los datos personales estuviera entre $1 y $10 dólares por mes (Malgieri & Custers, 2018). Con el fin de comprobar el valor estimado anterior, el reporte financiero anual 2016 de Facebook,[12] que presentó a la *Securities and Exchange Commission* (SEC por sus siglas en inglés), menciona que éste obtuvo un ingreso aproximado de $26.89 billones de dólares ($26,890,000,000 dólares) por publicidad. A su vez, menciona que el número de usuarios activos mensuales (MAUs por sus siglas en inglés)[13] que tuvo al 31 de diciembre de 2016 fueron 1.86 billones (1,860,000,000 usuarios). Con estas cifras podemos calcular de manera muy general un precio estimado de los datos personales de cada usuario: $26.89 billones/1.86 billones = $14.45 dólares. Es decir, el valor monetario aproximado de los datos personales de un usuario de Facebook por mes en el año 2016 fue de $1.2 dólares. Esta cifra se encuentra dentro del rango estimado por Malgieri y Custers (2018); sin embargo, es importante resaltar que en nuestro cálculo estamos asumiendo que todos los ingresos por publicidad se obtuvieron por publicidad personalizada o dirigida directamente a los usuarios, con el fin de establecer una relación entre los datos personales de los usuarios y la publicidad. Este supuesto puede no ser completamente acertado;

[12] http://www.annualreports.com/Company/facebook
[13] *Monthly Active Users (MAUs). We define a monthly active user as a registered Facebook user who logged in and visited Facebook through our website or a mobile device, or used our Messenger application (and is also a registered Facebook user), in the last 30 days as of the date of measurement.*

sin embargo, como lo mencionamos con anterioridad, el objetivo de este apartado no es definir con precisión el valor monetario de los datos personales sino demostrar que es viable cuantificar su valor.

Hasta este punto hemos mostrado que es viable cuantificar el valor monetario de los datos personales para la economía digital; sin embargo, aún no hemos abordado a detalle porqué tienen un valor comercial y quiénes están interesados en adquirirlos. En las siguientes líneas trataremos de responder a estos cuestionamientos.

En anteriores párrafos dimos una pista de los posibles interesados de nuestros datos personales (es decir, las empresas publicitarias); sin embargo, para poder comprender de mejor manera cómo y porqué nuestros datos personales generan un valor comercial, es importante entender cómo funcionan los servicios *online* de la economía digital. De manera muy general, los servicios y contenidos que se ofrecen a través de Internet y que se acceden a través de un dispositivo móvil (por ejemplo, redes sociales, servicios en la nube, Wi-Fi gratis, *video streaming*, etc.) utilizan plataformas (o aplicaciones) que funcionan como intermediarias entre el usuario y los servicios; es decir, pareciera que hacen la función de *gateways*, o puertos de entrada, hacia Internet. Toda la actividad de los usuarios sobre estas plataformas genera grandes cantidades de datos, entre ellos los personales, que potencialmente pueden ser usados para crear un cierto valor comercial. Por ejemplo, el análisis de los datos recolectados permite entender el comportamiento de los usuarios respecto a un servicio o aplicación, lo que potencialmente ayuda a mejorar la eficacia de dicho servicio. Esto a su vez permite atraer a más usuarios, quienes generan más datos, dando origen a lo que se conoce como el "efecto de red de datos" (*data-network effect*).[14]

En la actualidad existen muchos servicios que se benefician al conocer mejor a sus potenciales usuarios o clientes. Es decir, entre mejor conocen sus características demográficas, intereses, preferencias y costumbres adquisitivas mejor pueden ofrecer servicios y productos de acuerdo al perfil de los usuarios. Las empresas publicitarias y de marketing son un claro ejemplo de quienes se benefician de la recolección de datos personales a través de las distintas plataformas o aplicaciones. De ahí que las plataformas puedan ofrecer sus servicios "gratis" a través del financiamiento que reciben de estas empresas a cambio del acceso a los datos de los usuarios. Para ilustrar lo anterior, la figura 2 muestra un esquema general del modelo de negocio de la industria de Internet. Por ejemplo, recientemente Google en México puso a disposición su servicio de acceso a Internet "gratis" en centros comerciales, aeropuertos y estaciones de autobús,[15] a través del cual tiene la posibilidad de conocer, entre otros muchos aspectos, los datos de localización, preferencias y sitios web que visitan sus usuarios. Esta información es de gran interés para las empresas publicitarias y de marketing.

[14] https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy
[15] https://www.eleconomista.com.mx/tecnologia/Google-acerca-wifi-de-alta-velocidad-gratuito-a-usuarios-mexicanos-20180313-0052.html

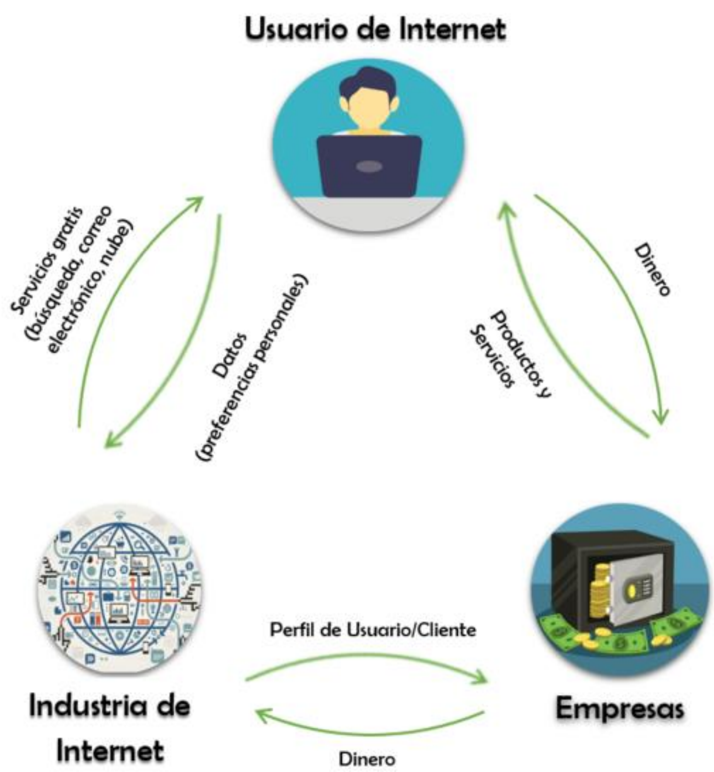

Figura 2. Modelo de negocio general de la industria de Internet

Actualmente la gran variedad de los servicios, aplicaciones y contenidos *online* que existen en el mercado son provistos por dos actores: los operadores tradicionales de telecomunicaciones (operadores) quienes cuentan con infraestructura propia para proveer la conectividad, y los OTTs quienes aprovechan la infraestructura de los operadores para ofrecer sus servicios a través de Internet, y quienes se han convertido en los nuevos jugadores disruptivos de la economía digital (Krämer & Wohlfarth, 2017).

Los OTTs proporcionan tanto servicios substitutos y complementarios al de los operadores (por ejemplo, WhatsApp, Skype, Netflix, Facebook, etc.) como servicios totalmente diferentes y novedosos (Airbnb, Uber, Amazon, etc.). Los primeros son los que tienen mayor impacto sobre los ingresos de los operadores: servicios de comunicación instantánea, servicios de entretenimiento en tiempo real, redes sociales, compartición de archivos, almacenamiento, servicios de banca *online*, servicios basados en la localización del usuario, entre otros (Peitz & Valletti, 2015). Los segundos tienen menor impacto sobre los ingresos de los operadores pero son los que lideran el potencial de crecimiento de los ingresos de la economía digital: servicios de hospedaje, transporte, comercio electrónico, entre otros.[16] En contraste con los modelos de negocio que utilizan los operadores, la gran mayoría de los OTTs, particularmente aquellos que ofrecen servicios substitutos y complementarios al de los operadores, son plataformas que adoptan modelos de negocio de dos o más lados (Krämer & Wohlfarth, 2017) que les permiten ofrecer servicios "gratis" a los usuarios. De esta manera, los OTTs son un claro ejemplo de las plataformas que adquieren el

[16] https://www.cnbc.com/2018/05/22/meet-the-2018-cnbc-disruptor-50-companies.html

financiamiento de terceros (e.g. empresas de publicidad y marketing) para ofrecer sus servicios y contenidos.

Los comercios electrónicos (*e-Commerce*) son otro ejemplo de quienes se benefician de la recolección de datos personales cuando los usuarios ingresan a sus sitios web. Los comercios electrónicos utilizan los datos personales para distintas cosas, en particular para: 1) mostrar publicidad dirigida al usuario; 2) asignar precios personalizados; y 3) brindar ofertas personalizadas de todo tipo (Krämer & Wohlfarth, 2017).

También existen los *data brokers* que se encargan de proveer de datos personales a otras empresas (e.g. redes de publicidad); es decir, su función es agregar, combinar y segmentar perfiles de múltiples usuarios que originalmente se adquirieron de otras empresas por medio de *tracking pixels*. Los métodos que se utilizan para la recolección de los datos son variados, tales como *cookies*, *pixels, tags,* etc., los cuales serán abordados a detalle en el siguiente apartado.

En particular, las empresas de publicidad y comercio electrónico, marketing, compañías de seguros, consultorías y de estadística dependen de los datos que las plataformas recolectan a través de sus servicios. La cadena de valor que existe de los modelos de negocio que se dedican a obtener ganancia de los datos personales está caracterizada por cuatro etapas generales: 1) acceso y recolección; 2) almacenamiento y agregación; 3) análisis y distribución; y 4) uso y explotación de los datos personales.[17]

Recientemente, empresas como Facebook y Google han descubierto que pueden ofrecer diversos servicios de Inteligencia Artificial (AI por sus siglas en inglés), o cognitivos, con los datos que recolectan de sus millones de usuarios. Por ejemplo, para ofrecer servicios de traducción instantánea, reconocimiento facial, y evaluación de personalidad a través de los escritos de una persona.[18]

El valor e interés comercial que existe actualmente por los datos personales ha despertado la preocupación de las autoridades y reguladores. Por una parte, existe la inquietud de proteger los datos personales para poder garantizar los derechos de las personas, en particular el derecho a la privacidad. Esta preocupación es el tema principal de análisis de este estudio, la cual se analizará a detalle en los siguientes apartados. Por otra parte, existe la preocupación sobre el posible poder de mercado que una empresa pudiera adquirir al acumular grandes cantidades de datos en un mercado relevante. Al respecto, existen muchas opiniones sobre la ventaja competitiva que pudiera generar la recolección y análisis de datos personales. Por un lado, están los que argumentan que la acumulación de datos no solo le permitiría a una empresa contar con un dominio temporal del mercado, sino que le permitiría mejorar su calidad más rápidamente que sus competidores, y potencialmente generar una ventaja permanente (Argenton & Prüfer, 2012). Esto a su vez, generaría barreras de entrada y como consecuencia podría constituirse en poder de mercado (Krämer & Wohlfarth, 2015; Schepp & Wambach, 2016).

Por otro lado, están los que mencionan que de existir poder de mercado lo que realmente se tendría que analizar y resolver sería el “abuso” de dicho poder (Krämer & Wohlfarth, 2017). Independientemente de lo anterior, también argumentan que las empresas identificadas como dominantes requerirían cubrir un costo por la actualización de los datos personales que recolectaran, considerando que éstos se vuelven obsoletos

[17] https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en
[18] https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

rápidamente. Lo anterior significa que estas empresas tendrían la necesidad de innovar a un ritmo constante, con el fin de generar confianza a largo plazo entre sus usuarios para mantenerlos y atraer a nuevos usuarios. De suceder lo anterior, los usuarios se verían beneficiados y restringiría la posibilidad de la empresa para aprovechar su potencial poder de mercado (Campbell, Goldfarb & Tucker, 2015).

Finalmente, están los que argumentan que más datos no siempre significa contar con mejores datos. De acuerdo con Hal Varian (*Chief Economist of Google*), cada dato adicional es menos valioso hasta el punto en el que no aporta nada. Lo que realmente es más valioso es el algoritmo que analiza y depura los datos.[19] La anterior opinión se debe analizar contemplando un escenario en el que ya existen mucho datos acumulados, de lo contario no persistiría el argumento que menciona que entre mayor detalle sea proporcionado por un dato adicional mayor será su valor. Por ejemplo, si un dato adicional permite conocer a mejor detalle el perfil de un usuario, mayor será el valor monetario de dicho dato.

Hoy en día existe una nueva tendencia tecnológica que está íntimamente relacionada con el poder de acumulación y análisis de los datos para descubrir patrones y generar información valiosa. *Big Data* es el término utilizado para adquirir y procesar las grandes cantidades de datos que se generan en el ecosistema digital, con el fin de conocer a mayor detalle cualquier cosa o situación y poder, por ejemplo, hacer predicciones sobre lo que sucederá en el futuro. El *Big Data* se caracteriza por su capacidad de procesamiento a gran velocidad, de grandes volúmenes de datos de distintas variedades con el fin de generar valor (es decir, las cuatro “v”). De esta manera, el *Big Data* puede proporcionar beneficios y eficiencias significativas a la sociedad. Sin embargo, si no es usado de manera responsable puede generar serios impactos sobre los derechos y libertades de las personas, particularmente sobre el derecho a la privacidad. Asimismo, como lo mencionamos anteriormente, la acumulación, posesión y uso de los datos podría significar un insumo esencial que impacte en la competencia efectiva del sector.

Haciendo un recuento, en este apartado hemos explicado la viabilidad de cuantificar el valor comercial de nuestros datos personales para comprender su importancia en la economía digital. También identificamos a los interesados comerciales más comunes en adquirir nuestros datos personales para ofrecer diversos servicios y contenidos de manera más efectiva. Asimismo, expusimos algunos argumentos de diversos estudios sobre el posible poder de mercado que una empresa pudiera adquirir al acumular grandes cantidades de datos. Todo esto nos ayuda a comprender que nuestros datos personales juegan un papel muy importante en la economía digital y que existen varios interesados en explotarlos para obtener una ganancia. Nuestro reconocimiento consciente al respecto puede ser el primer paso para entender que necesitamos tener un mejor control de nuestros datos personales, considerando que existen los incentivos para que terceros los recolecten y usen. Creemos que la concientización de las personas sobre el valor de sus datos personales permitiría mejorar su protección sin mermar la innovación y el desarrollo del ecosistema digital. Inclusive consideramos que un mayor nivel de protección y uso adecuado de los datos personales incrementaría la confianza entre las personas y fomentaría el crecimiento de la economía digital.

[19] https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

En el siguiente capítulo abordaremos los distintos métodos que se emplean para recolectar nuestros datos personales, los agentes involucrados y los dispositivos de los que más frecuentemente se adquieren los datos, así como las principales vulnerabilidades que existen.

Análisis del origen del problema

El propósito de este apartado es comprender en qué momento y de qué manera nuestros datos personales son recolectados o adquiridos cuando utilizamos cualquier aplicación o servicio *online*, navegamos en Internet o hacemos uso de algún servicio tradicional de telecomunicaciones. Con ese fin, en esta sección del estudio explicamos la manera en la que las aplicaciones (*apps*) adquieren información de nuestros dispositivos "inteligentes" (*smartphones, tablets, smart TV*, etc.) y el papel que juegan otros actores del ecosistema para dicho propósito (por ejemplo, desarrolladores de *apps*, sistemas operativos, fabricantes de dispositivos, operadores de telecomunicaciones, etc.). También abordamos los métodos más comunes que se utilizan para recolectar y rastrear datos personales cuando navegamos en Internet. Finalmente, presentamos algunas de las principales vulnerabilidades que existen de nuestros datos.

En primer lugar, es importante tener en cuenta que la recolección de los datos personales puede llevarse a cabo de dos formas muy generales: de manera voluntaria y de manera involuntaria. Por una parte, un usuario puede proporcionar sus datos personales voluntariamente, por ejemplo, cuando tiene la necesidad de llenar un formato *online*. Este sería el caso más sencillo en el que un usuario está consciente de proporcionar sus datos personales. Desafortunadamente el usuario promedio no tiene total conocimiento del trato que recibirán sus datos.[20]

Por otra parte, en algunas ocasiones no existe alternativa y nos vemos "forzados" a proporcionar nuestros datos "voluntariamente" para poder usar un servicio o aplicación "gratis". Inclusive en varias ocasiones "voluntariamente" tenemos que permitir el acceso a diversos recursos e información de nuestros dispositivos (por ejemplo, al descargar una *app*). Asimismo, existen servicios que están diseñados con el único propósito de que los usuarios revelen voluntariamente diversos datos personales (por ejemplo, las redes sociales). En consecuencia, los usuarios se enfrentan al dilema entre utilizar un servicio para satisfacer una necesidad a corto plazo y la necesidad de proteger su privacidad a largo plazo (Krämer & Wohlfarth, 2017). Curiosamente, a pesar de que algunas recientes encuestas muestran que la mayoría de los usuarios están más preocupados por su privacidad que en otras épocas, las mismas encuestas revelan que en la actualidad los usuarios comparten su información personal más fácilmente a cambio de pequeñas recompensas o ganancias. A esta incongruencia entre actitudes y comportamiento respecto a la privacidad se le conoce como la "paradoja de la privacidad" (Kokolakis, 2017).

Respecto a la recolección de datos personales de manera involuntaria, ésta sucede cuando el usuario no proporciona su consentimiento o simplemente se adquieren sus datos sin su conocimiento (por ejemplo, rastreo en la web a través de *cookies*, vigilancia gubernamental, robo de identidad, etc.). De hecho, es muy común que los datos personales sean recolectados sin que el usuario tenga conocimiento.

[20] https://www.marketingweek.com/2018/05/25/despite-gdpr-consumers-dont-understand-how-brands-use-data/

Para entender la manera en la que se adquieren nuestros datos personales a través de las aplicaciones, en las siguientes líneas explicamos su funcionamiento.[21]

Las *apps* son aplicaciones de software diseñadas para realizar tareas específicas que requieren de una interacción íntima con el hardware y sistema operativo (SO) de los dispositivos "inteligentes", con el fin de proporcionar el servicio o contenido *online* de interés, o para la gestión de los recursos e información contenida en el dispositivo. Específicamente, las *apps* tienen acceso a los diversos recursos de los dispositivos a través de las *Application Programming Interfaces* (APIs por sus siglas en inglés) provistas por el sistema operativo. Estas APIs, por ejemplo, permiten que las *apps* puedan procesar datos de geolocalización (e.g. a través de GPS y nodos de Wi-Fi) e información recolectada por los múltiples sensores de los dispositivos (e.g. cámaras, micrófonos, acelerómetros, giroscopios, etc.). Asimismo, les permiten tener la capacidad de intercambiar información a través de diversas interfaces de comunicación con otros dispositivos (Wi-Fi, Bluetooth, NFC). Inclusive les permiten acceder a los datos personales de los usuarios (por ejemplo, los contactos). De esta manera, los datos personales contenidos y generados en un dispositivo son adquiridos y procesados cuando la *app* interactúa con el dispositivo para proveer un servicio específico. Por ejemplo, muchas veces cuando tratamos de localizar un establecimiento comercial (por ejemplo, una farmacia), el dispositivo, a través de alguna *app*, nos sugiere e indica el lugar más cercano a nuestra ubicación.

Para tener más claro cuáles son los datos personales que las *apps* pueden recolectar de nuestros dispositivos, en las siguientes líneas presentamos algunos ejemplos que pueden tener un impacto directo en la vida privada de las personas:[22]

- Datos de geolocalización;
- Contactos;
- Datos de tarjetas de crédito o de cualquier otro método de pago;
- Logs de llamadas, SMS y mensajes instantáneos (e.g. WhatsApp);
- Historial del explorador;
- Correos, archivos, mensajes, información borrada (e.g. Google Gmail);
- Identidad de la persona (i.e. nombre);
- Identidad de del teléfono (i.e. ID del teléfono);
- Fotos y videos (e.g. Facebook);
- Datos biométricos (e.g. sistemas operativos);
- Identificadores de la terminal y usuario: IMEI, IMSI, UDID, número telefónico.

Además de los anteriores datos personales que pueden ser recolectados por las *apps*, los exploradores web también pueden recolectar estos y otros datos técnicos de nuestros dispositivos. Por ejemplo, pueden conocer la versión de nuestro sistema operativo, nuestra dirección IP, la resolución de nuestra pantalla, tiempo local, entre otros datos que abordaremos a detalle cuando expliquemos los métodos que se emplean para adquirir estos y otros datos personales.

[21] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[22] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Como podemos observar en la lista anterior, muchos datos personales no sólo permiten establecer directamente la identidad de una persona, sino también son datos que se pueden utilizar indirectamente para identificarla, o para asociarlos con otros datos aislados y así crear un perfil de la persona. Al respecto, la regulación de la Unión Europea (UE) en el sector de las comunicaciones electrónicas (*ePrivacy Directive*) en su recital 24 menciona lo siguiente:[23]

> *Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.*

Es decir, la gran mayoría de los datos resguardados y generados por nuestros dispositivos son datos personales. Estos datos pueden ser recolectados y procesados en el mismo dispositivo; sin embargo, también pueden ser transferidos a través de una conexión externa vía la API en tiempo real a terceros sin el conocimiento del usuario.

En el ecosistema de las *apps* existen otros actores involucrados que también juegan un papel importante en la recolección y tratamiento de nuestros datos personales.[24]

Primeramente, están los desarrolladores de las *apps* (incluidos los propietarios de éstas), que como su nombre lo indica, son los responsables de crear y ponerlas a disposición de los usuarios. En esta categoría están involucradas organizaciones privadas y públicas, así como las compañías y personas que diseñan y desarrollan las *apps*. El papel que juegan los desarrolladores de *apps* en el procesamiento de datos personales es muy importante porque son los que determinan la manera en que la *app* accede y procesa las diferentes categorías de datos personales que existen en nuestros dispositivos. Es decir, son los que definen el propósito y el medio del procesamiento de nuestros datos. De hecho, el GDPR define a este tipo de actores como Controladores (*Controllers* en inglés). En el siguiente apartado presentaremos a detalle varias de las definiciones novedosas que presenta la regulación europea, entre las que se encuentra la figura de Controlador.

Los creadores de sistemas operativos y fabricantes de dispositivos también juegan un papel importante en el procesamiento de los datos personales. Ellos son los responsables de las APIs que permiten a las *apps* el acceso a los diversos recursos de los dispositivos como lo mencionamos con anterioridad. De esta manera, los creadores de sistemas operativos y fabricantes de dispositivos determinan los medios para el acceso a los datos personales resguardados en los dispositivos. Su participación en esta categoría es importante porque son los que definen los procedimientos y estándares para el acceso a la información, y los que pueden delimitar dicho acceso a la información que realmente requieren las *apps* para su buen funcionamiento. En otras palabras, deben cumplir con la “protección de datos desde el diseño y por defecto” del GDPR que también abordaremos en el siguiente apartado. Cumplir con estos conceptos significa que desde el inicio del diseño de una *app* y fabricación de un dispositivo la protección de datos personales debe estar integrada. Inclusive la materialización de estos conceptos en los dispositivos ayudaría

[23] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002
[24] https://www.pdpjournals.com/docs/88097.pdf

a informar y educar a los usuarios sobre las cosas que una *app* puede realizar y la manera en se puede modificar la configuración de su dispositivo para delimitar el procesamiento de sus datos.

Por otro lado, aunque parezca extraño, las tiendas de *apps* también desempeñan un papel importante. En la actualidad existen dos grandes compañías que diseñan y fabrican sus propios dispositivos, crean sus propios sistemas operativos y cuentan con sus propias tiendas de *apps*: Apple y Google. La relación que existe entre estas diferentes categorías es muy íntima. Por ejemplo, las tiendas de *apps* tienen el control de los datos personales que los usuarios voluntariamente proporcionan para el registro, adquisición y compra de éstas. Esta información puede asociarse con el comportamiento del mismo usuario respecto a las *apps* que usa y descarga. Es decir, se puede generar un registro histórico del uso que un usuario hace respecto a diversas aplicaciones. Esta información es de gran interés para los desarrolladores de *apps* y por supuesto para los creadores de sistemas operativos y fabricantes de dispositivos que están ligados a todo este ecosistema.

Finalmente están los terceros involucrados: las redes de publicidad y marketing, los analizadores de datos y los operadores de telecomunicaciones. Como lo mencionamos con anterioridad, muchas *apps* supuestamente gratuitas están financiadas por redes de publicidad y marketing con el fin de tener acceso a los datos de los usuarios. De ahí que los desarrolladores de *apps* tengan un incentivo para permitir la integración de *trackers* a su diseño y así suministrar los datos de los usuarios a estas redes.

Por otra parte, quienes se dedican al análisis de datos permiten que los desarrolladores de *apps* conozcan, por ejemplo, el uso y popularidad de sus *apps* a través del análisis que realizan sobre el comportamiento de los usuarios. También pueden proporcionar servicios de análisis de los datos que exclusivamente genera una *app*; es decir, realizar procesamiento de datos para los desarrolladores. En este caso, los analizadores de datos hacen exclusivamente la función de Procesadores a diferencia de los desarrolladores de *apps* que hacen la función de Controladores. Es importante distinguir el papel que desempeñan los diversos actores en el tratamiento de los datos personales para comprender la distinción y regulación impuesta por la UE a través del GDPR. Cuando los analizadores de datos recolectan y procesan datos personales para sus propios fines a través de diversas *apps* se convierten en Controladores. Por ejemplo, cuando proporcionan un análisis estadístico a gran escala de la movilidad de las personas en una ciudad. Más adelante veremos que para este ejemplo específico su obligación respecto a la protección de datos personales, particularmente en México, dependería de si los datos utilizados para dicho fin fueron datos personales o datos anónimos y agregados que cumplen con la definición de disociación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP). En otras palabras, un analizador de datos no tendría la obligación de cumplir con la regulación sobre datos personales si los datos recolectados y procesados no pudieran asociarse a ninguna persona, ni permitieran por su estructura, contenido o grado de desagregación identificar a alguna persona. Es decir, si fueran datos no personales de acuerdo a la definición que mencionamos en el primer apartado. De lo contrario, tendrían toda la obligación de cumplir con la regulación.

Los operadores de telecomunicaciones también juegan un papel relevante en el ecosistema de las aplicaciones y recolección de los datos personales. Su participación comienza cuando ofertan y proporcionan dispositivos terminales con sus propias configuraciones. Esto es, los operadores ofrecen dispositivos hechos a la medida (*customized*), cuya configuración por *default* establece el procedimiento de actualización respecto a la seguridad y funcionalidad de los dispositivos. Además, en dichos dispositivos los operadores incluyen *apps* que fueron pre-instaladas y que comúnmente no consideran la configuración de preferencia que desearían tener los usuarios para proteger su privacidad.

Fuera del ecosistema de las *apps*, los operadores de telecomunicaciones cuentan con la posibilidad de recolectar, resguardar y procesar datos personales de sus usuarios cuando éstos hacen uso de sus servicios tradicionales. Por ejemplo, tienen la capacidad de estimar la ubicación de sus usuarios a través del conocimiento de la antena que les está proporcionando el servicio. También cuentan con los *Call Detail Record*s (CDRs por sus siglas en inglés) que son metadatos (datos sobre los datos) o información respecto a las llamadas y mensajes que realizan sus usuarios para elaborar la facturación de los servicios. Estos CDRs proporcionan información sobre dónde, cómo y cuándo se realizaron las llamadas o los mensajes. Con el fin de conocer con mayor precisión los datos personales que los operadores de telecomunicaciones pueden recolectar, en el siguiente párrafo incluimos las categorías de datos que AT&T recolecta de sus usuarios:[25]

Datos de contacto: datos para contacto general o con fines administrativos que pueden incluir, entre otros, el nombre, giro del trabajo, cargo, empleador, dirección, número telefónico, correo electrónico, nombre del usuario de mensajería instantánea, y datos similares.

Datos de identificación del dispositivo: datos que identifican un dispositivo desde el cual (o al que) se envían (o reciben) las comunicaciones electrónicas; puede incluir la dirección IP, la dirección MAC, el número de Identidad de Equipo Móvil Internacional (IMEI), el número de Identidad de Suscriptor Móvil Internacional (IMSI), el número de serie, y el Identificador de Dispositivo Único (UDID).

Metadatos de comunicaciones electrónicas: datos procesados en una red de comunicaciones electrónicas con el propósito de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas (pero sin incluir el contenido de las comunicaciones); incluye datos utilizados para rastrear e identificar el origen y destino de una comunicación, datos sobre la ubicación del dispositivo en el contexto de la prestación de servicios de comunicaciones electrónicas, y la fecha, hora, duración y tipo de comunicación.

Datos de autenticación: nombre de usuario, contraseña, número de identificación personal, sugerencias de contraseñas, y datos similares para autenticar a los usuarios en relación con el uso de los servicios o el acceso a la información relacionada con los servicios.

Por otro lado, cuando navegamos en Internet es común que la gran mayoría de los sitios web recolecten nuestros datos personales para identificarnos y obtener información sobre nuestra persona. Estos sitios web adquieren nuestra información personal a través de diversos métodos que rastrean nuestra actividad en Internet. El método de rastreo más común es el *HTTP cookie* que explicaremos más adelante. En general, estos métodos descubren y generan información personal a través de las cosas que buscamos, visitamos, contactamos o compramos en Internet.

[25] AT&T Business Customer GDPR Privacy Notice

Con el fin de tener un panorama general de todos los métodos y tecnologías que se emplean para rastrear nuestra actividad en Internet y obtener nuestra información, en la tabla 1 presentamos la descripción y propósito de algunos métodos (Bujlow, Carela-Español, Solé-Pereta & Barlet-Ros, 2017).

Tabla 1. Métodos de rastreo en Internet

Métodos de rastreo	**Descripción**	**Alcance**
Solo sesión		
Identificadores de sesión almacenados en campos ocultos	Se basa en pasar un identificador de un sitio web a otro en la URL o en un campo oculto en un formulario web.	Identidad de sesión
Autenticación explícita de formulario web	Requiere que un usuario inicie sesión en un sitio web antes de usar sus recursos.	Identidad de usuario
Propiedad Window.name DOM	Utiliza una propiedad especial Document Object Model para almacenar hasta 2 MB de datos, que luego se pueden compartir entre las diferentes partes visitadas.	Identidad de sesión
Basado en almacenamiento		
HTTP Cookies	Utiliza un mecanismo de navegador incorporado para almacenar una pequeña cantidad de datos en la computadora del usuario.	Identificador de instancia del navegador
Cookies Flash y servicio de persistencia Java JNLP	Utiliza el almacenamiento permanente de complementos de navegador Flash y Java para preservar los datos de seguimiento en la computadora del usuario.	Identificador de instancia del sistema operativo
Objeto Flash de conexión local	Utiliza un objeto compartido entre diferentes instancias de Flash que se ejecutan en una sola computadora para intercambiar mensajes entre ellas.	Identificador de instancia del sistema operativo
Almacenamiento aislado Silverlight	Utiliza el almacenamiento permanente de los complementos del navegador Silverlight para conservar los datos de seguimiento en la computadora del usuario.	Identificador de instancia del navegador

Almacenamiento global, local y de sesión HTML5	Utiliza almacenamientos estándar HTML5 para conservar los datos de seguimiento en la computadora del usuario.	Identificador de instancia del navegador
Base de datos web SQL y HTML5 IndexedDB	Utiliza un navegador SQLite no estándar para preservar los datos de seguimiento en la computadora del usuario.	Identificador de instancia del navegador
Almacenamiento de datos de usuario de Internet Explorer	Utiliza un almacenamiento propio de Internet Explorer para preservar los datos de seguimiento en la computadora del usuario.	Identificador de instancia del navegador
Basado en caché		
Caché web	Se basa en la presencia de algunos elementos distintivos en el caché del navegador para averiguar si un sitio web específico ya fue visitado por el usuario.	
Incrustar identificadores en documentos almacenados en caché		Identificador de instancia del navegador, historial de navegación
Pruebas de rendimiento de carga		Historial de navegación
ETags y últimos encabezados modificados		Identificador de instancia del navegador
Caché de DNS	Se basa en la presencia de solicitudes DNS previas en la memoria caché para averiguar si un sitio web específico ya fue visitado por el usuario.	Historial de navegación
Cachés operacionales	Aprovecha cachés de navegador avanzados (caché de redirección HTTP 301, caché de autenticación HTTP, caché de seguridad de transporte estricto de HTTP) para averiguar si un sitio web específico ya fue visitado por el usuario.	
Caché de redirección HTTP 301		Identificador de instancia del navegador
Caché de autenticación HTTP		Identificador de instancia del navegador
Caché de seguridad de transporte estricto de HTTP		Identificador de instancia del navegador
Caché de reanudación de sesión de TLS e Identificador de sesión de TLS		Identificador de instancia del navegador
Fingerprints		
Toma de huellas dactilares de red y ubicación	Utiliza varios medios para determinar la dirección IP real y la ubicación física del usuario.	Dirección IP, país del usuario, ciudad y vecindario
		Identificación del dispositivo, dirección IP (completa o una parte), sistema operativo, resolución de pantalla, zona horaria, lista de frentes del sistema, navegador web, información sobre hardware (ratón,

Toma de huellas digitales del dispositivo	Utiliza varios medios para distinguir un dispositivo físico de otro en la web.	acelerómetro de teclado, capacidad multitáctil, micrófono, cámara), marcas de tiempo TCP
Huella digital de instancia del sistema operativo	Utiliza varios medios para distinguir una instancia de un sistema operativo de otra en un dispositivo físico particular a través de la web.	Identificador de instancia del sistema operativo, versión y arquitectura del Sistema operativo, idioma del sistema, idioma específico del usuario, zona horaria local, fecha y hora local, lista de fuentes del sistema, profundidad del color, dimensiones de la pantalla, capacidades de audio, acceso a la cámara del usuario, micrófono y disco duro, soporte de impresión, identificadores de disco duro, parámetros TCP / IP, nombre de equipo, identificador de producto de Internet Explorer, identificador de producto digital de Windows, controladores de sistema instalados, identificador de instancia de sistema operativo almacenado por un applet privilegiado de Java
Huella digital de la versión del navegador	Utiliza propiedades HTML5, JavaScript y CSS para determinar la versión real del navegador web del usuario.	Versión detallada del navegador
Huella digital de instancia de navegador utilizando lienzo	Distingue una instancia de un navegador web de otra a través de la web mediante el uso de imágenes dibujadas en el lienzo del navegador.	Identificador de instancia del navegador
Huella dactilar de instancia del navegador utilizando el historial de navegación web	Distingue una instancia de un navegador web de otra en la web mediante el uso del historial de navegación web.	Identificador de instancia del navegador, historial de navegación
Otros métodos de huellas dactilares de instancia de navegador	Utiliza el análisis de respuestas HTTP, la lista de complementos del navegador, la resolución de pantalla, el desplazamiento de la zona horaria y otras propiedades para distinguir una instancia de un navegador web de otra a través de la web.	Identificador de instancia del navegador, versión de navegador detallada, formatos admitidos de imágenes y archivos multimedia, idiomas preferidos y aceptados, lista de complementos del navegador, idioma del usuario del navegador, dimensiones del navegador, versión Flash, resolución de pantalla, profundidad de color, zona horaria, fuentes del sistema, IP dirección, cabeceras HTTP aceptadas, cookies habilitadas, limitaciones de supercookies
Otros mecanismos de seguimiento		
	Utiliza encabezados distintivos especiales adjuntos a todas las solicitudes HTTP	

Encabezados adjuntos a solicitudes HTTP salientes	salientes, para que la web sepa exactamente quién está pidiendo contenido.	Identificación del cliente
Usar metadatos telefónicos	Utiliza los registros de llamadas capturados desde el dispositivo de un usuario para descubrir la identidad del usuario y para obtener información sensible, como la condición de salud (incluida la mental), las creencias religiosas y las adicciones.	Condición de salud (incluida mental), creencias religiosas y adicciones de una persona real específica
Ataques de tiempo	Utiliza las diferencias en el tiempo necesario para representar diferentes árboles DOM para determinar valores booleanos, por ejemplo, si el usuario tiene una cuenta en un sitio web probado.	Valores booleanos que dependen del aspecto del sitio web (e.g. si el usuario está conectado a un servicio en particular), robando cualquier gráfico incrustado o representado en la pantalla
Utilizando la colaboración inconsciente del usuario	Utiliza varios medios (como CAPTCHA falsos o cámara frontal del equipo portátil del usuario) para determinar la actividad de navegación pasada del usuario.	Historial de navegación, Identificador de instancia del navegador, ubicación del usuario
Clickjacking	Presenta un elemento del sitio web sensible fuera de contexto, por lo que el usuario actúa fuera de contexto. Esto puede llevar a comprometer el anonimato de los usuarios, robar correos electrónicos de usuarios y datos privados, y espiar a un usuario mediante una cámara web.	Correo electrónico del usuario y otros datos privados, credenciales de Paypal, espiar a un usuario mediante una cámara web
Evercookies (supercookies)	Combina varios mecanismos de seguimiento basados en el almacenamiento para poder rastrear al usuario de manera más eficiente.	Identificador de instancia del sistema operativo, Identificador de instancia del navegador

Asimismo, en las siguientes líneas explicamos los métodos más comunes con el fin de comprender a detalle su funcionamiento e implicaciones en la recolección de los datos personales (Bujlow et al., 2017).

Los *HTTP cookies* son bits de texto (máximo 4KB) que se almacenan en el disco duro de los dispositivos, o en el espacio designado para los archivos de los navegadores, cuando un usuario visita por primera vez un sitio web. Los archivos *cookies* contienen un identificador de usuario único que permite que el sitio web pueda recuperar este identificador cada vez que el usuario vuelve a visitar el sitio. Inclusive, el identificador permite que el sitio web pueda rastrear la actividad del usuario en otros sitios al integrar los mecanismos de rastreo de los otros sitios. Por ejemplo, cuando un usuario accede a los botones de Facebook que aparecen en algún sitio web el identificador del *cookie* es enviado a Facebook. De esta manera ambos sitios conocen la actividad del usuario en un tiempo específico y con la posibilidad de generar un perfil digital de éste.

El *HTTP cookie* ha sido el método de rastreo más popular; sin embargo, los métodos evolucionan todo el tiempo a través de técnicas que son cada vez más complejas e intrusivas que intentan violar los mecanismos de privacidad de los navegadores. Tal como lo muestra la tabla 1, varios métodos utilizan JavaScript que les permite acceder a diversa información de los sistemas operativos y de los navegadores de los usuarios. Esta posibilidad permite que los métodos de rastreo puedan generar *fingerprints* o identificadores únicos de los usuarios con mayor alcance. Además de JavaScript, hay métodos que utilizan otras tecnologías como Flash y Java que les permite ser aún más poderosos.

Los *fingerprints* son un grupo de métodos que utilizan una amplia gama de tecnologías capaces de identificar y recolectar diversos datos de los usuarios. Es decir, pueden crear un identificador único para un dispositivo, sistema operativo, versión de navegador o cualquier otra instancia cuando el usuario navega en un sitio web. Por ejemplo, los *fingerprints* tienen la capacidad de recolectar la dirección IP, la versión del sistema operativo, la resolución de la pantalla, la zona horaria, el ID del dispositivo, tipo y versión del navegador, información del hardware como mouse, teclado, micrófono, cámara, entre otros. De esta manera, a diferencia de los *cookies*, el usuario puede ser rastreado en múltiples sitios web que pertenecen a diferentes entidades. Estos métodos no generan *cookies* y el usuario no necesita iniciar sesión para ser rastreado; es decir, el seguimiento es transparente para el usuario y funciona independientemente de si el navegador acepta *cookies* o no. Por lo tanto, un usuario promedio no tiene ningún medio para saber si es rastreado o al menos para saber cómo prevenirlo. Una forma de evitar los *fingerprints* es al desactivar JavaScript, Java y Flash; sin embargo, no siempre se evita que se generen estos identificadores.

Web Cache es un grupo de métodos que permite identificar los sitios web que previamente fueron visitados por un usuario. Cuando un navegador descarga un objeto (e.g. una imagen) generalmente se almacena en el caché del navegador para una visualización más rápida cuando el usuario visita el sitio web nuevamente. Por lo tanto, cuando un usuario navega en un sitio web, el sitio web puede determinar fácilmente si este usuario lo visitó antes (si el objeto se extrae de la memoria caché) o no (si el objeto se descarga del servidor). Cuando una red publicitaria tiene sus objetos en muchos sitios web, ésta puede compararlos fácilmente con las copias en caché y determinar qué sitios fueron visitado por el usuario. De igual manera que los anteriores métodos, éste puede generar un perfil digital del usuario.

En virtud de lo anterior, observamos que los datos personales son el blanco principal de recolección para varios servicios *online* y que por ello existen diversos métodos y tecnologías que continuamente evolucionan para lograr su cometido. En el apartado anterior mencionamos el valor que representan los datos personales para la economía digital, lo que origina la susceptibilidad de los datos para ser explotados comercialmente con o sin el conocimiento de los usuarios. Dicho de otra manera, la privacidad, confidencialidad, seguridad y propiedad de los datos personales son vulnerables por significar un valor comercial. Desafortunadamente la explotación comercial de los datos personales no es la única vulnerabilidad que presentan sino también existen otras más severas que están dirigidas a realizar algún tratamiento ilícito o malintencionado de los datos, inclusive ser susceptibles de inspección por autoridades gubernamentales, empresas u organizaciones que tienen el poder pero que no necesariamente tienen la autorización para hacerlo, o simplemente aprovechan los vacíos legales.

El tratamiento ilícito de los datos está relacionado con las amenazas técnicas que existen actualmente en el mundo digital, debido a las carencias de seguridad existentes en las aplicaciones móviles, en los sistemas operativos o en las redes de los operadores. Por ejemplo, algunos riesgos que están asociados con los dispositivos que utilizamos para conectarnos a Internet son: el *phishing, malware, hacking*, suplantación e intercepción, ingeniería social, entre otros, para incurrir en delitos informáticos, prácticas anticompetitivas u obtener ventajas en múltiples situaciones relacionadas con diversos ámbitos, como el económico, político, social, laboral, entre otros, cuyo principal objetivo es obtener beneficios ilícitos en detrimento de otras personas u organizaciones (Broadhead, 2018). De acuerdo con estadísticas de Symantec el malware en dispositivos móviles a nivel mundial aumentó 54% en 2017 respecto al 2016, y bloqueó en promedio 24,000 aplicaciones móviles maliciosas diariamente en 2017.[26]

El tratamiento malintencionado se refiere al uso inadecuado de información personal con el fin de desorientar a las personas y dañar principalmente la reputación de un individuo, sin descartar también la posibilidad de perjudicar a una organización, empresa o entidad, cuyo objetivo es obtener algún beneficio económico, social o político. Generalmente se utiliza información sensacionalista para crear impacto en las redes sociales o medios de comunicación (e.g. *fakenews*).

Por otra parte, las autoridades gubernamentales pueden tener el poder suficiente para acceder a datos personales sin que los mecanismos diseñados para proteger dichos datos puedan impedirlo, en un ámbito en el que el marco legal no es claro respecto a las facultades de cada autoridad. Esto puede suceder cuando la "cooperación" por parte de los usuarios ocurre a partir de mandatos sin los cuales probablemente no habrían dado su consentimiento para compartir información que les solicita el gobierno (Mantelero, 2014).

Es evidente entonces que las vulnerabilidades de los datos personales pueden afectar la privacidad y confidencialidad de las personas, ya sea por el valor que éstos representan para la economía digital o por la posibilidad de obtener alguna ventaja en detrimento de otra persona u organización. Por lo tanto, de acuerdo con las explicaciones que hemos venido realizando y por la observación anterior, en el siguiente apartado analizamos las políticas y regulaciones que existen en el mundo para la protección de los datos personales, particularmente las regulaciones que existen en nuestro continente americano. Asimismo, analizamos la normativa europea que entró en vigor el pasado 25 de mayo de 2018 respecto a la protección de datos personales y su libre circulación.

Sin duda el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) es actualmente el referente internacional más completo y actualizado, que estable las normas para proteger los derechos y libertades fundamentales de las personas sin obstaculizar el desarrollo de la economía digital a través de la libre circulación de dichos datos. El GDPR es entonces el reglamento que permite hacer frente a los actuales retos que imponen los servicios *online* al utilizar los datos personales como su activo principal. De ahí que en el siguiente apartado dediquemos gran parte de su contenido al análisis del GDPR, con el fin de

[26] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf

comparar las regulaciones que existen en nuestro continente e identificar las áreas de oportunidad que fortalezcan nuestro marco regulatorio.

Análisis de políticas y regulaciones en el mundo

Uno de los principales objetivos de este apartado es presentar y analizar los conceptos y normas clave del GDPR relativos a la protección y libre circulación de los datos personales. Para tal fin, en los siguientes párrafos presentamos el análisis del contenido de algunos de los artículos del reglamento que consideramos son de mayor relevancia para este estudio. Asimismo, presentamos una comparativa entre la regulación europea y las regulaciones de algunos de los países de nuestro continente, con la intención de identificar las áreas de oportunidad que permitan fortalecer nuestro marco regulatorio.

El propósito fundamental del GDPR es hacer frente a los actuales retos de la economía digital respecto a la protección de los datos personales, a través del fortalecimiento del derecho a la privacidad digital de las personas sin mermar la innovación y el desarrollo de esta nueva economía. Particularmente, el GDPR establece las normas para la recolección, almacenamiento, procesamiento, acceso, utilización y transferencia de los datos personales que realizan los tratadores de datos en el ecosistema digital. Asimismo, el GDPR permite que las personas tengan el control y gestión de sus datos personales para fortalecer su derecho a la privacidad.

Con el propósito de comprender con mayor detalle el contenido del GDPR, tal como lo mencionamos con anterioridad, en los siguientes párrafos presentamos el análisis del contenido de los artículos más relevantes y novedosos que son de interés para este estudio.

En primer lugar, el GDPR establece claramente el **objeto y ámbito** de su aplicación (artículos 1 y 2, respectivamente). Al respecto, es importante resaltar que además de mencionar las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales, el reglamento también comprende las normas para la libre circulación de dichos datos. Este último aspecto es fundamental, considerando que el GDPR avala la posibilidad de circular los datos personales dentro de la UE y transferir los datos personales hacia terceros países u organizaciones internacionales. Asimismo, el GDPR indica que su aplicación recae en el tratamiento total o parcialmente automatizado y no automatizado de los datos personales. Es claro que el tratamiento automatizado es el de mayor interés y aplicación en los servicios *online,* debido a las propias características de procesamiento digital que utilizan dichos servicios.

El GDPR también reconoce el rápido desarrollo de las tecnologías, sobre todo la capacidad que actualmente tienen las redes de telecomunicaciones para transferir y procesar grandes volúmenes de datos, a grandes velocidades y a través de diversos servidores ubicados en distintos países del mundo. De ahí que el GDPR en su artículo 3 mencione que la regulación aplica a los Controladores y Procesadores de datos personales establecidos en la UE, independientemente del lugar donde se realice el procesamiento de los datos de los ciudadanos o residentes europeos. Además, señala que el reglamento también aplica a los Controladores y Procesadores de datos personales que no estén establecidos en la UE y que ofrezcan bienes o servicios en ese continente, o que simplemente monitoreen el comportamiento de los europeos.

De las **definiciones** que presenta el GDPR (artículo 4), consideramos que destacan las siguientes: elaboración de perfiles, seudonimización, datos genéticos, datos biométricos, datos relativos a la salud, normas corporativas vinculantes y violación de la seguridad de los datos personales. Sin explicar a detalle cada uno de los anteriores conceptos, consideramos que es importarte destacar al menos la definición de elaboración de perfiles y seudonimización. El GDPR menciona que la elaboración de perfiles es toda forma de tratamiento automatizado de los datos personales que permite determinar y predecir los aspectos personales de una persona física (i.e. situación económica, salud, preferencias, intereses, ubicación, comportamiento, etc.). Este concepto es clave para la regulación sobre la protección de datos personales, considerando que el principal objetivo de los métodos de rastreo es crear perfiles digitales de los usuarios con el fin de proveer publicidad y servicios personalizados, de acuerdo con lo que mencionamos en el apartado anterior. Respecto a la definición de seudonimización, el GDPR menciona que este término se refiere al procesamiento de datos personales de tal manera que los datos ya no puedan atribuirse a una persona en específico, sin utilizar información adicional. Este concepto también es clave debido a que tiene estrecha relación con la posibilidad que tendrán los proveedores para brindar un servicio *online* o de *Big Data*, a través del procesamiento y análisis de datos anónimos y agregados de los usuarios. No obstante, es importante resaltar que los datos seudonimizados continúan siendo datos personales a diferencia de los datos anónimos, por lo que requieren de protección.

El GDPR contempla los siguientes **principios** (artículo 5): 1) licitud, lealtad y transparencia; 2) limitación de la finalidad; 3) minimización de los datos; 4) exactitud; 5) limitación del plazo de conservación; 6) integridad y confidencialidad; y 7) responsabilidad proactiva. De acuerdo con un estudio (Tikkinen-Piri, Rohunen, & Markkula, 2018) estos principios son básicamente los mismos que se establecían en la Directiva 95/46/EC (DIR95) de la UE y que es sustituida por el actual GDPR; sin embargo, el estudio también menciona que el GDPR adiciona el principio de transparencia en el procesamiento de los datos y el de responsabilidad proactiva. Además, menciona que el GDPR aclara otros principios como el de minimización de los datos. Al respecto, el GDPR establece que los datos personales deben ser procesados de manera transparente para el usuario; es decir, que éste conozca los fines y medios en el procesamiento de sus datos personales. Para la observancia de este principio, el GDPR menciona que el Controlador de los datos personales debe demostrar que sus operaciones de procesamiento cumplen a cabalidad con las disposiciones del GDPR. Con relación al principio de responsabilidad proactiva, el GDPR introduce este concepto con la finalidad de establecer claramente la obligación que tienen los responsables del tratamiento de los datos con el cumplimiento de todos los principios definidos en el reglamento. Respecto al principio de minimización, el GDPR aclara que el procesamiento de los datos debe ser limitado a lo mínimo necesario en relación con los fines para los que fueron adquiridos y tratados.

Respecto al principio de licitud que establece el GDPR, el reglamento incorpora las condiciones bajo las cuales los responsables obtendrán el consentimiento para el tratamiento de los datos personales de los menores de edad (artículo 8). En particular, el GDPR establece que el procesamiento de los datos personales de un menor es legal si éste tiene al menos 16 años; sin embargo, si el menor es más joven, el procesamiento es legal sólo si se obtiene el consentimiento por parte de los padres. Para ello, el Controlador de los datos está obligado a realizar los esfuerzos pertinentes para obtener y verificar el consentimiento a través de la tecnología disponible.

El GDPR también establece el **derecho de acceso** (artículo 15) con el fin de permitir que el usuario conozca el procesamiento o tratamiento que están teniendo sus datos. Específicamente, el derecho de acceso contempla la posibilidad del usuario de conocer los fines del tratamiento, los destinatarios a los que se les comunicarán sus datos personales, el plazo previsto de conservación, el derecho a la rectificación, supresión, limitación u oposición del tratamiento (i.e. derechos ARCO en la regulación mexicana), inclusive la información sobre la manera en la que se elaboran sus perfiles digitales. Con relación a este derecho de acceso, sobresale el **derecho al olvido** (artículo 17) a través del cual el GDPR establece que las personas tienen el derecho de obtener del Controlador la eliminación de sus datos, así como la abstención de una posterior diseminación por cualquiera de las siguientes razones: 1) si los datos personales ya no son necesarios con relación a los propósitos originales por los cuales se recolectaron; 2) si la persona retira su consentimiento y no existe otro fundamento legal para el procesamiento; 3) si la persona se opone al procesamiento por razones específicas y no existen elementos legítimos; 4) si la persona se opone al procesamiento para fines de marketing directo; y 5) si los datos son procesados ilícitamente. El derecho al olvido es fundamental para respetar con precisión los fines y propósitos para los cuales los datos fueron recolectados y procesados inicialmente; sin embargo, el reto radica en la posibilidad real de borrar por completo cualquier dato personal que exista en Internet en el momento que una persona decida eliminar sus datos.

La **portabilidad de datos** (artículo 20) es un nuevo derecho incluido en el GDPR. Este derecho permite que una persona reciba los datos personales que le incumban, y que haya facilitado a un Controlador para su procesamiento, en un formato estructurado, de uso común y lectura mecánica, con el fin de transmitirlos a otro Controlador y con la posibilidad de realizar dicha transmisión de manera directa si resulta técnicamente factible. Este nuevo derecho posibilita que las personas tengan el control sobre sus datos personales que originalmente fueron suministrados a un Controlador de un servicio *online*, así como de los datos que dicho servicio haya generado de las personas. Por ejemplo, este derecho permite que cualquier usuario de Facebook pueda solicitar la portabilidad de sus datos personales a otra plataforma similar como lo es Google+.

El **derecho de oposición** (artículo 21) del GDPR menciona que cualquier persona tiene derecho a oponerse en cualquier momento al procesamiento de sus datos. Este derecho contempla la oposición que tengan las personas cuando sus datos sean utilizados para fines de mercadotecnia o marketing directo. Es decir, las personas tienen derecho a objetar el tratamiento de sus datos personales respecto a la elaboración de perfiles digitales que funcionen como insumo para el marketing. En estos casos, el Controlador de los datos personales tiene la obligación de suspender el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los intereses de las personas.

Respecto a las obligaciones generales que impone el GDPR a los **Controladores y Procesadores** de datos personales (artículos 24 a 31), resaltan las siguientes: 1) protección de datos **desde el diseño y por defecto** (*protection by design and by default* en inglés); 2) corresponsabilidad del tratamiento; 3) obligaciones del Procesador; 4) registro de las actividades del tratamiento; y 5) cooperación con la autoridad de control. Con relación a la seguridad, el GDPR menciona que el Controlador de los datos personales aplicará las medidas técnicas y organizativas apropiadas, como la seudonimización (o encriptación) y la minimización de datos, con el fin de que desde el diseño se protejan los datos y que por defecto sólo sean objeto de tratamiento los datos necesarios para cada uno de los fines del tratamiento. Por otro lado, cuando dos o más Controladores determinen conjuntamente los objetivos, fines y medios del tratamiento de los datos, éstos serán considerados corresponsables del tratamiento. En lo concerniente a las obligaciones de los Procesadores, el GDPR menciona que el Controlador elegirá al Procesador que ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas que cumplan con el reglamento.

Además, el GDPR indica que el Procesador de datos no recurrirá a otro Procesador sin la autorización previa por escrito del Controlador. Todas estas obligaciones específicas que contempla el GDPR tanto para el Controlador como para el Procesador de datos personales son fundamentales para identificar el papel y responsabilidad de cada uno de los involucrados en el tratamiento de datos personales. En uno de los apartados anteriores mencionamos que existen muchos actores involucrados en el tratamiento de los datos personales, desde los desarrolladores de *apps* hasta los operadores de telecomunicaciones. Es por ello que la distinción y aclaración que hace el GDPR sobre las obligaciones de los Controladores y Procesadores en el tratamiento de los datos es muy importante para su adecuada protección. No obstante, el reto clave de esta regulación específica recae en la identificación precisa del papel que juega cada uno de los involucrados en la provisión de un servicio *online*. Pareciera que esta identificación tuviera que realizarse caso por caso en un ecosistema digital que incorpora diariamente a nuevos actores en el mundo digital.

Como parte de las obligaciones de los Controladores y Procesadores de datos también se encuentra la del registro de las actividades del tratamiento. Esta obligación señala que el Controlador tiene que realizar un registro de las actividades del tratamiento efectuadas bajo su responsabilidad para el caso en que la autoridad de control lo solicite. Finalmente, el GDPR también señala que tanto el Controlador como el Procesador, y en su caso sus representantes, tienen que cooperar con la autoridad de control para el desempeño de sus funciones.

Adicional a la protección de datos desde el diseño y por defecto que señala el GDPR, el reglamento también menciona (artículo 32) algunas **medidas técnicas y organizativas** concretas que los Controladores y Procesadores deben aplicar como: a) la seudonimización y el cifrado de los datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios del tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso de los datos personales de forma rápida en caso de incidente físico o técnico; y d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Todas estas medidas de seguridad tienen como objetivo proteger los datos personales contra la destrucción, pérdida o alteración accidental o ilícita de los datos transmitidos, conservados o tratados, así como por la comunicación o acceso no autorizados a dichos datos.

Otra de las obligaciones que indica el GDPR para los Controladores de datos personales es la **notificación** que deben realizar a la autoridad de control cuando ocurra una violación a la seguridad de los datos personales (artículo 33). Al respecto, el GDPR señala que el Controlador tiene que notificar a la autoridad de control sobre una violación sin dilación indebida y, de ser posible, a más tardar en las 72 horas posteriores.

El GDPR también incorpora una nueva obligación para los Controladores: la **evaluación de impacto** relativa a la protección de los datos previa a la ejecución de cualquier tratamiento o procesamiento (artículo 35). El objetivo de esta nueva obligación es prevenir que ocurra un riesgo sobre los derechos y libertades de las personas cuando un proveedor ponga a disposición un nuevo servicio, particularmente si utiliza nuevas tecnologías. Esta previa valoración impacta directamente en la evaluación sistemática y exhaustiva que un proveedor quiera realizar sobre los aspectos personales de una persona para la elaboración, por ejemplo, de perfiles digitales a través de procesamientos automatizados. El GDPR indica que la evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones del tratamiento; b) una evaluación de la necesidad y proporcionalidad de las operaciones del tratamiento; c) una evaluación de los riesgos para los derechos y libertades de las personas; y d) las medidas previstas para afrontar los riesgos.

Respecto a las transferencias de datos personales a **terceros países u organizaciones internacionales** (artículo 44 al 46), el GDPR establece las condiciones que deben cumplir los Controladores y Procesadores de datos personales para realizar una transferencia adecuada. Estas condiciones son dos: 1) transferencias basadas en una decisión de adecuación; y 2) transferencias mediante garantías adecuadas. La primera establece que una transferencia puede realizarse si el tercer país, territorio, sectores específicos de ese tercer país o la organización internacional garantizan un nivel de protección adecuado. Esta decisión se realiza al evaluar el Estado de Derecho respecto a los derechos humanos y libertades fundamentales, el funcionamiento efectivo e independencia de la autoridad de control y los compromisos internacionales asumidos por el país u organización sobre acuerdos o instrumentos jurídicamente vinculantes. En caso de que no se haya realizado una decisión de adecuación de este tipo, el Controlador o el Procesador de datos personales sólo puede transmitir los datos a un tercer país u organización internacional si ofrece las garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. La posibilidad que plantea el GDPR de transferir los datos personales a otros países es acorde con la realidad, considerando que las tecnologías actuales permiten distribuir y procesar los datos en diversos servidores ubicados en distintos países.

Por último, el GDPR señala (artículo 83) que las autoridades de control son las encargadas de la aplicación efectiva de **multas o sanciones** en las que incurran los Controladores y Procesadores de datos personales por incumplimiento del reglamento. Las multas administrativas se imponen en función de las circunstancias de cada caso individual. Por ejemplo, el GDPR establece que por la infracción de los principios establecidos en el reglamento la multa será de hasta 20 millones de euros o el 4% del volumen de negocio total anual global del ejercicio anterior, optándose por el de mayor cuantía.

Hasta este punto hemos analizado el contenido de los artículos del GDPR que consideramos son de mayor interés para este estudio. Por lo tanto, y con el fin de cumplir con el segundo objetivo de este apartado, en los siguientes párrafos presentamos una comparativa entre la regulación europea y las regulaciones vigentes, o prontas a entrar en vigor, de algunos de los países de nuestro continente con el propósito de identificar aquellos aspectos en común y en los que aún requerimos trabajar para afrontar los retos de la economía digital.

Derivado de nuestra investigación y análisis de las regulaciones existentes en el continente americano, observamos que países como Canadá, México, Argentina, Uruguay, Chile, Brasil, Colombia y Perú, así como los lineamientos de la OCDE sobre privacidad (*Privacy Guidelines*),[27] contemplan en sus regulaciones nacionales normas y conceptos en común con el GDPR como lo son: el objeto y ámbito de aplicación de la regulación; las definiciones clave sobre el tema (e.g. definición de datos personales, tratamiento, Controlador y Procesador de datos, etc.); los principios reguladores (e.g. licitud, consentimiento, finalidad, proporcionalidad, etc.); la necesidad del consentimiento para el tratamiento de los datos personales (incluido el consentimiento para el tratamiento de datos de los menores de edad); la identificación de datos personales sensibles (e.g. información genética, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual, etc.); el derecho de acceso (contemplado como parte de los derechos ARCO que reconocen varios países); la seguridad del tratamiento con medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad apropiado; la notificación a la autoridad de control correspondiente en caso de una violación a la protección de los datos; y las sanciones o multas que aplican en caso de un incumplimiento por parte de los tratadores de datos.

Todos estos conceptos y normas están reflejados en las regulaciones de cada país y mencionan características muy similares al del reglamento europeo. Sin embargo, también identificamos las normas novedosas del GDPR que consideramos no están completamente reflejadas en las regulaciones de cada país, debido a que no cubren con claridad ni con la misma extensión todos los requisitos, derechos, obligaciones o condiciones que establece el reglamento europeo, o simplemente no cuentan con normas similares. Con el propósito de ilustrar lo anterior, en la figura 3 presentamos un esquema gráfico comparativo que nos permite visualizar las normas novedosas del GDPR y sus grados de similitud con las regulaciones de cada país de América.

Es importante resaltar que los Estados Unidos de América (EUA) no cuenta con una única regulación de aplicación general en todo su territorio sobre la protección de datos personales, tomando en cuenta que ha optado por implementar leyes para cada sector específico y regulaciones que trabajan en conjunto con la legislación nacional y de cada estado. De acuerdo con un estudio (Data protection laws of the world, 2018)[28] EUA tiene alrededor de 20 leyes nacionales específicas sobre privacidad y seguridad de datos para ciertos sectores, así como cientos de leyes entre sus 50 estados. Por tal motivo, y por la gran diversidad de leyes que existen en EUA, en este estudio no contemplamos su comparación con el GDPR.

[27] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[28] https://www.dlapiperdataprotection.com/

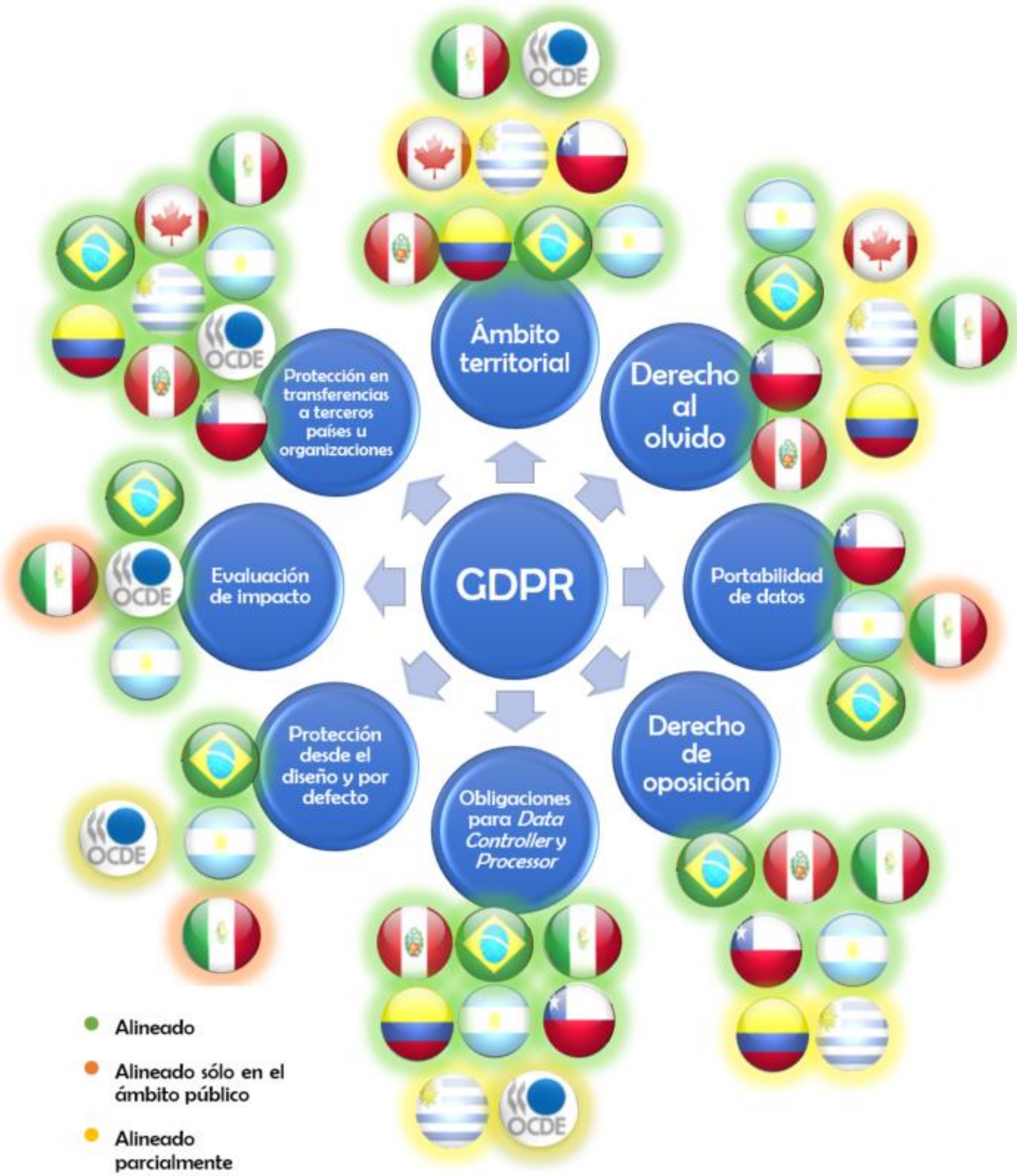

Figura 3. Esquema comparativo del GDPR con las regulaciones de algunos países de América

Para poder interpretar correctamente el esquema comparativo de la figura 3, es importante mencionar en primer lugar que una bandera sombreada en color verde significa que dicho país contempla en su regulación el objeto principal de la norma particular del GDPR. Por ejemplo, países como Chile, Argentina y Brasil sí mencionan claramente en sus regulaciones nacionales la "portabilidad de datos" como un derecho de las personas. Para el caso particular de México, en donde existen dos leyes respecto a la protección de datos personales, una para el ámbito privado (LFPDPPP) y otra para el ámbito público (LGPDPPSO) como lo veremos en el siguiente apartado, el color naranja significa que México contempla el objeto principal de la norma particular del GDPR únicamente para el ámbito público. Es decir, retomando el ejemplo anterior, significa que México también menciona claramente el derecho a la "portabilidad de datos" pero sólo para el ámbito público. Lo anterior no significa que en aquellas normas donde México aparece con su bandera sombreada en color verde sólo aplique para el ámbito privado. Por el contrario, significa que aplica tanto para el ámbito privado como para el público, con la única excepción de la norma sobre el "ámbito territorial" que sólo aplica para el ámbito privado.

Una bandera sombreada en color amarillo significa que dicho país se alinea parcialmente con la norma del GDPR, debido a que no abarca en su totalidad el objeto principal de dicha norma o simplemente no menciona con claridad los requisitos, derechos, obligaciones o condiciones como lo establece el reglamento europeo.

Finalmente, si la bandera de alguno de los países no aparece agrupada junto a una de las normas del GDPR significa que el país simplemente no contempla dicha norma en su regulación nacional.

Con la explicación anterior sobre el código de colores del esquema, podemos resaltar que países como Brasil y Argentina contemplan todas las normas novedosas que menciona el GDPR. Para el caso particular de México, observamos que también contempla todas las normas pero sólo para el ámbito público. Es decir, a diferencia de Brasil y Argentina, México no contempla el derecho de portabilidad de datos, la protección desde el diseño y por defecto ni la evaluación de impacto para el ámbito privado. Lo anterior significa que en México aún no existe una obligación nacional respecto a las anteriores normas definidas en el GDPR para todas aquellas empresas privadas que tratan datos personales en nuestro país (e.g. Facebook, Google, Microsoft, Uber, Amazon, operadores de telecomunicaciones, etc.). La portabilidad de datos, la evaluación de impacto y la protección desde el diseño y por defecto son normas clave que surgen del proceso de modernización de la regulación europea, para fortalecer la protección de los datos ante los retos de las nuevas tecnologías y servicios.

La portabilidad de datos originalmente surgió como un debate sobre la necesidad del usuario para transferir datos de un servicio a otro. Por ejemplo, para la transferencia de los datos generados en un correo electrónico o para la transferencia automática de una lista de contactos. Actualmente, la idea de la portabilidad de datos se ha comparado con los beneficios que ha generado la portabilidad numérica. Es decir, se considera como un mecanismo para prevenir la competencia desleal y hacer efectiva la protección de los datos personales, inclusive se percibe como un mecanismo que beneficiará la interoperabilidad entre los sistemas que ofrecen servicios *online* (Van der Auwermeulen, 2017).

De acuerdo con el mismo estudio anterior, la portabilidad de datos se define como el mecanismo que otorga a los usuarios *online* el derecho de controlar sus datos, mediante la posibilidad de transferir y compartir dichos datos de un servicio a otro para elegir el servicio que más les convenga. Por una parte, algunos argumentan que la portabilidad permitirá que los datos personales se transfieran sin obstáculos para fomentar la competencia, contrarrestando el *lock-in* del usuario en un servicio. Esto a su vez creará un ambiente más amigable y confiable para los usuarios al permitirles que transfieran sus datos de manera fácil y transparente. Por otra parte, están los que argumentan que la portabilidad incrementará la complejidad en el control y procesamiento de los datos personales. Asimismo, mencionan que abrirá la posibilidad para que empresas que se dedican al tratamiento de datos personales puedan adquirir más datos de los que realmente necesitan. Inclusive argumentan que la portabilidad podría repercutir en el fraude de identidad (Van der Auwermeulen, 2017). Independientemente de los argumentos que existen sobre las ventajas y desventajas de la portabilidad de datos, consideramos que México, a través de sus autoridades competentes, debe analizar la importancia de este derecho y definir una postura normativa para el ámbito privado que dé certeza jurídica a los millones de usuarios *online* que existen en México.

La protección desde el diseño y por defecto que deben adoptar los tratadores de datos personales consiste en implementar políticas y medidas internas tales como la seudonimización, la transparencia y la reducción al máximo del tratamiento de los datos personales.[29] El objetivo de esta obligación es garantizar la seguridad y el tratamiento lícito de los datos personales por parte de los tratadores. Asimismo, tiene la finalidad de alentar a los productores de dispositivos, sistemas y aplicaciones a tomar en cuenta el derecho a la protección de los datos personales desde el momento en el que desarrollan y diseñan estos productos, para asegurar que los Controladores y Procesadores puedan cumplir con sus obligaciones en materia de protección de datos.

La evaluación de impacto consiste en identificar anticipadamente el origen, naturaleza, particularidad y gravedad potencial del riesgo de un tratamiento de datos que desee implementar un Controlador, particularmente cuando dicho tratamiento represente un alto riesgo para los derechos y libertades de las personas (e.g. tratamiento de datos sensibles).[30] El objetivo de esta obligación es garantizar que los Controladores contarán con las medidas, garantías y mecanismos adecuados para mitigar cualquier riesgo, en términos de tecnología disponible y costes de aplicación, antes de realizar el tratamiento. Asimismo, esta obligación permite que la autoridad de control conozca con antelación la probabilidad del alto riesgo que representa el nuevo tratamiento y exigir que el Controlador cumpla en todo momento con el reglamento.

Como vemos, tanto la protección desde el diseño y por defecto como la evaluación de impacto son normas fundamentales para mitigar los riesgos en la protección de los datos personales. De ahí que también consideremos que en México sea indispensable adoptar normas similares para el ámbito privado, tomando en cuenta que en nuestro país existen alrededor de 71.3 millones de usuarios de Internet,[31] de los cuales

[29] GDPR
[30] GDPR
[31]http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-713-millones-de-usuarios-de-internet-y-174-millones-de-hogares-con-conexion-este-servicio

aproximadamente 83 de cada 100 navegan a través de un smartphone.[32] Es decir, la probabilidad de que los datos personales de la gran mayoría de los mexicanos sean tratados por parte de cualquiera de los servicios *online* existentes es alta, más si consideramos que el activo principal de estos servicios son precisamente los datos personales. Sobre la relevancia de estas tres normas clave, es importante mencionar que no nos pasa por desapercibido que los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos (RIPD), de la cual es parte México tal como lo mencionamos en el siguiente apartado, sí contempla estas normas de manera muy similar al GDPR. Sin embargo, y a pesar de que uno de los objetivos de la RIPD es crear un conjunto de principios y derechos que puedan adoptar y desarrollar en su legislación nacional todos los estados miembros, en la actualidad ningún instrumento jurídico mexicano menciona estas normas para su cumplimiento obligatorio en el ámbito privado. No obstante, creemos que en el futuro cercano México actualizará los instrumentos normativos vigentes en la materia para incluir estas normas, o simplemente fomentará como medida de autorregulación los estándares de la RIPD, considerando que el INAI ha tenido una participación muy activa en esta Red.

Del esquema comparativo de la figura 3 y de todo el análisis que hemos realizado hasta este punto, observamos que en términos generales México, al igual que otros países como Canadá, Uruguay, Chile, Colombia y Perú, requieren actualizar y complementar algunos conceptos y normas dentro de sus regulaciones si desean alinearse de mejor manera con el GDPR. Por ejemplo, algunos únicamente requieren incorporar tres normas adicionales como en el caso de México (sólo para el ámbito privado), Uruguay, Colombia y Perú respecto a las normas de portabilidad de datos, evaluación de impacto, y protección desde el diseño y por defecto. Otro, como lo es Chile, únicamente requiere abordar claramente dos normas adicionales: evaluación de impacto y protección desde el diseño y por defecto. Finalmente, Canadá requiere evaluar y analizar la manera en la que todas sus regulaciones nacionales y regionales se alinearán específicamente con lo establecido en el GDPR, considerando que cuenta con leyes robustas pero con diferentes matices en algunos casos específicos.

En general, tal como lo describimos con anterioridad, también observamos que la gran mayoría de los países de América ya han contemplado varias de las normas establecidas en el GDPR. Inclusive varios lo hicieron anticipadamente a la entrada en vigor del reglamento europeo. Esta armonización resulta fundamental para lograr una regulación común y moderna a nivel mundial que permita fomentar la comercialización global. De ahí que el GDPR haya incorporado, como parte de su modernización, una regulación extraterritorial sin importar el lugar donde se realice el tratamiento de los datos.

Marco jurídico mexicano en materia de protección de datos personales

En este apartado presentamos el marco jurídico existente en México sobre la protección de datos personales. Para tal fin, presentamos brevemente el desarrollo y evolución que ha tenido el marco jurídico en la materia de acuerdo con Peschard (2013). Asimismo, mencionamos los instrumentos jurídicos vigentes que regulan directamente la protección de datos personales. Finalmente destacamos algunas de las virtudes de estos instrumentos jurídicos y algunas estadísticas sobre protección de datos personales en México.

[32] INEGI, ENDUTIH 2017. La encuesta se realizó a personas de seis años o más en todo el país. Esto representa una población objetivo de 111.7 millones de personas.

El primer instrumento normativo en materia de protección de datos personales fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Ley Federal de Transparencia),[33] publicada el 11 de julio de 2002 en el Diario Oficial de la Federación (DOF). El objetivo de esta ley fue garantizar a toda persona el acceso a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal y cualquier otra entidad federal. Esta ley contemplaba un capítulo de protección de datos personales en el cual se establecían los principios generales que debían regir el tratamiento de los datos en posesión de entes públicos, tales como consentimiento, información, seguridad, calidad, entre otros, así como disposiciones generales que dan vida a los derechos de acceso y rectificación (Peschard, 2013).

Posterior a la Ley Federal de Transparencia, el 20 de julio de 2007 se aprobó el decreto por el cual se adicionó un segundo párrafo con siete fracciones al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en el que se reconoce expresamente el derecho de acceso a la información como un derecho fundamental, y particularmente las fracciones II y III del inciso A de dicho artículo en materia de protección de datos personales:

> *II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*
>
> *III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

Además, el 30 de abril de 2009 se publicó en el DOF el decreto para reformar el artículo 73 de la CPEUM con el fin de dotar de facultades al Congreso Federal para legislar en materia de protección de datos en posesión de los particulares.

Adicionalmente, el 1 de junio de 2009 fue aprobada la reforma al artículo 16 de la CPEUM que menciona lo siguiente:

> *Toda persona tiene derecho a la protección de sus datos personales, el acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

Paralelamente, México participa en diversos foros y pertenece a distintos organismos internacionales sobre protección de datos personales, de los cuales ha contraído obligaciones y compromisos encaminados a garantizar un marco legislativo adecuado, y a su vez, impedir la creación de barreras que frenen la libre circulación de los datos en el mundo. Algunos de estos foros y organismos internacionales son (Peschard, 2013):

- La Organización para la Cooperación y el Desarrollo Económicos (OCDE);

[33] http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf

- La Organización de las Naciones Unidas (ONU);
- El Foro de Cooperación Económica de Asia Pacífico (APEC);
- El Tratado de Libre Comercio con la Unión Europea;
- La Alianza para la Seguridad y la Prosperidad de América del Norte;
- La Red Iberoamericana de Protección de Datos (RIPD);
- El Comité Trilateral para el Flujo Transfronterizo de Información.

De esta manera en México existen dos leyes sobre el derecho de protección de datos personales según su ámbito de aplicación.[34] Por una parte, en el ámbito privado a nivel federal existe la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) publicada en el DOF el 5 de julio de 2010. El objeto de esta ley es la protección de los datos personales en posesión de los particulares (personas físicas y morales de carácter privado), con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. La LFPDPPP cuenta con un Reglamento y los siguientes instrumentos normativos:

- Los Lineamientos de Aviso de Privacidad;
- Los Parámetros de autorregulación en materia de protección de datos personales;
- Las Reglas de operación del registro de esquemas de autorregulación vinculante;
- Los Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del INAI;
- Los Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet del INAI, para dar a conocer avisos de privacidad a través de medidas compensatorias.

Es importante resaltar que la LFPDPPP en su artículo 38 menciona que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es la institución encargada de “difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento”.

Asimismo, es de destacar que la LFPDPPP y su Reglamento constituyen el marco general que establece las reglas, requisitos, condiciones y obligaciones mínimas para garantizar un adecuado tratamiento de la información personal por parte de los particulares, sin perjuicio de lo que establezca la normativa sectorial o específica aplicable al tratamiento de datos personales por parte de los particulares.

En la comparación que hicimos en el aparatado anterior, entre el GDPR y las regulaciones de algunos países de América, mencionamos que México, junto con otros países, contempla en el contenido de sus leyes el objeto de varias normas clave del GDPR (e.g. principios, datos sensibles, consentimiento, derecho de acceso, derecho de olvido, etc.). No obstante, en este apartado consideramos importante resaltar algunos de los aspectos más relevantes de la LFPDPPP. Por ejemplo, algunas definiciones importantes que marca

[34] http://inicio.inai.org.mx/Guias/Guia%20Titulares-01_PDF.pdf

esta ley y su reglamento son: aviso de privacidad; base de datos; bloqueo; disociación; entorno digital; Responsable (Controlador); Encargado (Procesador); supresión, entre otros. Al respecto, es de destacar la definición de disociación como el procedimiento mediante el cual los datos personales no pueden asociarse a un titular ni permitir su identificación. Esta definición es importante dado que permite que nuevas tecnologías como el *Big Data* puedan realizar procesamientos y análisis de grandes volúmenes de datos siempre y cuando sean datos disociados, seudonimizados o anónimos.

Otro aspecto a destacar de la LFPDPPP es el reconocimiento de los derechos ARCO, los cuales permiten la actualización, rectificación, cancelación u oposición de los usuarios respecto a los datos personales que les conciernen. El derecho al olvido que establece el GDPR está de alguna forma contemplado en el derecho de cancelación, que puede significar la eliminación total de los datos. También es de resaltar que el reglamento de esta ley menciona el ámbito territorial de aplicación de manera similar al GDPR; es decir, menciona que la ley se aplica sin importar el lugar donde se realice el procesamiento de los datos personales siempre y cuando resulte aplicable la legislación mexicana.

Por otra parte, en el ámbito público existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) publicada en el DOF el 26 de enero de 2017. Uno de los objetivos de esta ley es "proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento". De manera adicional, cada entidad federativa del país debe contar con una ley específica que detalle las disposiciones que regularán el tratamiento de datos personales en el sector público de su propio ámbito territorial y que esté armonizada con la LGPDPPSO.

Es importante resaltar que la LGPDPPSO, además de contemplar varios de los conceptos, condiciones, derechos y obligaciones de la LFPDPPP, también contempla los aspectos novedosos establecidos en el GDPR como la portabilidad de datos, la evaluación de impacto y la protección desde el diseño y por defecto, debido a la innovación tecnológica de los últimos años tal como lo mencionamos en el apartado anterior. Asimismo, define las facultades y responsabilidades de los Responsables (Controladores) y de los Encargados (Procesadores) de manera más precisa que la LFPDPPP. Esta ley representa el marco jurídico más reciente respecto a la protección de datos personales en México.

Como vemos, el derecho de protección de datos personales en nuestro país es un derecho reconocido a nivel constitucional y el marco jurídico está principalmente constituido por dos leyes específicas en la materia. Además, este marco reconoce el establecimiento de normatividad sectorial o específica (i.e. tratamiento de datos fiscales, financieros o de salud). También reconoce la implementación de esquemas de autorregulación vinculante en el ámbito privado que permiten incluir principios, normas y procedimientos para adecuar y armonizar las disposiciones previstas en la LFPDPPP a la realidad de los sectores específicos. De esta manera existen Normas Oficiales Mexicanas (NOM) y Normas Mexicanas (NMX) que regulan aspectos específicos en la materia. Por ejemplo, la NOM-024-SSA3-2010 establece las funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico, y la NMX-I-27018-NYCE-2016 establece los objetivos de control y medidas de protección de los datos personales para ambientes públicos de cómputo en la nube. Asimismo, en el ámbito internacional, México recientemente se adhirió al Convenio 108 del Consejo de Europa y forma parte de la Red Iberoamericana de Protección de Datos (RIPD) como lo mencionamos con anterioridad.

De lo anterior podemos observar que el marco jurídico mexicano es sólido, al menos respecto al contenido de los instrumentos jurídicos vigentes sobre la protección de datos personales. Entonces, ¿cuál es el mayor problema que existe en México para garantizar y hacer efectiva la protección de los datos personales? Con el fin de responder al anterior cuestionamiento, en las siguientes líneas presentamos algunas estadísticas.

De acuerdo con la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016,[35] la cual se enfocó principalmente a recabar información sobre los conocimientos, actitudes y prácticas de la población respecto al derecho de acceso a la información y protección de datos personales, estimó que a nivel nacional el 95.9% de la población de 18 años y más proporcionó sus datos personales a alguna organización. Asimismo, estimó que la gran mayoría de la población manifestó preocupación por el uso indebido de sus datos personales proporcionados a instituciones públicas o empresas como se observa en la figura 4.

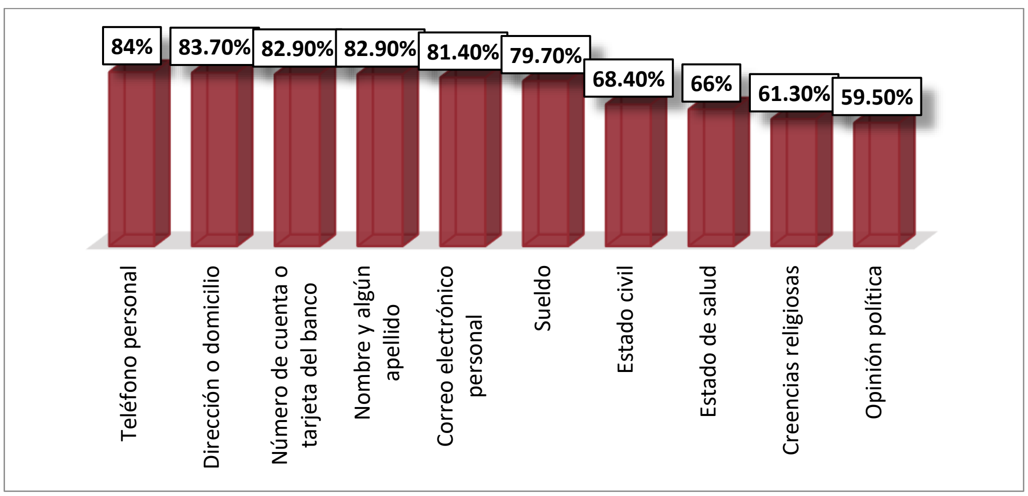

Figura 4. Porcentaje de población preocupada por el mal uso de sus datos personales

Por otra parte, la misma encuesta estimó que sólo el 55.8% de la población nacional tiene conocimiento o ha escuchado sobre la existencia de una ley encargada de garantizar la protección de los datos personales. Respecto a la obligación de proporcionar un aviso de privacidad previo al tratamiento de datos personales, la encuesta estimó que a sólo el 32.7% de la población nacional le dieron a conocer un aviso de privacidad tal como se observa en la figura 5.

[35] http://www3.inegi.org.mx/rnm/index.php/catalog/223

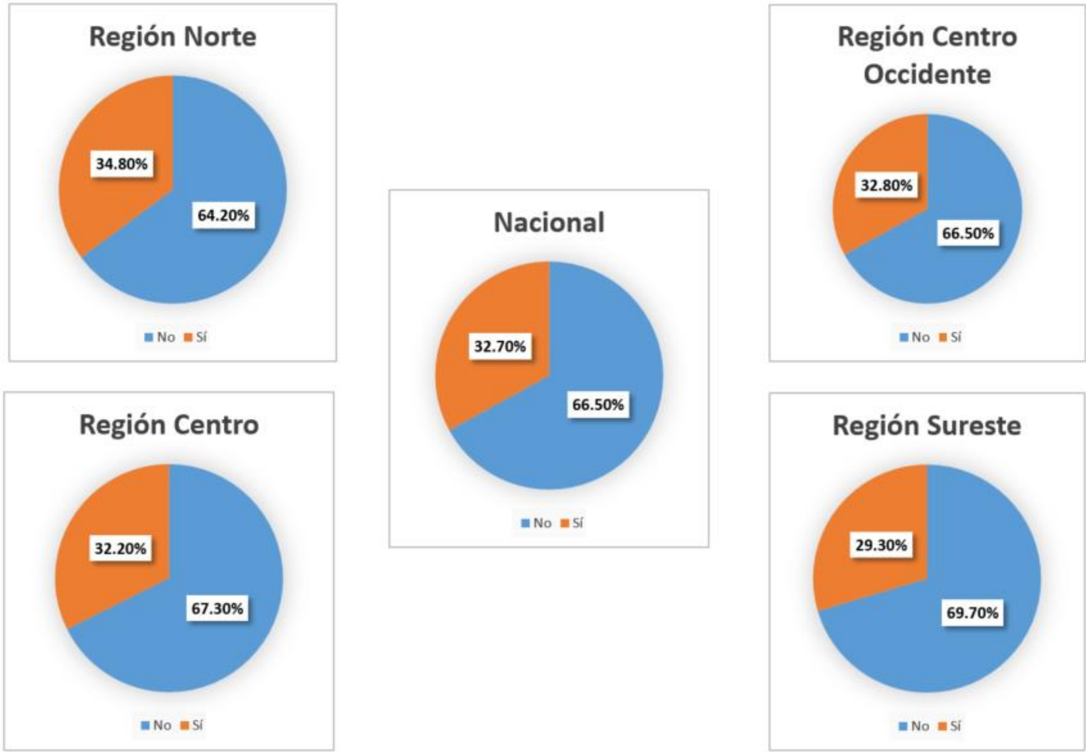

Figura 5. Recepción de un aviso de privacidad

Sin embargo, la encuesta también estimó que sólo el 65.1% de la población nacional que recibió un aviso de privacidad leyó dicho aviso. Finalmente, la encuesta estimó que sólo el 10.1% de la población a nivel nacional presentó ante el INAI una queja por uso indebido de sus datos personales.

De las estadísticas anteriores podemos observar que prácticamente toda la población ha proporcionado en alguna ocasión sus datos personales a alguna organización. Asimismo, la gran mayoría se preocupa por el mal trato que pudieran recibir sus datos. A pesar de ello, también observamos que sólo el 55.8% de la población tiene conocimiento sobre la existencia de una ley de protección de datos personales, y muy pocos presentan alguna queja por el uso indebido de sus datos. También observamos que sólo el 32.7% de la población recibió un aviso de privacidad cuando le solicitaron sus datos. Es decir, más allá de los alcances y fortalezas de nuestras leyes respecto a la protección de datos personales, vemos que sólo una parte de la población tiene conocimiento de su existencia, a pesar de la inminente preocupación que existe entre las personas sobre el uso o explotación de sus datos. Por otro lado, pareciera que el sector privado no está realizando los esfuerzos necesarios para informar y garantizar la protección de los datos personales, pues sólo la tercera parte de la población recibió un aviso de privacidad (generalmente escrito en lenguaje no comprensible) de acuerdo con la ENAID 2016.

En general, creemos que existe un desconocimiento del tema entre la población y que se carece de mecanismos apropiados para la correcta aplicación y cumplimiento de las leyes. Sin una adecuada concientización de las personas y sin los procedimientos correctos para hacer efectivas las obligaciones de los sujetos responsables es difícil garantizar la protección de los datos personales. Creemos que el esfuerzo por mejorar esta situación debe realizarse por parte tanto de las autoridades como de las personas.

Finalmente, es de suma importancia para este estudio rescatar, por una parte, lo que señala el artículo 77 del Reglamento de la LFPDPPP en relación a la coordinación que el INAI puede llevar a cabo con otras autoridades para la emisión de regulación secundaria:

> *Artículo 77. Cuando la dependencia competente, atendiendo a las necesidades que advierta sobre el sector que regule, determine la necesidad de normar el tratamiento de datos personales en posesión de los particulares podrá, en el ámbito de sus competencias, emitir o modificar regulación específica, en coadyuvancia con el Instituto.*
>
> *Asimismo, cuando el Instituto derivado del ejercicio de sus atribuciones advierta la necesidad de emitir o modificar regulación específica para normar el tratamiento de datos personales en un sector o actividad determinada, podrá proponer a la dependencia competente la elaboración de un anteproyecto.*

El artículo anterior es de gran relevancia para el Instituto Federal de Telecomunicaciones (IFT), considerando que significa una ventana de oportunidad para coadyuvar con el INAI en la emisión de regulación específica, en caso de que así lo determinaran ambas partes, sobre la protección de los datos personales en el sector de telecomunicaciones. Al respecto, y con toda razón, cualquier persona podría argumentar que el artículo 77 del Reglamento de la LFPDPPP se refiere únicamente a la coadyuvancia entre el INAI y las dependencias de la administración pública federal (i.e. las Secretarias de Estado y la Consejería Jurídica del Ejecutivo Federal) de acuerdo con la Ley Orgánica de la Administración Pública Federal.[36] Es decir, el artículo no hace mención de los organismos autónomos como los es el IFT; sin embargo, el INAI tiene la facultad de suscribir convenios de colaboración[37] con otras autoridades entre las que se encuentra el IFT. Además, tratándose del sector de telecomunicaciones, es indudable que el IFT tiene todas las facultades para promover y supervisar cualquier regulación que impacte al sector.

De esta manera, el IFT tendría la posibilidad de trabajar en conjunto con el INAI en la realización de una posible regulación respecto a la protección de datos personales en el sector. Por ejemplo, podría crearse regulación específica respecto de los datos personales que recolectan y resguardan los operadores de telecomunicaciones, o sobre el tratamiento que recibieran los datos debido al uso de tecnologías emergentes (e.g. IoT, *Big Data*, 5G, etc.) por parte de los operadores. Al respecto, en el siguiente apartado presentamos el posible impacto que tendrá el cumplimiento del GDPR para los operadores de telecomunicaciones, particularmente en la provisión de servicios que involucren tecnologías de nueva generación.

[36] http://www.diputados.gob.mx/LeyesBiblio/pdf/153_150618.pdf
[37] http://inicio.ifai.org.mx/SitePages/Convenios.aspx

Por otra parte, también es importante mencionar y analizar el alcance de la fracción III del artículo 145, respecto a la neutralidad de las redes, de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) que a la letra dice lo siguiente:[38]

> ***Artículo 145.*** *Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:*
>
> *I a II* [...].
>
> ***III. Privacidad****. Deberán preservar la privacidad de los usuarios y la seguridad de la red;*
>
> *IV a VII* [...].

De conformidad con lo que hemos expresado en este estudio, y con el artículo 1 de la LFPDPPP,[39] la protección de datos personales está íntimamente relacionada con el derecho de privacidad de las personas. Desde ese punto de vista, podríamos decir que la protección de los datos personales es un elemento clave para preservar la privacidad de los usuarios; por lo tanto, por extensión, los prestadores del servicio de acceso a Internet también deberían proteger los datos personales de sus usuarios. Sin embargo, consideramos que la interpretación del alcance de esta fracción requiere de un análisis jurídico a mayor detalle que está fuera del objetivo de este estudio. No obstante, consideramos que este artículo también puede representar otra ventana de oportunidad para que el IFT pueda emitir, en caso de así determinarlo, regulación relacionada con la protección de los datos personales en el sector de telecomunicaciones.

Impacto en el sector de Telecomunicaciones

Los operadores de telecomunicaciones son y seguirán siendo (al menos para el futuro cercano) los principales facilitadores de conectividad para la provisión de diversos servicios, aplicaciones y contenidos *online* del ecosistema digital, sin importar quién sea el proveedor original de dichos servicios (e.g. OTT). Es decir, el mayor volumen de los datos que se transmita entre distintas partes del mundo, debido al tráfico generado por usuarios y proveedores, viajará a través de las redes de los operadores. Por tal motivo, los operadores juegan un papel importante respecto a la protección de los datos personales que viajen a través de sus redes, más si consideramos que los datos representan el activo principal para la creación de nuevos modelos de monetización. Un descuido en la protección de los datos personales de los usuarios puede desatar una pérdida de confianza, una degradación en la imagen del operador y el riesgo de una penalización por parte de la autoridad de control. De ahí que los operadores tengan la necesidad de analizar y abordar a detalle los requisitos, condiciones y obligaciones que establecen las regulaciones sobre la protección de datos personales de cada uno de los países donde tienen presencia. Tal como lo hemos afirmado en apartados anteriores, el GDPR es actualmente el reglamento internacional más actualizado y el referente para este estudio; por lo tanto, en los siguientes párrafos describimos algunos de los cambios

[38] http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

[39] **Artículo 1.-** La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

y estrategias que consideramos tendrán que adoptar los operadores para cumplir con el reglamento europeo, de conformidad con algunos estudios (Tikkinen-Piri et al., 2018):[40,41]

La regulación europea impacta a los operadores en cuatro dimensiones generales:

1. Legal

   Los operadores deben traducir los requerimientos y obligaciones de la regulación en políticas internas y en mecanismos de comunicación externos que les permitan cumplir a cabalidad con el reglamento, particularmente respecto al consentimiento explícito que deben obtener de sus usuarios (especialmente el de menores de edad) y sobre la creación de un marco general de protección de datos;

2. Tecnología

   Los operadores deben implementar la tecnología necesaria que les permita asegurar la protección y seguridad de los datos personales. Particularmente para garantizar: la portabilidad; la minimización; la gestión de acceso; la rectificación; el derecho al olvido; la identificación de una violación a la protección y seguridad de los datos; la protección desde el diseño y por defecto (por ejemplo, encriptación, seudonimización, anonimización, etc.); y para el registro del tratamiento de los datos;

3. Modelo de negocio

   Los operadores deben realizar una evaluación de impacto en su modelo de negocio que responda a las siguientes preguntas: ¿Qué tratamientos están permitidos? ¿Qué tratamientos son los más propensos de violar la regulación? ¿Cómo afecta la contratación/operación con terceros (es decir, Procesadores)? ¿De qué manera se verán afectados los ingresos?

4. Organización

   Los operadores deben asignar un área exclusiva para la protección de datos personales. Asimismo, deben nombrar a un delegado o responsable para verificar que cumplen con: la protección desde el diseño y por defecto; las evaluaciones de impacto; y la representatividad ante la autoridad de control.

Como vemos, el GDPR tiene un impacto directo en la manera con la que actualmente los operadores recolectan, resguardan y procesan los datos personales de sus usuarios. Asimismo, consideramos que el reglamento europeo significa un reto para el desarrollo de las tecnologías emergentes de las cuales los operadores también son parte. Por ejemplo, sabemos que en principio el *Big Data* consiste en reutilizar los datos recolectados para descubrir patrones, adquirir conocimiento u obtener un valor adicional a través del procesamiento y análisis masivo de dichos datos; sin embargo, el principio de limitación de la finalidad del GDPR menciona que los datos no serán tratados ulteriormente de manera incompatible con los fines originales, por lo que esto representa un reto para los operadores que deseen poner en práctica sus

[40] http://www.terminsstarttelekom.se/upload/termin/pdf/pres461.pdf
[41] https://www.tcs.com/content/dam/tcs/pdf/Industries/communication-media-and-technology/Abstract/Ensuring-GDPR.pdf

tecnologías de *Big Data* y ofrecer nuevos servicios. Al respecto, podemos identificar algunos desafíos específicos a los que probablemente se enfrentaran los operadores con el *Big Data*:[42]

- Evitar mostrar información sensible de las personas como resultado del análisis de varios datos, sin importar que dichos datos no hayan sido sensibles originalmente;
- Evitar crear estereotipos digitales que den lugar a la discriminación, debido al resultado del análisis estadístico de los datos personales a los que únicamente tienen acceso;
- Evitar generar perfiles digitales que relacionen inequívocamente a un individuo.

Algunas recomendaciones para evitar un incumplimiento del GDPR por parte de los operadores cuando deseen utilizar tecnologías de *Big Data* son:[43]

- Siempre obtener el consentimiento de las personas para el procesamiento y análisis de sus datos personales;
- Usar datos anónimos para evitar riesgos en la privacidad de sus usuarios. Si deciden utilizar datos seudonimizados es importante tener en cuenta que éstos siguen siendo datos personales y por lo tanto requieren protección;
- Cuando tengan interés en usar los datos personales para otros propósitos diferentes a los originales, es importante evaluar la compatibilidad del nuevo propósito con el original sobre una base de caso por caso, beneficiando en todo momento la protección de la privacidad de las personas;
- Utilizar tecnologías de *Big Data* que cumplan con la protección desde el diseño y por defecto de los datos personales;
- Realizar una evaluación de impacto en el uso tecnologías de *Big Data* respecto a la protección de datos personales.

Otra de las tecnologías emergentes en la que se vislumbran retos para los operadores respecto a la protección de datos personales es en la nueva generación de redes inalámbricas 5G. Las redes 5G se caracterizarán principalmente por la automatización y virtualización de las redes. Es decir, las tecnologías que en conjunto darán origen a los nuevos atributos de las redes 5G (más velocidad y banda ancha, conectividad masiva para dispositivos o cosas y conectividad con alto nivel de confianza y baja latencia) también permitirán automatizar y hacer más eficiente el procesamiento de los datos que se recolecten. Algunas de estas tecnologías que serán cruciales para el desarrollo de las redes 5G son: Inteligencia Artificial (AI por sus siglas en inglés), *Edge Computing, Machine Learning*, *Big Data*, entre otras. La adopción creciente de estas tecnologías en redes 5G genera muchas expectativas, pero también muchas inquietudes relacionadas con los efectos involuntarios que pudieran ocurrir debido a la autonomía de estos sistemas, particularmente en el tratamiento automatizado de los datos personales. Al respecto, existen algunas opiniones que mencionan ciertas recomendaciones en la operación de las redes 5G para cumplir con el GDPR:[44]

- Contar con sistemas automatizados para la gestión de la seguridad y privacidad en tiempo casi real;

[42] https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/
[43] https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/
[44] https://www.ericsson.com/research-blog/5g-and-the-eu-general-data-protection-regulation/

- Implementar procedimientos automatizados para el cumplimiento de los derechos de los usuarios como: la verificación del consentimiento; la portabilidad y eliminación de los datos; entre otras acciones;
- Adoptar estándares y protocolos que cumplan con la protección desde el diseño y por defecto. Asimismo, utilizar dispositivos y equipos de los *vendors* que cumplan con dicha protección;
- Implementar medidas de protección adecuadas que permitan garantizar el cifrado e integridad de los datos personales almacenados, así como su anonimización y seudonimización cuando sea necesario;
- Separar los datos almacenados de acuerdo con los propósitos legales que deban cumplir, con el fin de evitar que dichos datos sean accidentalmente procesados para otros propósitos.

La protección de datos personales también resulta de gran relevancia para el ecosistema de IoT, considerando que en la actualidad los dispositivos de IoT cuentan con múltiples sensores y geolocalización, inclusive cámaras de video y micrófonos, que permiten adquirir una gran diversidad de datos del ambiente físico que les rodea para transmitirlos por Internet (Alkhalil & Ramadan, 2017). La capacidad de estos dispositivos puede emplearse, por ejemplo, para crear perfiles digitales de las personas con los datos que se adquieren y comparten cuando monitorean sus actividades. La falta de un control adecuado en la seguridad de dichos datos puede afectar la privacidad y seguridad de las personas. La creación de perfiles digitales pudiera representar el escenario menos riesgoso para la privacidad de las personas; sin embargo, un escenario de mayor riesgo pudiera ocurrir si los datos, videos, sonidos o imágenes de las actividades que realizan las personas no estuvieran protegidos y fueran usados de manera ilícita como lo mencionamos en uno de los apartados anteriores. De ahí que sea necesaria una regulación apropiada que permita tanto el desarrollo de los diversos sistemas de IoT, como la protección adecuada de la privacidad de las personas con el fin de generar confianza entre los usuarios.

Respecto al desarrollo apropiado de loT hemos identificado que varios estudios han descrito los requerimientos elementales para su seguridad, algunos de los cuales son: la implementación de procedimientos de autenticación para la comunicación entre dispositivos; la aplicación de mecanismos de encriptación que garanticen la confidencialidad de los datos que se transmiten; fortalecer la capacidad de resistencia a ataques cibernéticos; y adoptar un control de acceso a la información, entre otros (Khan & Salah, 2018; Alkhalil & Ramadan, 2017).[45]

En relación con la protección de la privacidad en sistemas de IoT existe como referencia una propuesta específica sobre las comunicaciones electrónicas por parte de la UE conocida como *ePrivacy Regulation* (la cual sustituirá a la *ePrivacy Directive* de 2002, incluida su modificación del 2009). Esta propuesta de regulación se encuentra actualmente en revisión y contempla aspectos relevantes relacionados con el ecosistema de IoT, particularmente un análisis sobre las comunicaciones máquina-a-máquina (M2M). Al respecto, la propuesta menciona que existe el riesgo de crear una carga excesiva para los proveedores de servicios M2M en caso de que tuvieran que cumplir a cabalidad, por ejemplo, con el principio de licitud del GDPR, considerando que requerirían del consentimiento de cada uno de los usuarios que recibieran

[45] https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/

comunicaciones, o algún servicio, a través de dispositivos de M2M. Por tal motivo, la propuesta contempla la posibilidad de permitir el procesamiento de las comunicaciones M2M para los casos en los que no se procesen datos personales o cuando se requiera la metadata de las comunicaciones, tomando en cuenta que son comunicaciones que generalmente se realizan con una intervención humana limitada y en algunos casos ni siquiera existe dicha intervención. Sobre lo anterior, independientemente de la determinación de la UE sobre una regulación para M2M, nosotros creemos que sería conveniente dejar exentas del cumplimiento de dicha regulación a las comunicaciones de M2M que se realicen exclusivamente entre máquinas, que no procesen datos personales y que no tengan un impacto sobre la privacidad de las personas. Sin embargo, también creemos que el reto para este escenario será justamente la identificación precisa de las categorías de comunicaciones M2M que no procesen datos personales, tomando en cuenta las posibilidades actuales que brindan diversas tecnologías para asociar los datos recolectados de los diversos sensores con las personas.

La aplicación y el cumplimiento de una regulación general para todo el ecosistema de IoT se vislumbra complejo debido a la naturaleza de operación de los sistemas de IoT. Por una parte, los dispositivos de IoT suelen operar, por diseño, de manera discreta y sin el consentimiento de las personas, considerando que son dispositivos que comúnmente no tienen una interfaz gráfica para interactuar directamente con las personas como los *smartphones* o las *laptops*. Por otra parte, el proceso de adquisición, transmisión, almacenamiento, procesamiento y distribución de los datos involucra a múltiples actores, lo que supondría un análisis complejo para la identificación precisa de aquellos que fungen como Controladores o Procesadores de datos para el debido cumplimiento de sus obligaciones de acuerdo con el GDPR. Además, si consideramos que el procesamiento y análisis de los datos de IoT se realiza en la nube, el cumplimiento de una regulación como la europea supondría emplear una gran cantidad de tiempo. Por ejemplo, imaginemos un caso de uso de IoT en el que existe un timbre inteligente habilitado con video en una casa. El fabricante del timbre fácilmente podría adquirir el consentimiento del propietario para procesar imágenes y video de la persona en el momento que le vende el producto; sin embargo, el proceso no resulta igual de rápido y sencillo para conocer la voluntad de los visitantes respecto al procesamiento de sus datos en la nube cuando hacen uso de dicho timbre. Otro caso de uso son las redes de cámaras en las ciudades inteligentes. Si una persona hace uso de su derecho al olvido como lo establece el GDPR, los operadores tendrían que identificar todo el histórico de aquellas imágenes que estuvieran relacionadas con dicha persona para poder eliminarlas. Esto resultaría impráctico por el tiempo y dificultad que representa el proceso, además podría repercutir en implicaciones negativas en la seguridad de las ciudades.

La aplicación del GDPR para casos como los anteriores no resulta claro y algunos podrían argumentar que ciertos servicios de IoT podrían estar exentos del consentimiento de las personas; otros podrían argumentar que la protección desde el diseño y por defecto que determina el GDPR podría ayudar a evitar esfuerzos adicionales para el cumplimiento con dicho reglamento. Sin embargo, es precisamente la delimitación y efectividad en la aplicación de una regulación para IoT lo que resulta ser el mayor reto para los reguladores y las autoridades, considerando que uno de sus objetivos principales es permitir la innovación y el desarrollo adecuado del ecosistema digital sin afectar los derechos fundamentales de las personas. No obstante, a pesar de la complejidad que puede resultar la aplicación efectiva de una regulación para IoT sobre la protección de datos personales, la propia tecnología pudiera ser la herramienta que ayudaría a mitigar los riesgos de seguridad y privacidad en los dispositivos de IoT. Por ejemplo, en la actualidad existen diversos estudios sobre tecnologías de bases de datos y de *data mining* que están tratando de crear procesos que permitan detectar con precisión el origen, propagación y difusión de los datos a través de las redes (Alkhalil & Ramadan, 2017). Es decir, están tratando de crear procesos que permitan mapear el flujo completo de los datos para los casos en los que existió una violación a la seguridad de un sistema. Estos procesos se pueden adaptar y aplicar a los sistemas de IoT para evitar faltas a la privacidad de las personas.

Por otra parte, el gobierno británico recientemente publicó un código de prácticas de seguridad para sistemas de IoT.[46] El cumplimiento de este código es voluntario y está conformado por 13 recomendaciones para asegurar que todos los dispositivos y servicios de IoT sean seguros desde el diseño. Es decir, este código permite que los fabricantes de dispositivos, los desarrolladores de aplicaciones y los proveedores de servicios de IoT implementen soluciones de seguridad desde el diseño en sus productos para cumplir con esta norma particular del GDPR, así como con la regulación del propio UK. Las recomendaciones son las siguientes:

- **Sin contraseñas por *default***: todas las contraseñas de los dispositivos de IoT deben ser únicas, sin restablecerlas a valores predeterminados de fábrica;
- **Implementar una política de divulgación de vulnerabilidad:** todos los proveedores de productos y servicios de IoT deben monitorear, identificar y rectificar las vulnerabilidades de sus productos;
- **Mantener el software actualizado:** el software de todos los dispositivos de IoT debe estar actualizado;
- **Almacenar de menara segura los datos sensibles y de acceso:** cualquier dato de acceso debe estar almacenado de manera segura dentro de los servicios y en los dispositivos;
- **Comunicar de manera segura:** los datos de seguridad, incluidos los de gestión y control, deben estar encriptados durante su transmisión;
- **Minimizar la exposición a ataques:** bajo el principio del menor privilegio, todos los productos y servicios de IoT deben deshabilitar los puertos que no se utilicen, los servicios no deben estar disponibles sino se solicitan, y el hardware no debe admitir accesos innecesarios;
- **Asegurar la integridad del software:** los dispositivos de IoT deben verificarse a través de mecanismos de arranque seguros. Cualquier cambio realizado sin autorización debe ser reportado al administrador y los dispositivos no deben conectarse a otras redes que no sean las necesarias;
- **Asegurar que los datos personales estén protegidos:** los fabricantes, desarrolladores de aplicaciones y proveedores de servicios de IoT deben cumplir con las obligaciones relacionadas con la protección de datos personales (es decir, GDPR y *UK Data Protection Act* 2018). Los usuarios deben recibir asistencia y contar con los medios para asegurar que los dispositivos operen consistentemente con lo especificado, y su privacidad deberá estar protegida mediante la configuración apropiada;

[46]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

- **Sistemas resistentes:** los dispositivos y servicios deben ser resistentes a pérdidas de conectividad y cortes de energía eléctrica cuando sea técnicamente posible. La reconexión de los dispositivos con las redes debe ser ordenada para evitar reconexiones masivas;
- **Monitorear sistemas de telemetría:** si los servicios y dispositivos de IoT recolectan datos de telemetría (incluidos los logs de registro), como datos de mediciones y uso, deben ser monitoreados para identificar anomalías de seguridad;
- **Facilitar la eliminación de los datos personales:** los servicios y dispositivos de IoT deben configurarse de tal manera que los datos personales puedan ser borrados cuando exista una transferencia de propiedad, el usuario así lo desee o cuando quiera deshacerse del dispositivo;
- **Facilitar la instalación y el mantenimiento de los dispositivos:** la instalación y mantenimiento de los dispositivos de IoT deben contemplar las mínimas instrucciones posibles, así como adoptar las mejores prácticas de seguridad;
- **Validación de datos:** los datos de acceso ingresados a través de interfaces de usuario y transferidos por medio de las APIs, o transferidos entre redes, de los servicios y dispositivos IoT deben ser validados.

Tal como lo mencionamos en el anterior apartado, el desarrollo y aplicación de regulación específica para la protección de datos personales en el sector de telecomunicaciones es de suma importancia para el IFT. Por lo anterior, una de nuestras recomendaciones para el IFT sería elaborar un proyecto sobre prácticas de seguridad para el ecosistema de IoT, muy similar al del Reino Unido y al de otros países que sean adecuados para nuestro país, tomando en cuenta que actualmente existen poco más de 8 millones de conexiones de IoT en bandas móviles concesionadas en nuestro país (las cuales representan el 10% del total de suscriptores a servicios móviles).[47]

Asimismo, consideramos que tanto el cumplimiento de la norma sobre evaluación de impacto como la de protección desde el diseño y por defecto del GDPR son clave para el sector de telecomunicaciones de nuestro país. Máxime que no existe una regulación al respecto para el ámbito privado en México. De esta manera, otra de nuestras recomendaciones para el IFT sería elaborar un código de buenas prácticas, o recomendaciones, de seguridad exclusivas para el sector respecto a la protección de los datos personales que recolectan, resguardan y procesan los operadores, mediante el uso e implementación de dispositivos, sistemas y redes seguros desde el diseño. Es decir, proponer un código de seguridad que fomentara el uso de medidas técnicas y organizativas apropiadas para el sector, acorde con las nuevas tecnologías y exigencias del ecosistema.

Respecto a la norma sobre la evaluación de impacto, consideramos que es de gran importancia para el sector debido a que está muy relacionada con el uso de nuevas tecnologías para el procesamiento de los datos. En particular, creemos que el IFT puede promover la realización de evaluaciones de impacto entre los operadores con el fin de evitar que nuevos servicios pongan en riesgo la privacidad de las personas.

[47] GSMA Intelligence

Conclusiones

Este estudio nos ha permitido comprender que los datos personales representan el activo fundamental o la materia prima de la economía digital. Por una parte, hemos entendido que el valor monetario de los datos personales aislados es mucho menor, inclusive podríamos decir que insignificante, respecto al valor comercial que pueden alcanzar los perfiles digitales de las personas para dicha economía. La diferencia radica en la información que se pueda obtener o descubrir del procesamiento de los múltiples datos personales de una o varias personas. Por otra parte, sabemos que los datos personales, a diferencia de otros recursos, son fácilmente replicables y transferibles gracias a las facilidades de comunicación que actualmente ofrecen las tecnologías digitales. Sin embargo, también hemos entendido que existe un costo por la adquisición, actualización, almacenamiento y procesamiento de los datos para todos aquellos que deseen obtener un beneficio o lucro, más si consideramos el actual crecimiento exponencial de los datos en el ecosistema digital.

Está claro entonces que el procesamiento de los datos personales genera información valiosa para las empresas u organizaciones que desarrollan y venden servicios o productos como parte de la economía digital. Es decir, en tanto que los datos personales representan un insumo primordial para crear potenciales ingresos, esto los convierte en elementos vulnerables a diversos tratamientos con o sin el consentimiento de las personas.

De esta manera, hemos observado que el valor comercial de los datos personales genera dos riesgos principales que las autoridades y reguladores no deben perder de vista: 1) efectos en la competencia y 2) privacidad de las personas. En la actualidad múltiples sectores productivos del mundo ya son parte de la economía digital, inclusive hay quienes se atreven a decir que la economía digital es la economía actual. De ahí que la protección de los datos personales tenga un impacto transversal en múltiples sectores y que diversas autoridades tengan la necesidad de coordinar sus esfuerzos para abordar el tema.

Respecto a los posibles efectos en la competencia, hemos explicado que existen diversos argumentos a favor y en contra sobre el posible poder de mercado que una empresa pudiera adquirir al acumular grandes cantidades de datos en un mercado relevante. Este fenómeno tiene gran relevancia en el uso de nuevas tecnologías como el *Big Data*. Las tecnologías de *Big Data* pueden proporcionar beneficios y eficiencias significativas a la sociedad como servicios de mejor calidad, mayor eficiencia en procesos productivos, más innovación, entre otras. Sin embargo, también pueden representar barreras a la entrada y mayor capacidad de discriminación.

Con relación a la protección de datos personales como parte del derecho a la privacidad de las personas, que es el tema principal de este estudio y particularmente para el sector de las telecomunicaciones, hemos mencionado que es fundamental contar con normas, mecanismos de aplicación y códigos de buenas prácticas que estén a la altura de los retos que actualmente representan los nuevos servicios y tecnologías. Para ello hemos analizado las normas y conceptos que el reglamento europeo (GDPR) contempla como parte de su proceso de modernización para hacer frente a estos nuevos retos. Particularmente identificamos las normas del GDPR que consideramos son clave para el sector de telecomunicaciones y que México podría adoptar de manera similar para el ámbito privado: portabilidad de datos, evaluación de impacto y protección desde el diseño y por defecto.

En el sector de las telecomunicaciones, el Instituto Federal de Telecomunicaciones (IFT) es quien tiene la enorme responsabilidad de desarrollar de forma eficiente las telecomunicaciones e impulsar la competencia efectiva del sector en beneficio de todos los usuarios de nuestro país. Sin lugar a dudas sabemos que el IFT tiene todas las facultades para atender cualquier afectación al sector, de ahí que consideremos la gran relevancia de la protección de datos personales para el desarrollo adecuado de este sector. Por un lado, en este estudio mostramos que los operadores recolectan, resguardan y procesan datos personales de sus usuarios cuando éstos hacen uso de sus servicios. Por otro lado, sabemos que los operadores desarrollarán o harán uso de tecnologías emergentes (por ejemplo, 5G, IoT, *Big Data*, etc.) que tienen el potencial de recabar grandes cantidades de datos personales y procesarlos. Además, consideramos que los operadores son y seguirán siendo (al menos para el futuro cercano) los principales facilitadores de conectividad para la provisión de diversos servicios, aplicaciones y contenidos sin importar quién sea el proveedor original. Es decir, la gran cantidad de tráfico que continúe generándose en el mundo será transmitido por los operadores. Por tal motivo, consideramos que los operadores juegan un papel importante en la protección de datos personales.

Por lo anterior, y por el análisis que hemos desarrollado a lo largo de este estudio, podemos concluir puntualmente lo siguiente:

- Las autoridades y reguladores tienen el gran reto de garantizar el derecho de privacidad de las personas sin mermar la innovación y el desarrollo del ecosistema digital, particularmente en la provisión de nuevos servicios que involucren la utilización de tecnologías emergentes (por ejemplo, IoT, *Big Data*, 5G, etc.).

- El primer paso que debemos realizar para tener un mejor control de nuestros datos personales y hacer valer nuestros derechos es fomentar una cultura de mayor conciencia sobre el valor y protección de nuestros datos. Observamos que en México existe un desconocimiento general entre la población y que no existen los mecanismos apropiados para la correcta aplicación y cumplimiento de nuestras leyes sobre protección de datos personales. También creemos que el fortalecimiento de la protección de datos personales debe realizarse en conjunto entre personas, empresas y autoridades.

- Una mayor concientización de las personas, un mayor nivel de protección y un uso más adecuado de los datos son factores habilitadores para el desarrollo de la economía digital, particularmente creemos que incrementarían la confianza de las personas sobre el comercio electrónico.

- El contenido del marco regulatorio mexicano sobre protección de datos personales es sólido; sin embargo, en el ámbito privado, en comparación con otros países como Argentina o Brasil, México requiere adoptar normas similares al reglamento europeo que regulen y promuevan la portabilidad de datos, la protección desde el diseño y por defecto, así como la realización de evaluaciones de impacto que identifiquen aquellos servicios que potencialmente pongan en riesgo la privacidad de las personas. Estas nuevas normas y conceptos son fundamentales, tomando en cuenta que surgen del proceso de modernización del reglamento europeo debido a la innovación tecnológica de los últimos años.

- Es claro que la implementación y observancia general sobre la regulación de la protección de datos personales en nuestro país está a cargo del INAI; sin embargo, también es muy claro que la promoción y supervisión de cualquier regulación que impacte al sector de telecomunicaciones está a cargo del IFT. Por tal motivo, consideramos que el IFT tiene todas las facultades para promover la implementación de normas similares al reglamento europeo que estén íntimamente ligadas con el uso y desarrollo de nuevas tecnologías de comunicación, y que tengan un impacto directo en el procesamiento de los datos personales de los usuarios de telecomunicaciones. Particularmente consideramos pertinente la implementación de la protección desde el diseño y por defecto en los dispositivos, sistemas y redes que utilizan los operadores, así como el fortalecimiento de medidas técnicas y organizativas que garanticen dicho principio en sus procesos e instalaciones.

- Asimismo, la promoción de recomendaciones (o códigos de buenas prácticas) respecto a la protección y seguridad desde el diseño, exclusivas para el sector de telecomunicaciones, son acciones que el IFT puede impulsar en favor de la protección de los datos personales.

- Además, consideramos como buena práctica la realización de evaluaciones de impacto entre los operadores cuando deseen brindar nuevos servicios que involucren el uso de nuevas tecnologías (e.g. IoT, *Big Data*, 5G, etc) y que tengan un potencial riesgo en la privacidad de los usuarios.

- Finalmente, coincidimos que cualquier distorsión en el mercado que afecte al sector de telecomunicaciones, debido a la acumulación de datos por parte de cualquier empresa u organización, debe analizarse bajo un esquema de colaboración entre todas las autoridades competentes: IFT, Comisión Federal de Competencia Económica (COFECE) e INAI.

Bibliografía

1. Akram, R. N., Chen, H., Lopez, J., Sauveron, D., Yang L. T. (2018). *Security, privacy and trust of user-centric solutions*. ScienceDirect. Future Generation Computer Systems. Recuperado de http://iranarze.ir/wp-content/uploads/2018/05/320-English-IranArze.pdf

2. Alkhalil, A., & Ramadan, R. A. (2017). *IoT Data Provenance Implementation Challenges*. Procedia Computer Science. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S1877050917311183?token=6CE17FF96B9AA7BECDE88800C9D14A2EF9DEA1C36D6ECA262C236CFB91B53D5C90138890092F1AEA297A4F5D12990F66

3. Argenton, C., & Prüfer, J. (2012). *Search engine competition with network externalities*. Journal of Competition Law and Economics, 8(1), 73–105.

4. Article 29 Data Protection Working Party. (2013). *Opinion 02/2013 on apps on smart devices*. European Commission. Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

5. Article 29 Data Protection Working Party. (2014). *Opinion 8/2014 on the on Recent Developments on the Internet of Things*. European Commission. Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

6. Article 29 Data Protection Working Party. (2015). *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*. European Commission. Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

7. Asociación Mexicana de Internet. (2017). *Estudio sobre el Valor Económico de los Datos Personales.* Recuperado de https://asociaciondeinternet.mx/images/valor_eco_Datospersonales_FINAL.pdf

8. AT&T. (2018). *AT&T Business Customer GDPR Privacy Notice*. Recuperado de https://about.att.com/content/dam/sites/Privacy%20Policy/GDPR_Customer_Privacy_Notice_May_2018.pdf

9. Barnard-Wills, D. (2017). *The technology foresight activities of European Union data protection authorities*. Technological Forecasting & Social Change. Recuperado de https://ac.els-cdn.com/S0040162516305571/1-s2.0-S0040162516305571-main.pdf?_tid=facbe8cf-4a0b-4957-a4ca-17ae610b0b74&acdnat=1529952708_ff7515e59988c4554b2b540fff20e166

10. Broadhead, S. (2018). *The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments*. Computer Law & Security Review. Elsevier Ltd. Recuperado de https://ac.els-cdn.com/S026736491830308X/1-s2.0-S026736491830308X-main.pdf?_tid=db5f0e86-016d-4fdf-a844-df3bbd22777b&acdnat=1539803210_f44f050a50476a72d1fbf1b461fd823f

11. Bouazzouni, M. A., Conchond, E., & Peyrarda, F. (2018). *Trusted mobile computing: An overview of existing solutions*. ScienceDirect. Future Generation Computer Systems. Recuperado de https://ac.els-cdn.com/S0167739X16301510/1-s2.0-S0167739X16301510-main.pdf?_tid=98f36141-696a-412d-a73d-b312aa6ca49c&acdnat=1530302296_972c7464fb53fc50037b759e579dbedb

12. Bujlow, T., Carela-Español, V., Solé-Pareta, J., & Barlet-Ros, P. (2017). *A Survey on Web Tracking: Mechanisms, Implications, and Defenses*. Proceedings of the IEEE. Recuperado de https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7872467

13. Campbell, J., Goldfarb, A., & Tucker, C. (2015). *Privacy regulation and market structure.* Journal of Economics & Management Strategy, 24(1), 47–73.

14. Carolina da Motta, A. (2017). *Chile government proposes bill to modernise the protection of privacy and personal data*. Cullen International. Recuperado de https://www.cullen-international.com/product/pdf/FLMECL20170002

15. Centro de Estudios de Telecomunicaciones de América Latina. (2018). *IoT para el Sector Empresarial en América Latina*. Deloitte. Recuperado de https://cet.la/estudios/cet-la/iot-sector-empresarial-america-latina/

16. Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., & Kohno, T. (2018). *Computer security for data collection technologies*. Development Engineering. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S2352728516300677?token=5EF9B8E3DF766F01AE2C8053601BE86143CCB7DE4CD43FA0E2990E4CEFAB9D2A46432C1F5CC8E9F074A8315FF37BC2F0

17. Comisión Europea. (2017). *Reglamento Del Parlamento Europeo y Del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES

18. CONPES (Consejo Nacional de Política Económica y Social). (2018). *Política Nacional de Explotación de Datos (Big Data)*. Bogotá, D.C. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

19. Consumers International. (2017). *Connecting voices: a role for consumer rights in developing digital society*. Recuperado de https://www.consumersinternational.org/media/154869/ci_connecting-voices_2017_v2.pdf

20. Cornock, Marc. (2018). *General Data Protection Regulation (GDPR) and implications for research*. Maturitas. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S0378512218300367?token=3A1CF20676349B5CA9C28FBBEF8E2394FC19F8B9D74328FBA09994A5989156AF8264F462303091CA1DF76828BC429F33

21. Council of the European Union. (2018). *Interinstitutional File: 2017/0003 (COD). 5165/18 TELECOM 4 COMPET 18 MI 14 DATAPROTECT 2 CONSOM 3 JAI 16 DIGIT 2 FREMP 2 CYBER 4 CODEC 14*. Brussels. Recuperado de http://data.consilium.europa.eu/doc/document/ST-5165-2018-INIT/en/pdf

22. Council of the European Union. (2018). *Interinstitutional File: 2017/0003(COD). 10975/18 TELECOM 221 COMPET 513 MI 522 DATAPROTECT 149 CONSOM 205 JAI 748 DIGIT 147 FREMP 123 CYBER 158 CODEC 1253* . Brussels Recuperado de https://www.iab-austria.at/wp-content/uploads/2018/07/ePrivacy-july-discussion-paper.pdf

23. Cullen International. (2017). *New EU e-Privacy Regulation (ePR). What could it mean for you?*. Cullen International's Digital Economy. Recuperado de https://iapp.org/media/pdf/resource_center/Cullen-Intl-epriv-reg-infographic.pdf

24. Data Protection Office. (2016). *A guide on Apps on Smart Devices*. Government of Mauritius. Recuperado de http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Guidelines%20on%20apps.pdf

25. Diario Oficial de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).* Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf

26. Diario Oficial de las Comunidades Europeas. (2002). *DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=EN

27. Dimitrova, D., Pichierri, F., Boehm, F. (2016). *D8.1 Privacy Implications*. European Union's. Recuperado de http://www.starrproject.org/deliverables/D8.1-PrivacyImplications-FIZ.pdf

28.DLA Piper. (2017). *Data Protection Laws of The World*. Recuperado de http://www.straightlineinternational.com/docs/Data-Protection-Full.pdf

29. DOF: 26/01/2017. *DECRETO por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Diario Oficial de la Federación, 20 de agosto de 2018.

30. El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso. (2017). *Anteproyecto reforma ley protección de los datos personales nueva versión*. Recuperado de https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pdf

31. Elahi, H., Wang, G., & Xie, D. (2017). *Assessing Privacy Behaviors of Smartphone Users in the Context of Data Over-Collection Problem: An Exploratory Study*. IEEE Xplore Digital Library. Recuperado de https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8397613

32. Ernst & Young Global Limited. (2018). *How will GDPR effect the telecom business?*. UK. Recuperado de http://www.terminsstarttelekom.se/upload/termin/pdf/pres461.pdf

33. European Data Protection Supervisor. (2014). *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

34. European Data Protection Supervisor. (2015). *Guidelines on the protection of personal data in mobile devices used by European institutions*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-12-17_mobile_devices_en.pdf

35. European Data Protection Supervisor. (2016). *Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf

36. European Data Protection Supervisor. (2016). *Guidelines on the protection of personal data processed through web services provided by EU institutions*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf

37. Gomes, A. M. (2018). *Brazilian regulator consults on regulatory review of IoT*. Cullen International. Recuperado de https://www.cullen-international.com/product/pdf/FLTEBR20180006

38. Guo, A., & Ma, J. (2015). *A Smartphone-based System for Personal Data Management and Personality Analysis*. IEEE International Conference on Computer and Information Technology. IEEE Computer Society. Recuperado de https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7363360

39. Guo, A., & Ma, J. (2017). *Context-Aware Scheduling in Personal Data Collection From Multiple Wearable Devices*. IEEE Access. Recuperado de https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7847301

40. Hallam, C., & Zanella, G. (2017). *Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards*. ScienceDirect. Computers in Human Behavior. Recuperado de https://ac.els-cdn.com/S0747563216307749/1-s2.0-S0747563216307749-main.pdf?_tid=d427c65f-6ee6-40f5-9809-28f035c6f79e&acdnat=1530209816_b722a4f4f8d2c92c802f9927d7e74823

41. Hare, S. (2016). *For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection*. ScienceDirect. Elsevier Inc. Kelley School of Business, Indiana University. Recuperado de https://ac.els-cdn.com/S0007681316300362/1-s2.0-S0007681316300362-main.pdf?_tid=cbaff8a1-b785-4e70-9fb4-d4eb4a1df8e2&acdnat=1530051688_65ad54ae1032bd774500b5cb90a44a24

42. INAI. (2017). *Guía para titulares de datos personales. Volumen 1*. Cinvestav Recuperado de https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf

43. International Working Group on Data Protection in Telecommunications. (2014). *Working Paper on Big Data and Privacy Privacy principles under pressure in the age of Big Data analytics*. *Skopje.* Recuperado de https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf

44. International Working Group on Data Protection in Telecommunications. (2015). *Working Paper on Location Tracking from Communications of Mobile Devices*. Berlin. Recuperado de https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2015/14102015_en.pdf

45. International Working Group on Data Protection in Telecommunications. (2015). *Working Paper on Privacy and Wearable Computing Devices*. Seoul. Recuperado de https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2015/28042015_en_2.pdf

46. International Working Group on Data Protection in Telecommunications. (2016). *Working Paper: Update on Privacy and Security Issues in Internet Telephony (VoIP) and Related Communication Technologies*. Oslo. Recuperado de https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2016/25042016_en.pdf

47. Kesler, R., Kummer, M., & Schulte, P. (2017). *User Data, Market Power and Innovation in Online Markets: Evidence from the Mobile App Industry*. Economic Research. Recuperado de http://www.law.northwestern.edu/research-faculty/searlecenter/events/internet/documents/KeslerKummerSchulteSEARLE17.pdf

48. Khan, M. A., & Salah, K. (2018). *IoT security: Review, blockchain solutions, and open challenges*. Future Generation Computer Systems. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S0167739X17315765?token=D99A4C74DCF7147BD64624D8730801E0A0AB54E978A880770695CB53AF832A1A52C0A399CAA3257065FE8067CB5C4F64

49. Kokolakis, S. (2017). *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. ScienceDirect. Computers & Security. Recuperado de https://ac.els-cdn.com/S0167404815001017/1-s2.0-S0167404815001017-main.pdf?_tid=872ff563-5ccb-421d-8d5e-33afc89ba6d3&acdnat=1530203819_dd5a366012ff0d35296e3a0aee7cd7dc

50. Krämer, J., & Wohlfarth, M. (2015). *Regulating over-the-top service providers in two-sided content Markets: Insights from the economic literature.* Digiworld Economic Journal, 1(99), 71–90.

51. Krämer, J., & Wohlfarth, M. (2017). *Market power, regulatory convergence, and the role of data indigital markets*. Telecommunications Policy. Recuperado de https://doi.org/10.1016/j.telpol.2017.10.004

52. Ley 1581. *Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial de Bogotá, 18 de octubre de 2012.

53. Ley DOF 05-07-2010. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Diario Oficial de la Federación de México, 5 de Julio de 2010.

54. Ley Nº 29733. *Ley de Protección de Datos Personales*. Diario Oficial El Peruano, 22 de marzo de 2013.

55. LEY No 13.709. *Dispone sobre la protección de datos personales y altera la Ley nº 12.965, de 23 de abril de 2014 (Marco Civil de Internet)*. Diario Oficial de la Unión. 14 de agosto de 2018.

56. Ley Nº 18.331. *Protección de Datos Personales y Acción de "Habeas Data"*. Diario Oficial de Uruguay, 18 de agosto de 2008.

57. Malgieri, G., & Custers, B. (2018). *Pricing privacy – the right to know the value of your personal data*. Computer Law & Security Review. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S0267364917302819?token=79AE5E07C4393B62E2AF9327AF379781978B75445BECA7AA4D2CF733FDCDC5A40DC264C30D5DCF7EFAF8ABA2015EFB3E

58. Mantelero, A. (2014). *Social Control, Transparency, and Participation in the Big Data World*. Journal of Internet Law. Recuperado de http://staff.polito.it/alessandro.mantelero/JIL_0414_Mantelero.pdf

59. Monopolies Commission. (2015). *Competition policy: The challenge of digital markets*. Recuperado de https://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf

60. Nº Boletín: 11144-01 y 11092, refundidos. *Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.* Senado República de Chile, 22 de enero de 2018.

61. Nakarmi, P. K., Schaefer, C., & Casella, D. (2018). *5G and the EU General Data Protection Regulation*. Ericsson Research Blog. Recuperado de https://www.ericsson.com/research-blog/5g-and-the-eu-general-data-protection-regulation/

62. Norberg, P. A., Horne, D. R., & Horne, D. A. (2018). *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*. JSTOR. Wiley. Recuperado de https://www.jstor.org/stable/23860016

63. OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*. OECD Digital Economy Papers No. 220. OECD Publishing, Paris. Recuperado de http://dx.doi.org/10.1787/5k486qtxldmq-en

64.OECD. (2013). *The OECD Privacy Framework*. Recuperado de https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

65. Official Journal of the European Communities. (2002). *DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

66. Peitz, M., & Valletti, T. (2015). *Reassessing competition concerns in electronic communications markets*. Telecommunications Policy, 39(10), 896–912.

67. Peschard Mariscal, J. (2013). *El derecho fundamental a la protección de datos personales en México. En La Protección de datos personales en México* (19-38). México: tirant lo blanch.

68. Raab, C., & Szekely, I. (2017). *Data protection authorities and information technology*. ScienceDirect. Computer Law & Security Review Recuperado de https://reader.elsevier.com/reader/sd/4E40D9F248DF4996E19E7A36C2356EA1198C95692FB377D85D5E454C318EECE8DCFB540D601EAA5A7554E0CFF8504EA0

69. Reglamento DOF 21-12-2011. *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Diario Oficial de la Federación, 21 de diciembre de 2011.

70. Renaud, K., & Shepherd, L. (2018). *GDPR: its time has come.* Network Security. Recuperado de https://doi.org/10.1016/S1353-4858(18)30017-5

71. Romanou, A. (2018). *The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise*. ScienceDirect. Computer Law & Security Review. Recuperado de https://ac.els-cdn.com/S0267364917302054/1-s2.0-S0267364917302054-main.pdf?_tid=8da3038f-8bcb-4dfa-b246-fb44e86b0c7b&acdnat=1529953316_83d6863379fcb04979ce13df979eeaf8

72. Rumbold, J. M. M., & Pierscionek, B. K. (2018). ScienceDirect. Big Data Research. Recuperado de https://reader.elsevier.com/reader/sd/pii/S2214579617302010?token=9D0F61F7191412F72185642F67FC9C5ACA560F948B59F090868A377AE2EAB70D374EC2C9DA7C1A3189B3C69171795823

73. S.C. 2000, c. 5. *Personal Information Protection and Electronic Documents Act*. Canadá, 23 de junio del 2015.

74. Schepp, N.-P., & Wambach, A. (2016). *On Big Data and its relevance for market power assessment.* Journal of European Competition Law & Practice, 7(2), 120–124.

75. Steppe, R. (2017). *Online price discrimination and personal data: AGeneral Data Protection Regulation perspective*. ScienceDirect. Computer Law & Security Review. Recuperado de https://reader.elsevier.com/reader/sd/3989845DA087942C63BE694B4EC948387C92443211C63BB25138F1BF05F4D02F18E78B6AA88B1B7AED65D331572ED005

76. The Economist. (2017). *Fuel of the future. Data is giving rise to a new economy. How is it shaping up?*. Recuperado de https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

77. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*. Elsevier. Recuperado de https://www.sciencedirect.com/science/article/pii/S0267364917301966

78. United Nations Conference on Trade and Development (UNCTAD). (2016). *Data protection regulations and international data fl ows: Implications for trade and development*. Switzerland. UNITED NATIONS PUBLICATION. Recuperado de https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

79. Van der Auwermeulen, B. (2017). *How to attribute the right to data portability in Europe: A comparative analysis of legislations*. ScienceDirect. Computer Law & Security Review. Recuperado de https://ac.els-cdn.com/S0267364916302175/1-s2.0-S0267364916302175-main.pdf?_tid=148ffa85-13c8-4318-adeb-6b4637752003&acdnat=1530124421_e5db3e4f8e1d21de4719f0e97b57833d

80. van-Dijk, N., Gellerta, R., & Rommetveit, K. (2016). *A risk to a right? Beyond data protection risk assessments*. ResearchGate. Computer Law & Security Review. Recuperado de https://www.researchgate.net/publication/294577405_A_risk_to_a_right_Beyond_data_protection_risk_assessments

81. Wachter, S. (2018). *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*. Computer Law & Security Review. ScienceDirect. Recuperado de https://reader.elsevier.com/reader/sd/pii/S0267364917303904?token=FADC9E8E538BF62E8FE54FEA52781A34C2B2BC44B1F8063CBFDF046984818E8BF0C9819250FE5B8709149EB17E44A8DF

82. Wessels, B., Finn, R. L., Wadhwa, K., Sveinsdottir, T., Bigagli, L., Nativi, S., & Noorman, M. (2017). *Big data, open data and the commercial sector*. Amsterdam University Press. JSTOR. Recuperado de https://www.jstor.org/stable/j.ctt1pk3jhq.13

83. Wohlfarth, M. (2018). *Data as a Competitive Resource. Essays on Market Power, Data Sharing, and Data Portability*. University of Passau. Recuperado de https://d-nb.info/1160442045/34

84. Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2017). *Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing*. ScienceDirect. Information Sciences. Recuperado de https://ac.els-cdn.com/S002002551630250X/1-s2.0-S002002551630250X-main.pdf?_tid=accec4eb-7338-4ac6-b270-b48620880c23&acdnat=1530642780_0a86cb382745c6b9fca8b6065191116f

85. Zhuravlev, M. S., & Brazhnik, T. A. (2017). *Russian data retention requirements: Obligationto store the content of communications*. ScienceDirect. Computer Law & Security Review. Recuperado de https://reader.elsevier.com/reader/sd/8CC70FF19386CBA53D81D8964C397897CB4C9795FC5DEC3FB119F40B51CBF157A9CA6299F4F946F5E43C0A68C3A48406