REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

SEGUNDO SEMESTRE 2015 VOL. 4 NÚM. 2

FACULTAD DE
DERECHO
UNIVERSIDAD DE CHILE
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO

REPRESENTANTE LEGAL

PROF. DAVOR HARASIC YAKSIC

Decano, Facultad de Derecho, Universidad de Chile.

DIRECTOR RESPONSABLE

PROF. ALEX PESSÓ STOULMAN

EDITOR GENERAL

PROF. DANIEL ÁLVAREZ VALENZUELA

COMITÉ EDITORIAL

MG. ALBERTO CERDA

Profesor Asistente, Facultad de Derecho, Universidad de Chile, Chile. LL.M. in International Legal Studies, Georgetown University. Magíster en Derecho Público, Universidad de Chile.

MG. MARCELO CORRALES

Investigador Senior, Institute for Legal Informatics, Leibniz University of Hanover, Alemania. LL.M. in European Intellectual Property Law, Stockholm University. LL.M. in Law and Information Technology, Stockholm University.

DR. CARLOS DELPIAZZO

Profesor de Derecho Administrativo y Derecho Informático, Universidad de la República, Uruguay. Doctor en Derecho y Ciencias Sociales, Universidad de la República, Uruguay.

DR. RONALDO LEMOS

Director, Instituto de Tecnologia & Sociedade do Rio de Janeiro. Doctor en Derecho, Universidad de Sao Paulo, Brasil. LL.M. in Law, Harvard University.

DR. JULIO TÉLLEZ

Investigador Titular Derecho de la Informática. Universidad Nacional de México, México. Doctor en Informática Jurídica y Derecho de la informática, Universidad de Montpellier I, Francia.

La *Revista Chilena de Derecho y Tecnología* es una publicación semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile que tiene por objeto difundir en la comunidad jurídica nacional, regional e internacional, el conocimiento científico relevante y necesario para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en las ciencias jurídicas y sociales.

Revista Chilena de Derecho y Tecnología
Rev. chil. derecho tecnol. (impr.)
Centro de Estudios en Derecho Informático
Facultad de Derecho · Universidad de Chile
Pío Nono núm. 1, 4.º piso, Providencia
Santiago de Chile

+56 2 29785263
rchdt@derecho.uchile.cl
http://www.cedi.uchile.cl
http://twitter.com/rchdt

ISSN 0719-2584

La *Revista Chilena de Derecho y Tecnología* es publicada en formatos electrónicos (pdf, epub y mobi) disponibles para descarga en la página web <http://www.rchdt.uchile.cl/>.

Una guía para la presentación de manuscritos a la *Revista Chilena de Derecho y Tecnología* está disponible en el siguiente enlace: <http://www.revistas.uchile.cl/index.php/rchdt/about/submissions#authorguidelines>.

Algunos derechos reservados.
Publicada bajo los términos de la licencia Creative Commons
ATRIBUCIÓN - NO COMERCIAL - COMPARTIR IGUAL 2.0 CHILE.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
SEGUNDO SEMESTRE 2015 VOL. 4 NÚM. 2
Rev. chil. derecho tecnol. (impr.)

7-8 *Editorial*

9-51 PAULA JERVIS ORTIZ
Internet de las cosas y protección de datos personales

53-74 ARTURO J. CARRILLO Y DAWN C. NUNZIATO
El precio de la priorización pagada: Las consecuencias internacionales y domésticas del fracaso de proteger la neutralidad en la red en los Estados Unidos

75-107 FELIPE FIGUEROA ZIMMERMANN
¿Qué significa justificar el derecho de autor?

109-177 FERDINAND SCHNETTLER CHÁVEZ
Responsabilidad civil extracontractual de los usuarios de programas P2P por infracción a los derechos de autor

179-213 MARÍA PAZ CANALES LOEBEL
Oracle versus Google: Protección de derecho de autor sobre elementos funcionales de programas computacionales que ponen en riesgo la interoperabilidad y la innovación

215-261 ANA MARÍA MUÑOZ MASSOUH
Eliminación de datos personales en internet: El reconocimiento del derecho al olvido

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2584 • VOL. 4 NÚM. 2 (2015) • PÁGS. 9-51 • DOI 10.5354/0719-2584.2015.37509

Internet de las cosas y protección de datos personales

Internet of the Things and Data Protection

PAULA JERVIS ORTIZ
Abogada, Chile

RESUMEN El presente artículo tiene como objetivo conceptualizar a la internet de las cosas, establecer cuáles son sus principales características, actores y elementos relevantes que determinan que sea considerada como una amenaza a la privacidad y a la protección de los datos personales. Se revisará cuáles son esas amenazas, la problemática particular de la internet de las cosas que las genera y los modelos de protección que se han elaborado para mitigar el riesgo de concreción de dichas amenazas. Se termina proponiendo un modelo de protección en el cual los derechos a la privacidad y a la protección de los datos personales son realmente amparados por herramientas legales, de mercado, tecnológicas y sociales que actúan sistémicamente y en forma efectiva para el logro de la finalidad buscada.

PALABRAS CLAVE Internet de las cosas, IoT, privacidad, protección de datos personales, modelos de protección de datos.

ABSTRACT This article aims to conceptualize the Internet of the Things, to establish what are its main characteristics, actors and relevant elements that determine it to be considered as a threat to privacy and to the protection of personal data. It will review what those threats are,

the particular problems of the Internet of the Things that generate it and the protection models that have been developed to mitigate the risk of realization of these threats. It ends by proposing a model of protection in which the rights to privacy and to the protection of personal data are really protected by legal, market, technological, and social tools that act systemically and effectively to achieve the intended purpose.

KEYWORDS Internet of the things, IoT, privacy, data protection, models of data protection.

INTRODUCCIÓN

La internet de las cosas (IoT, en su acrónimo en inglés) es una tecnología que resulta cada vez más cercana a las personas, y constituye hoy en día un negocio atractivo para grandes y pequeñas empresas, en el extranjero y en Chile.[1] Por otra parte, sus efectos tanto desde la perspectiva de los avances que puede entregar a la sociedad como de eventuales amenazas y desafíos a la seguridad y a la privacidad de las personas, constituyen un asunto al cual los gobiernos de distintos países,[2] organismos no gubernamentales y sociedad civil están muy atentos.[3]

1. La inversión en Chile de internet de las cosas superó los 300 millones de dólares durante 2014. Los expertos estiman que la inversión en IoT continuará al alza en Chile durante 2015, con un crecimiento de 11,7% con respecto a 2014. Una tendencia que se repite a nivel global y regional. Sólo en el mundo se espera que para 2020 la cantidad de cosas conectadas aumente 19% anualmente, triplicando los 10 billones durante el año 2014. Mientras que a nivel regional, se prevé que para 2015 el tamaño total llegue a los 8.8 billones de dólares. Véase IDC (2015).

2. La Unión Europea tiene a la IoT dentro de los aspectos relevantes en la Agenda Digital Europea (véase Comisión Europea, 2015a). Por su parte, la Federal Trade Commission de Estados Unidos también se ha pronunciado respecto del tema en el reporte «Internet of Things. Privacy & Security in a Connected World» de junio de 2015 (véase Federal Trade Commission 2015).

3. En Estados Unidos, por ejemplo, el Electronic Privacy Information Center (EPIC) indica que: «Esta mayor conectividad (la que genera la IoT) plantea innumerables problemas respecto de la privacidad del consumidor y de seguridad de datos. Las agencias gubernamentales, como la Comisión Federal de Comercio, están preocupadas de estos temas. El desarrollo de la IoT significa que las empresas preservan la privacidad. Entre

Se trata de un avance tecnológico que permite, por ejemplo, determinar cuál es el comportamiento de manejo por parte de un conductor y con ello elegir qué prima de seguro automotriz es eficiente cobrar conforme el nivel de riesgo que presenta en base a un historial de comportamientos; registrar los movimientos de los pacientes dentro de la urgencia de una clínica u hospital para mejorar sus flujos y restringir accesos conforme sus perfiles; contar con hogares inteligentes que permitan regular la temperatura y la luz según sus preferencias y horarios o evitar robos o accidentes domésticos con sistemas de monitoreo y alarmas apropiadas; encontrar objetos que usualmente se extravían mediante tecnología RFID[4] o reconocer que han sido movidos de su lugar ya sea con o sin consentimiento; efectuar actualizaciones automáticas en redes sociales respecto a actividades o lugares que visitan sus usuarios; utilizar dispositivos que permitan a los individuos llevar un registro de sus propios hábitos o estilo de vida, como patrones de sueño, hábitos alimenticios, actividad física, distancias caminadas y calorías quemadas.[5]

Considerando que la gran cantidad de aplicaciones y usos, tanto conocidos como aún no explorados, que permitiría la IoT pueden constituir una amenaza a la privacidad de las personas,[6] fundamentalmente

---

otras cosas, esto implica la adopción de las mejores prácticas en materia de privacidad y seguridad, recolectar la información personal sólo con el consentimiento expreso de sus titulares, y proporcionar a los consumidores el acceso a sus datos» (Electronic Privacy Information Center, 2015).

4. Sistema de rotulación por radiofrecuencia que proporciona datos de identificación para los bienes a fin de que pueda realizarse el seguimiento de los mismos (cf. International Telecommunication Union, 2015).

5. Para las diversas aplicaciones que permite la IoT, véase Atzori, Iera y Morabito (2010).

6. La privacidad es un concepto jurídico anglosajón acuñado por Warren y Brandeis (1890) en su artículo «The Right to Privacy» y es entendido como el derecho a ser dejado solo, frente al acoso periodístico. Este concepto inicial de privacidad ha ido evolucionando en el tiempo, conforme —fundamentalmente— los avances tecnológicos; en este sentido se han perfilado hasta seis categorías de privacidad: i) como derecho a ser dejado solo (Warren y Brandeis); ii) límite al acceso a uno mismo, como la posibilidad de protegerse uno mismo del acceso no deseados por parte de terceros; iii) secreto, como la no revelación de ciertas materias a otros; iv) control sobre la información personal, como la habilidad de ejercer control sobre la información sobre uno mismo; v) personalidad, como la protección de la personalidad, individualidad y dignidad de uno mismo; y, v)

en su aspecto asociado a la privacidad informacional o de protección de datos personales, cabe preguntarse cuáles serían tales amenazas y cuáles son los requisitos que debe cumplir un sistema de protección para que exista un marco adecuado que entregue a las personas la certeza que se respetarán sus derechos en tanto titulares de datos personales, lo cual constituye un requisito básico en el cual se debe cimentar esta nueva tecnología.[7]

Este artículo desarrolla en su primer subtítulo un acercamiento al concepto y principales características de su objeto de estudio, elaborando un marco adecuado para esbozar cuál es el ecosistema de la IoT y cuáles son sus elementos y actores relevantes. Una vez asentados los conceptos básicos de esta tecnología, el segundo subtítulo explora cuáles son los problemas y amenazas que la IoT genera para la privacidad y protección de datos personales, pronunciándose respecto de si se trata de nuevas o distintas amenazas a las que nacen de la ya vieja relación entre tecnología e información personal. Finalmente, en el último subtítulo, se revisan en primer lugar los principales modelos de protección que se han evidenciado por la literatura como idóneos para mitigar las amenazas que la IoT produce, para luego proponer un modelo de protección que contempla herramientas de diversa naturaleza para solucionar el proble-

---

intimidad, control sobre o limitar el acceso a las relaciones o aspectos íntimos de uno mismo (cf. Solove, 2002).

7. En este sentido se pronuncia, por ejemplo, el Article 29 Working Party (en adelante, WP29) de la Comisión Europea, al indicar: «De hecho, empoderar a los individuos manteniéndolos informados, libres y seguros es la llave que soporta la confianza y la innovación, y por lo tanto el éxito de estos mercados. Creemos firmemente que los actores que cumplan con estas expectativas tendrán una excepcional ventaja competitiva sobre los otros cuyos modelos de negocio se sostengan en mantener a sus clientes inadvertidos de la extensión en que sus datos son procesados, compartidos y contenidos dentro de sus sistemas» (Article 29 Working Party, 2014). Por otra parte, existen estadísticas que demuestran que las personas están interesadas en resguardar su privacidad, aun cuando muchas de ellas consideren que la divulgación creciente de datos personales forma parte de la vida moderna, ellos sienten que no tiene control sobre su información; un gran porcentaje (74%) le gustaría dar un consentimiento específico antes que sus datos personales fueran recolectados y procesados. Por otra parte, la confianza en las compañías de internet es baja: sólo el 22% de las personas confían en los proveedores de servicio de internet como buscadores, redes sociales y servicios de correo electrónico (Comisión Europea, 2015a).

ma planteado y que enmienda las falencias de los modelos actuales que se concentran en sólo una vía de protección.

NOCIONES DE LA INTERNET DE LAS COSAS

CONCEPTO

Aun cuando ya han trascurrido casi dos décadas desde que el concepto IoT fuera utilizado por primera vez por Kevin Ashton en una presentación en 1998,[8] no existe consenso aún en una definición única, al parecer, a consecuencia de que el mismo nombre está compuesto de dos términos que orientan su alcance a visiones distintas. Así, el primero, supone una visión de red, mientras que el segundo pone el foco en el genérico «objetos». De esta forma, como a continuación se podrá observar, las definiciones de los distintos actores en la IoT están orientadas hacia una u otra visión, según sean sus intereses, finalidades o experiencias (cf. Atzori, Iera y Morabito, 2010).

La IoT ha sido conceptualizada por la Comisión de la Unión Europea como aquella que permite a los objetos compartir información con otros objetos/miembros en la red, reconociendo eventos y cambios de manera de reaccionar autónoma y apropiadamente. La IoT, por lo tanto, se basa en la comunicación entre cosas (máquinas, edificios, autos, animales, etcétera) que conduce a la acción y creación de valor (Comisión Europea, 2015a). Por su parte, la Unión Internacional de Telecomunicaciones (ITU, por su nombre en inglés) la define como una infraestructura global para la sociedad de la información permitiendo servicios avanzados mediante la interconexión de cosas (físicas y virtuales), basados en la interoperabilidad de las tecnologías de información y comunicación existentes y en evolución (International Telecommunication Union, 2015).

Por otra parte, organismos vinculados a la protección de los datos personales, como el WP29,[9] la han definido como una infraestructura en la cual billones de sensores incorporados en dispositivos cotidianos

8. Kevin Ashton mencionó que la IoT tiene el potencial de cambiar el mundo, tal como internet lo hizo, incluso más. El centro Auto-ID de MIT presentó su visión de la IoT en el 2001, y luego en el año 2005, la International Telecommunication Union introdujo formalmente el concepto en su *ITU Internet report* (cf. Perera 2014).

9. Article 29 Working Party (2014).

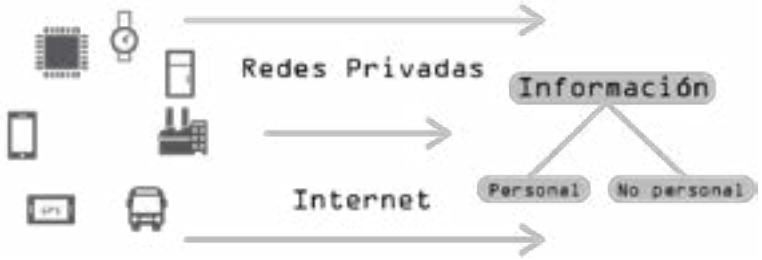

Figura 1.

—«cosas» como tal, o cosas vinculadas a otros objetos o a individuos— son diseñados para registrar, procesar, almacenar y transferir datos y, ya que están asociados con identificadores únicos, interactuar con otros dispositivos o sistemas que utilizan capacidades de red.

En este artículo se entiende a la IoT como una arquitectura que permite que objetos (en un sentido amplio de la palabra[10]) compartan información ya sea de ellos mismos o acerca de personas a través de una red. En consecuencia, son elementos esenciales de esta definición, la existencia de una cosa u objeto, la cual debe compartir información que puede ser personal o no, y que esa entrega de información se efectúe a través de una red, que puede ser internet u otra, como se grafica en la figura 1.

La definición anterior releva la importancia que tiene la información dentro de la IoT, ya que obtenerla es su finalidad. El valor de la información, sobre todo la personal, es innegable dentro de la sociedad del conocimiento; las empresas la buscan para tomar decisiones más eficientes y obtener mayores ventajas competitivas, el gobierno para ejecutar mejores políticas públicas, y las mismas personas para contar con mayores beneficios o comodidades en su vida cotidiana. Basta con constatar cómo las personas llevan sus teléfonos inteligentes a todas partes y comparten sus vidas en las redes sociales para evidenciar que estamos viviendo una penetración creciente de la tecnología en las vidas privadas y públicas de las personas que permite la recolección de datos y, con ello, la identificación, registro y perfilamiento de las personas.[11]

10. El Parlamento Europeo (2010) ha indicado que la «internet de los objetos» se refiere al concepto general de objetos (tanto artefactos electrónicos como objetos de uso cotidiano) que se pueden leer, reconocer, dirigir, localizar o controlar a distancia a través de Internet.

11. Véase Ziegeldorf, García Morchon y Wehrle (2013). Como señala Solove y

APLICACIONES IOT Y SU CLASIFICACIÓN

Las potencialidades que ofrece la IoT hacen posible el desarrollo de una enorme cantidad de aplicaciones, las cuales, sólo en una pequeña parte, se encuentran disponibles actualmente. El conocer y clasificar estas aplicaciones o usos de la IoT facilita, a los efectos del presente trabajo, entender más cabalmente su alcance y contenido; asimismo, permite establecer las fronteras respecto a aquellos usos que pueden constituir una amenaza a la privacidad de aquellos que no, debido fundamentalmente a que no tratan información personal.

- Salud: Dispositivos insertos en el cuerpo humano o adjuntos a él que sirven para monitorear y mantener la salud y el bienestar humano, a través del registro y medición de ingesta de calorías, ejercicio físico, horas de sueño, números de pasos, entre otros, o gestionar enfermedades de pacientes crónicos, a través del monitoreo de los latidos del corazón, los niveles de insulina u otros indicadores de salud.
- Ambientes inteligentes: Sensores y aplicaciones que permiten contar con hogares y oficinas inteligentes que pueden hacer la vida más confortable en varios aspectos. La temperatura de las piezas puede ser adaptada a las preferencias de sus usuarios y al clima; la luz puede ser cambiada de acuerdo a la hora del día; la energía puede ser ahorrada automáticamente apagando los aparatos eléctricos cuando no se usan o a cierta hora del día. Asimismo, en el ámbito de seguridad se puede contar con alarmas automáticas en caso de

Schwartz (2009: 1): «Vivimos en un mundo conformado por tecnología y lleno de información. Herramientas tecnológicas, como teléfonos, video y audio, computadores e internet, han revolucionado nuestra habilidad para capturar información sobre el mundo y comunicarla. La información es el alma de la sociedad actual. Crecientemente, nuestras actividades diarias envuelven transferencia y registro de información. El gobierno recolecta vastas cantidades de información personal en registros relativos al nacimiento, matrimonio, divorcio, propiedades, procedimientos judiciales, vehículos motorizados, votaciones, actividades criminales, licencias profesionales y otras actividades. Las entidades del sector privado también amenazan gigantescas bases de datos de información personal con finalidades de marketing o de historial crediticio. Donde quiera que vayamos, lo que sea que hagamos, podemos fácilmente dejar una huella de datos que es registrada y compartida».

movimiento de objetos valiosos, que avisan inmediatamente a un teléfono inteligente o a otro dispositivo de tal movimiento.

- Industrias manufactureras: Empresas con rutina de trabajo repetitivas pueden optimizar equipos e inventario al utilizar aplicaciones IoT, en particular, usando etiquetas RFID asociadas a partes de la producción y así lograr eficiencias operativas.
- Transporte: Respecto de vehículos, incluyendo autos, camiones, embarcaciones, aviones, y trenes, se puede manejar a través de dispositivos la información necesaria que permita establecer su condición de mantenimiento, uso basado en el diseño o análisis de preventa. Por otra parte, respecto del transporte, es posible que los usuarios tengan un conocimiento y gestión más adecuada del tráfico de buses o locomoción colectiva, ya que pueden conocer de antemano, a través de dispositivos insertados en estos medios de transporte, cuán cerca del paradero se encuentran, cuánto demorará el recorrido, entre otra información de utilidad.
- Medio ambiente: La integración inteligente de aplicaciones descentralizadas de medición de eficiencia de fuentes de energía renovables, de uso de redes eléctricas y consumo de energía proporcionan una retroalimentación constante para las empresas de distribución y clientes, en orden a equilibrar las actividades de suministro y demanda.
- Consumo personal: Aplicaciones avanzadas conectadas que ofrecen contenido personalizado de todos los puntos de contacto con clientes en varios ámbitos, desde el comercio minorista al entretenimiento, ofreciendo nuevos métodos de pago o entregando al cliente información más oportuna y cercana respecto a opciones de compra en base a sus preferencias previamente declaradas o concluidas de su comportamiento.
- Redes sociales: Aplicaciones que se relacionan con la actualización automática de información acerca de actividades sociales en estas redes, por ejemplo, aplicaciones que generan eventos acerca de la gente y lugares, que entregan a los usuarios actualizaciones en tiempo real, las cuales luego pueden ser compartidas y subidas a internet. Las interfaces de las aplicaciones despliegan una serie de

Figura 2.

eventos que sus usuarios han preliminarmente definido junto a los otros usuarios que pueden acceder a dichos eventos.

La figura 2 grafica la clasificación de aplicaciones IoT según su naturaleza o finalidad, y distinguiendo entre ellas las que son más intensivas en uso de información personal.

ECOSISTEMA DE LA IOT

El ecosistema de la IoT está determinado por la compleja relación que existe entre los diversos actores y elementos que lo conforman. Es compleja ya que no solamente existe un tipo de proveedor único y un usuario típico de esta tecnología, sino que existe una variedad de proveedores y usuarios, que además se ven influenciados por elementos exógenos al mercado propiamente tal, como son los aspectos tecnológicos y legales, junto con considerar que existen diferentes estados de tratamiento de datos personales en este ecosistema, como se muestra en la figura 3.[12]

12. Para mayor información respecto del ecosistema de la IoT, véase IDC y TXT (2014), Article 29 Working Party (2014), Ziegeldorf, García Morchon y Wehrle (2013) y Perera, Ranjan y otros (2015).

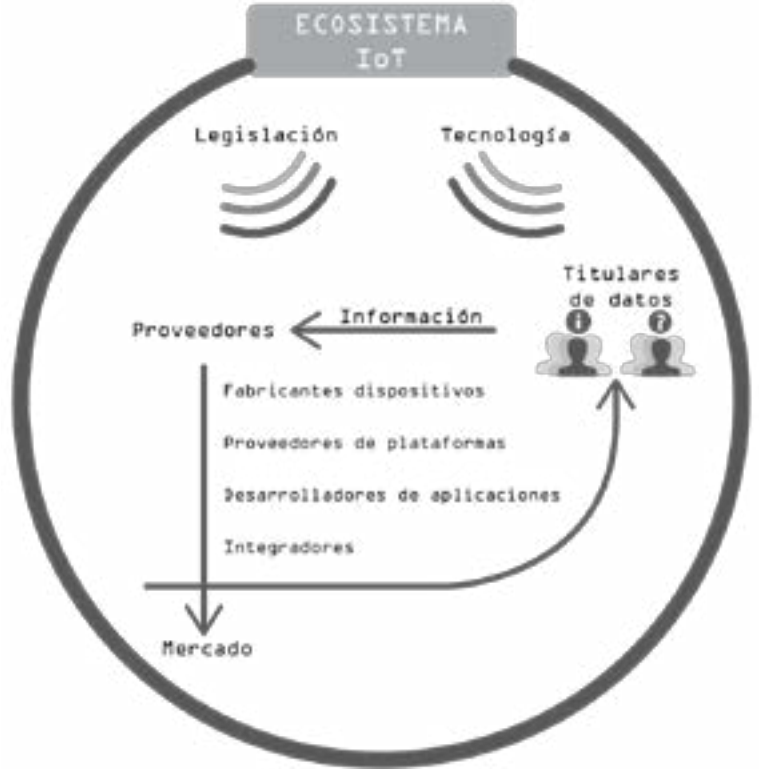

Figura 3.

Actores

Titulares de datos personales

Este artículo entiende que son titulares de datos personales, aquellas personas naturales que entregan información que les concierne, ya sea de forma consentida o no, mediante las aplicaciones IoT, a los proveedores de estas soluciones.[13]

13. Cabe señalar que en Chile, conforme al artículo 2 letra ñ) de la Ley 19.628 sobre Protección a la Vida Privada, es titular de datos personales la persona natural a la que se refieren los datos de carácter personal. A su vez, datos personales o de carácter personal son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables conforme el artículo 2 letra f) de la referida ley. Nuestra legislación opta por no comprender a las personas jurídicas, como sí lo han hecho otros ordenamientos, como, por ejemplo, el argentino. Esto, debido a que nuestro legislador entiende que la intimidad y la vida privada son derechos que le corresponden en propiedad a las personas naturales y no a las jurídicas, a las cuales se les puede proteger por

En el ecosistema de la IoT, son los derechos a la privacidad y a la protección de los datos personales de estos sujetos los que pueden verse afectados.

Proveedores

Dentro de la categoría de proveedores del ecosistema de IoT, se encuentran los siguientes:

- Fabricantes de dispositivos: Se trata de aquellas empresas que proveen los dispositivos o equipos físicos que captan la información. Estos fabricantes no sólo se encargan de proveer el hardware, sino que también pueden haber desarrollado o modificado el sistema operativo del dispositivo o software para determinar su funcionalidad en general, incluidos los datos y la frecuencia de recogida, o cuándo y a quién se transmiten los datos. En realidad, la mayor parte de estos proveedores recogen y procesan los datos personales que se generan por el dispositivo, con la finalidad y por los medios que ellos mismos han determinado (Article 29 Working Party, 2014).
- Proveedores de plataforma: Acá se incluyen aquellos proveedores que ofrecen los servicios de alojamiento de las aplicaciones o software IoT. Tales plataformas pueden ser servicios en la nube[14]

---

otras vías, como, por ejemplo, por vía de reserva o secreto. A este respecto el Primer Informe de la Cámara de Diputados indicó: «En principio, el concepto de dato personal —y más aún el de intimidad— no es aplicable a las personas jurídicas y, por tanto, sus datos podrán ser siempre conocidos, pues prima el derecho a la información. Otra cosa será lo que se regule respecto del secreto comercial o industrial, por ejemplo». Informe de la Comisión de Constitución, Legislación y Justicia recaído en el proyecto de ley sobre protección a la vida privada, Cámara de Diputados, segundo trámite, sesión 3, pág. 152, 4 de junio de 1996. No obstante lo anterior, cabe consignar que han existido algunas iniciativas legales en orden a incorporar a las personas jurídicas dentro del ámbito de aplicación de la ley. Es el caso, por ejemplo, del Boletín 2422-07 que «Establece normas sobre protección de la información de las personas jurídicas».

14. La ITU (2014) ha definido a los servicios en la nube como «una o más capacidades ofrecidas a través de *cloud computing* utilizando una interfaz declarada», y al *cloud computing* como «un paradigma que permite el acceso a la red a una cantidad escalable y elástica de recursos físicos y virtuales que se pueden compartir con el aprovisionamiento y la administración bajo demanda y autoservicio».

o servidores físicos locales. La problemática que ha sido detectada respecto de estos actores es que debido a la falta de estandarización y la interoperabilidad, cada fabricante ha definido su propio conjunto de interfaces y formatos de datos que se encuentran alojados en servidores físicos no virtuales, lo que impide de manera efectiva la transferencia de datos desde un dispositivo a otro. Sin embargo, los teléfonos inteligentes y las tabletas se han convertido en las pasarelas naturales de los datos recogidos a través de muchos dispositivos IoT a internet. Como resultado, los fabricantes han desarrollado progresivamente plataformas que tienen como objetivo almacenar los datos recogidos a través de estos distintos dispositivos con el fin de centralizar y simplificar su gestión.

- Desarrolladores de aplicaciones IoT: Para que la tecnología IoT funcione, se requiere de instrucciones, de programas computacionales, de aplicaciones, las que usualmente en este ecosistema son provistas por empresas que no caben dentro de las categorías anteriores, que suelen ser más pequeñas y que se dedican a desarrollar tales aplicaciones para los fabricantes de dispositivos IoT. Cuando los titulares de datos instalan estas aplicaciones de terceros o las utilizan, usualmente se les permite a estos desarrolladores acceder a sus datos, almacenados por el fabricante del dispositivo.
- Integradores: Son empresas que comercializan directamente al usuario final estas tecnologías integrando todos los servicios IoT, es decir, proveen el dispositivo, las aplicaciones y la plataforma en donde se alojan. Los integradores, a su vez, pueden ser generadores directos de estas tecnologías o subcontratarlas a otros proveedores.

Elementos exógenos

La legislación

El ecosistema de la IoT es influenciado por la legislación. Desde una perspectiva general, la literatura, gobiernos y organismos internacionales apuntan a que esta legislación debiera, mediante incentivos a la autorregulación o derechamente estableciendo deberes y obligaciones, regular principalmente los aspectos que a continuación se mencionan, con

el objeto de estimular el desarrollo de la IoT asegurando un crecimiento continuo debido principalmente a la calidad de sus servicios y generación de confianza en el consumidor (cf. International Telecommunication Union, 2015; Weber y Weber, 2010; Federal Trade Commission, 2015; Weber 2009).

- Competencia: Asegurar la libre competencia, considerando que algunas configuraciones del mercado de los servicios IoT, podrían fortalecer la posición de grandes empresas y aumentar el potencial de dependencia de los consumidores de los servicios IoT de esas empresas. Por otra parte, el acceso limitado a los datos por parte de los consumidores reduce la capacidad de cambiar de proveedor y de entender las implicancias en materia de privacidad.
- Como parte de las políticas públicas en materia de telecomunicaciones se debiera gestionar y licenciar el espectro de manera de asegurar que éste esté disponible para una amplia gama de aplicaciones de la IoT, a corto y largo plazo, y en bandas con licencia y sin licencia.
- Privacidad: La regulación debiera establecer obligaciones y principios claros en materia de protección de datos personales, de manera de asegurar que se respetará la privacidad del consumidor.
- Requerimientos de infraestructura: La infraestructura de la IoT debiera, al menos, cumplir con cuatro características: ser robusta, tener alta disponibilidad, confiabilidad e interoperabilidad.
- Seguridad: Se debieran establecer incentivos normativos para que la seguridad forme parte del diseño de la IoT y se establezcan procesos previos de testeo.
- Transparencia: De manera de permitir que los consumidores estén informados del funcionamiento de los servicios IoT, y de las consecuencias de sus acciones, lo que incluye características como claridad, certeza, accesibilidad, exactitud y veracidad.

La tecnología

Asimismo, el ecosistema IoT se ve influenciado en su alcance y posibilidades de expansión por las diversas tecnologías que actualmente se

relacionan con él o le dan sustento, junto con los diversos impactos que pueden tener ellas en la privacidad (cf. IDC y TXT, 2014; De Filippi, 2014; Cisco, 2014), a saber:

- *Big data*:[15] El creciente número de dispositivos conectados a sistemas inteligentes que pueden compartir, procesar, almacenar y analizar los datos entre sí dará lugar a miles de millones de máquinas y cosas conectadas a las redes, creando aún más datos. Como resultado de ello, el análisis y técnicas inteligentes de gestión de datos tendrán que ser desplegados para obtener un resultado significativo de esta inmensa cantidad de datos.
- *Cloud computing*: Dada las características de esta tecnología constituye una clave para contribuir al crecimiento presente y futuro de la IoT.
- Infraestructura de red: Desarrollos de red (como por ejemplo LTE[16]) y despliegues de redes de células pequeñas han hecho cada vez más omnipresente la conectividad, ya sea mediante el uso de redes de área personal (por ejemplo, 6LoWPAN o Bluetooth), redes de área local inalámbricas (WiFi), o redes de área amplia (celular), además de la conectividad por cable (xDSL, fibra, etcétera). Esta capacidad de conectar cualquier cosa en cualquier momento está ayudando a hacer de la IoT una realidad.
- Sensores/actuadores:[17] Se trata de dispositivos físicos que se co-

15. El concepto de *big data* se refiere a la recolección y acumulación de grandes cantidades de datos producida por y sobre las personas, cosas o las interacciones entre ellas (cf. De Filippi, 2014).

16. *Long erm Evolution* o evolución a largo plazo es una estándar de la norma 3GPP y que se entiende como una evolución de la norma 3G, la 4G, y que en términos sencillos permite a los usuarios de dicha tecnología navegar por internet a mayor velocidad y tener una mejor experiencia de uso de datos.

17. Un sensor de entrada puede medir una variable de forma análoga, o un valor discreto (temperatura, humedad, etcétera). Por otra parte, se pueden utilizar sensores que miden una variable dicotómica del tipo sí/no (se detectó humedad sí/no, alta temperatura sí/no, etcétera). Los actuadores son dispositivos que se accionan ante una solicitud para controlar el estado de una variable y normalmente son del tipo sí/no. Un ejemplo simple es un termostato: se elevó la temperatura entonces se enciende el sistema de refrigeración y mantengo el estado de la variable en un valor prefijado. Véase Cisco (2014).

nectan con el entorno entregando la información que recaban al ecosistema IoT, como, por ejemplo, medidores de temperatura, presión, polución, velocidad, frecuencia, calidad, dirección, peso, movimiento, luminosidad, energía, saturación, estrés, tiempo, ruido, GPS, entre otros. En el futuro, este tipo de sensores pueden insertarse dentro del cuerpo humano, por ejemplo, para detectar síntomas de enfermedades.

Etapas del tratamiento de datos personales

Entendiendo al tratamiento de datos personales en un sentido amplio,[18] se advierten las siguientes principales etapas o estados del tratamiento de datos en el ecosistema IoT:

- Recogida de datos: Esta etapa inicial requiere que la tecnología IoT de que se trate, como un sensor por ejemplo, extraiga datos personales de un determinado sujeto que haya interactuado de alguna forma con dicha tecnología, ya sea en forma activa o pasiva, es decir, con o sin consentimiento/conocimiento. Una vez recogidos tales datos, éstos son transferidos a través de redes, ya sean públicas o cerradas.
- Procesamiento de datos: Se efectúa por parte del proveedor del servicio respectivo, el análisis y cruce de los datos recogidos, con el objeto de obtener un determinado resultado valioso de la información.
- Perfilamiento: Eventualmente un resultado de la etapa de procesamiento de datos, será la creación de un perfil del usuario respectivo, es decir, el establecimiento de determinados rasgos peculiares

18. La Ley 19.628 sobre Protección a la Vida Privada define al tratamiento de datos personales como «cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma». De la definición legal destaca que se trata de un concepto amplio y genérico, dada la utilización del vocablo «cualquier» y de la frase «o utilizarlos en cualquier otra forma» y que comprende diversas acciones de carácter técnico a título ilustrativo. La amplitud de la definición hace que la referida ley se aplique a cualquier operación que permita utilizar datos personales de alguna forma.

que caracterizan a ese usuario, usualmente vinculados con preferencias de consumo o determinadas conductas.

- Entrega de datos: Luego, los datos obtenidos de las etapas de tratamiento anteriores son entregados ya sea al mismo usuario o a terceros, en este último caso, hablamos de comunicación o transmisión de datos.[19]

PROBLEMÁTICA DE LA IOT

LA IOT, ¿UNA NUEVA AMENAZA A LA PRIVACIDAD?

Habiendo ya revisado las principales características y alcance de la IoT, se procede a continuación a explorar por qué se señala que esta tecnología puede constituir una amenaza a la privacidad.

A este respecto, cabe señalar que la literatura y la opinión de organismos tanto no gubernamentales como gubernamentales declara que la IoT constituye una amenaza para la privacidad,[20] opinión a la cual adherimos. La disyuntiva radica en determinar si se trata de una nueva amenaza con características diversas a las que conllevan en general las tecnologías, o bien, si estamos en presencia de un avance tecnológico que no trae consigo distintas amenazas a las ya existentes en materia de privacidad. La gran mayoría escoge la primera opción, es decir, se inclina por señalar que la IoT constituye una nueva amenaza para la privacidad y la protección de datos personales en base a argumentos como los siguientes: se indica que las nuevas formas de interacción que

19. La Ley 19.628 indica en su artículo 2 letra c) que la «comunicación o transmisión de datos es dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas». La definición legal es bastante amplia por lo que debemos entender que constituye comunicación cualquier operación que implique poner en conocimiento los datos personales a un tercero, ya sea en forma gratuita u onerosa; ya sea a través de la entrega de un soporte físico o a través del envío de los registros en formato digital por una red, o permitiendo la sola visualización; ya sea permitiendo que la persona a la cual se comunican los datos efectúe a su vez tratamiento de dichos datos o no.

20. Esto cuando la información que se trata es personal, cosa que no ocurre, por ejemplo, en el caso de tecnología de comunicación M2M *(machine to machine)* aplicada a la mejora de la eficiencia de inventario en una fábrica, por ejemplo.

envuelven a la IoT conducen a amenazas y desafíos específicos y distintos para la privacidad (cf. Ziegeldorf, García Morchon y Wehrle, 2013): que los peligros ocultos de la IoT plantean importantes desafíos para la seguridad de la información y la privacidad personal, porque en varias ocasiones la IoT necesita utilizar transmisión por *wireless* , dicha exposición de señales en lugares públicos puede ser fácilmente accedida (Zhang y Ye, 2010); que mientras los problemas tradicionales de privacidad en internet surgen mayormente para los usuarios que juegan un rol activo, en la IoT estos problemas surgen incluso para las personas que no usan un servicio IoT (cf. Atzori, Iera y Morabito, 2010); que la IoT genera un intercambio constante e invisible de datos entre cosas y personas, y entre cosas y otras cosas, lo que ocurre sin conocimiento de los dueños y originadores de tales datos (International Telecommunication Union, 2005); que tecnologías IoT como Google Glass, Apple iWtach, Google Fit, Apple Health Kit, y Apple Home Kit, pueden recolectar información sensible de sus usuarios desde condiciones de salud hasta actividades diarias (cf. Perera, Ranjan y otros 2015); o que la IoT es alta en cantidad, calidad y sensibilidad de los datos que recoge, lo que significa que las inferencias que de su uso pueden extraerse son más grandes y sensibles, y la identificación se hace más probable (36th International Conference of Data Protection and Privacy Commissioners, 2014).

Este artículo plantea que efectivamente la IoT manifiesta especificidades como las ya señaladas por la literatura, sin embargo éstas no constituyen nuevas o distintas amenazas a la privacidad o a la protección de datos personales, sino que más bien ellas se acentúan en su magnitud y eventuales efectos lesivos, como se ejemplifica a continuación:[21]

- Perfilamiento: Busca deducir los intereses de las personas creando

21. En este sentido, Escribano (2014: 1-2) señala que los desafíos de la IoT en materia de privacidad se ven amplificados por algunas de sus características, como las siguientes: la cadena de valor de la IoT es larga y compleja con un número significativo de actores; las combinaciones y comunicaciones de datos a través de servicios en la nube incrementan los lugares y jurisdicciones en donde reside la información personal; o que el exponencial volumen de datos que puede ser recolectado, y sus posterior cruce y almacenamiento en la nube y el uso de herramientas de análisis predictivo, puede transformar la información personal en algo útil pero también permite a las compañías tener perfiles muy detallados de nuestras vidas.

un perfil de ellas, mediante la correlación de datos con otros perfiles y datos. Actividades que a partir del perfilamiento son vulneratorias de la privacidad son la discriminación arbitraria de precios, publicidad no solicitada, decisiones automáticas erróneas por *credit scoring*.[22] La IoT agrava este problema ya que conduce a una explosión de las fuentes de datos a medida que más y más cosas se conectan (aspecto cuantitativo), y, por otra parte, se recogen datos de la vida privada de las personas que antes eran inaccesibles (aspecto cualitativo) (cf. Ziegeldorf, García Morchon y Wehrle, 2013).

- Localización y rastreo: Mediante dispositivos como GPS (Global Positioning System), tráfico de internet o celdas de telefonía móvil es posible localizar y rastrear a una persona considerando tiempo y espacio, permitiendo conocer, en consecuencia, qué lugares visita y en qué horarios, lo que puede llevar a revelar información sensible, como una enfermedad, por ejemplo (cf. Chow y Mokbel, 2009), o a sentirse permanentemente vigilado (Toch, Wang y Faith, 2012). Estas tecnologías si bien son previas a la IoT, revisten especial importancia en ella ya que son utilizadas con intensidad en sus aplicaciones. Se señala que la IoT cambia y agrava esta amenaza de tres maneras. En primer lugar, se observa un uso creciente de servicios basados en localización (LBS),[23] ya que las tecnologías de la IoT no sólo apoyan al desarrollo de este tipo de LBS y mejoran su exactitud, sino que también amplían los servicios en los ambientes de interior, por ejemplo, efectuado análisis de preferencias de visita en el *retail*. En segundo lugar, como la recolección de datos es

22. El *credit scoring* o modelos de calificación crediticia se caracterizan por utilizar una gran cantidad de bases de datos a objeto de entregar un resultado estadístico útil y, en ocasiones, determinante en la evaluación y otorgamiento de un crédito (Gambi Moreira, 2004).

23. Los servicios basados en localización son servicios de información y entretenimiento que son de fácil acceso por los usuarios móviles a través de dispositivos portátiles con GPS y las redes móviles (por ejemplo, 2G/3G de telefonía móvil y redes WiFi). Ejemplos de LBS incluyen hallazgo de recursos (por ejemplo, ¿dónde está mi gasolinera?), búsqueda de rutas (por ejemplo, ¿cuál es la ruta más corta de mi ubicación actual a un centro comercial?), las redes sociales (por ejemplo, ¿dónde están mis amigos?), y la ubicación y juegos (por ejemplo, GPS juego en línea) (cf. Chow y Mokbel, 2009).

más pasiva, más penetrante y menos intrusiva, los usuarios pueden ser menos conscientes de cuándo se está efectuando localización y rastreo, y los riesgos que ello implica.[24] En tercer lugar, la creciente interacción con los objetos y los sistemas inteligentes deja rastros de datos que no sólo ponen al usuario en riesgo de identificación, sino que también permiten hacer un seguimiento de su ubicación y actividad (cf. Ziegeldorf, García Morchon y Wehrle 2013).

- Cruce de información personal: Mediante cruce de información personal que se encuentra en distintas bases de datos se revela información (veraz o errónea) que el sujeto no dio a conocer a los titulares de las referidas bases consideradas aisladamente. La vulneración a la privacidad se consuma, por ejemplo, cuando datos que se encontraban disociados,[25] mediante este cruce se vuelven personales, o cuando la información ha sido revelada inicialmente con una determinada finalidad, después del cruce se desvirtúa o se pierde. A este respecto es posible señalar que esta amenaza se agrava debido a la existencia de diversos proveedores en el sistema de la IoT que pueden compartir o cruzar información de forma no consentida (cf. Ziegeldorf, García Morchon y Wehrle, 2013).
- Datos sensibles: Si bien desde los orígenes del tratamiento de datos personales se han recogido y utilizado datos sensibles,[26] las

24. En este mismo sentido, la Declaración de Mauricio sobre la Internet de las Cosas, indica: «El sensor de datos del internet de las cosas es alto en cantidad, calidad y sensibilidad. Esto significa que las inferencias que de ello puedan extraerse son más grandes y sensibles, y la identificación se hace más probable. Considerando que la identificabilidad y la protección del *big data* (metadatos) son ya retos importantes, está claro que el *big data* derivado de los dispositivos del internet de las cosas hace que este reto sea aún mucho más grande. Por tanto, esta información debe ser considerada y tratada como datos personales» (International Conference of Data Protection an Privacy Commissioners, 2014).

25. La Ley 19.628 en su artículo 2 e) define al dato estadístico como el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable, y que en consecuencia, al no ser un dato personal, no se le brinda la protección que entrega la ley.

26. Según el artículo 2 letra g) de la Ley 19.628 sobre Protección a la Vida Privada, datos sensibles son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad,

aplicaciones que ofrece la IoT generan una mayor probabilidad de vulneración a la privacidad, por ejemplo: la domótica o el *quantified self*.[27] En el primer caso, se está en presencia de un conjunto de sistemas que automatizan las diferentes instalaciones de una vivienda, mediante el uso de dispositivos inteligentes que permiten registrar información y su envío a través de internet, como, por ejemplo, cuándo se enciende la luz, cuándo se lava, qué se saca del refrigerador, cuál es la temperatura deseada, cuándo se está en casa, alarmas de humo, cuándo se enciende la televisión y los programas vistos, cámaras que graban movimientos y registran sonidos e interactúan con las personas cuando éstas no se encuentran en el hogar. Toda esta información es enviada a través de internet a los usuarios pero también a los otros actores del sistema IoT. En el segundo caso, se está en presencia de ciertos dispositivos que permiten medir patrones usualmente asociados a la salud, como, por ejemplo, la cantidad de pasos que una persona camina diariamente, sus patrones de sueño (cuántas veces se despierta, se levanta o duerme profundo), calorías quemadas, ritmo cardíaco o de la respiración, nivel de estrés, entre otros muchos datos sensibles, los que luego de ser registrados y analizados son informados no solamente al usuario, sino que también a uno o más de los actores del ecosistema de la IoT.

LAS FALENCIAS DEL SISTEMA

Las amenazas ya revisadas se concretan en vulneraciones a la privacidad y, en particular, a la protección de datos personales, cuando concurren una o más de las siguientes circunstancias, que constituyen las falencias del ecosistema de la IoT.

a) Asimetría de información: Peter Swire (1997) entrega una doble

tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual; por ejemplo: fichas clínicas, registros penales, registros de afiliación sindical o política, costumbres de navegación en internet, por nombrar sólo algunos.

27. Se trata de cosas que son diseñadas para ser regularmente llevadas por individuos que desean registrar información acerca de sus propios hábitos y estilos de vida (Article 29 Working Party, 2014).

visión de las fallas del mercado. Por una parte, indica que el fracaso del mercado se ha definido con respecto a los derechos humanos y, por otra, respecto de enfoques contractuales a la protección de información personal. Bajo los derechos humanos, la meta es proteger el derecho de los individuos a la privacidad según la teoría moral que define el derecho. El mercado fallará cuando proteja la privacidad menos de lo que es deseable bajo la teoría moral. Bajo el enfoque contractual, la meta es que todos los individuos tengan igual nivel de información y, por lo tanto, tengan igual poder de negociación. En este sentido, para el autor el mercado generalmente falla debido a las asimetrías de información entre el que efectúa el tratamiento de datos y el titular de ellos. Así, señala que «los costos de información se presentan debido a la asimetría de información existente entre la empresa y el consumidor, la empresa generalmente sabe mucho más que el consumidor sobre cómo la información será usada por la empresa» (1997: 3-4) y, por otra parte, reconoce la existencia de altos costos de transacción al señalar que «el consumidor puede enfrentar costos significativos por el simple hecho de tratar de entender la naturaleza de las políticas de privacidad de una empresa» (1997: 4).

Como señala la Comisión de la Unión Europea (2015a), que los consumidores no sepan qué datos suyos son recolectados y cómo son usados, constituye una asimetría de información entre los actores del mercado, lo que puede interferir con sus derechos fundamentales a la privacidad y a la protección de datos personales y puede resultar en una violación al derecho a no ser discriminado. En el ámbito específico de la IoT, esta falla de mercado se encuentra muy presente, ya que al existir diversos actores y eventuales usos subsecuentes de los datos personales, la probabilidad que los titulares no tengan conocimiento respecto de quién y cómo se tratan sus datos, es mayor.

b) Ausencia de control sobre la información personal: Íntimamente vinculada con la falencia anterior, es la falta de control sobre la información personal, ya que si no se cuenta con información adecuada, mal podrán los titulares de ella efectuar un control efectivo sobre sus datos personales que poseen terceros.[28] A este respecto, el WP29 ha indicado

28. Entendemos que el control de datos personales se efectúa mediante el ejercicio de dos herramientas, a saber: la autorización o consentimiento en el tratamiento de datos

que los datos recogidos por servicios IoT pueden no estar adecuadamente sujetos al control del titular de los datos antes de su publicación, lo que sin duda genera un riesgo de falta de control y autoexposición excesiva para el usuario. Además, la comunicación entre objetos puede ser activada de forma automática, así como por defecto, sin que el individuo sea consciente de ello.

Sin la posibilidad de controlar eficazmente cómo interactúan los objetos o de definir límites virtuales mediante la definición de zonas activas o no activas para cosas específicas, será extraordinariamente difícil controlar el flujo de datos generado y aun más difícil de controlar su utilización posterior (Article 29 Working Party, 2014).

c) Consentimiento inexistente o ineficaz: Por una parte, hay ocasiones en que las personas no saben que se está efectuando tratamiento de sus datos personales por una tecnología IoT (como, por ejemplo, el caso de las personas cuyas imágenes son captadas por los Google Glasses o por drones) en donde claramente si no existe conocimiento, mal puede haber consentimiento. En cambio, habrá otras ocasiones en que si bien formalmente el titular de los datos personales pudo haber otorgado su consentimiento al tratamiento, tal consentimiento es ineficaz porque no es de calidad (libre e informado) o tiene vicios que lo hacen nulo; por ejemplo, en aquellas ocasiones en que se presume que el consumidor ha dado su consentimiento sin que éste haya sido expreso e informado, como ocurre en los *wraps agreement*.[29]

d) Malas prácticas de los actores de la IoT: Obviamente el sistema falla si los actores de la IoT ejecutan malas prácticas, como no recabar el consentimiento de los titulares de datos personales cuando se debe hacer

---

personales y mediante el ejercicio de los derechos subjetivos del titular de los datos reconocidas en la ley, que, en el caso de Chile, son el derecho de información, de modificación, de bloqueo y de cancelación de los datos personales.

29. Se trata de contratos en que el consentimiento del consumidor se presume por abrir el paquete que contiene el producto o haber visitado una determinada página o sitio web (usualmente se refiere a licenciamientos). Respecto de esta materia, la Ley 19.496 sobre Protección a los Derechos de los Consumidores establece en el inciso segundo del artículo 12 A, que «la sola visita del sitio de internet en el cual se ofrece el acceso a determinados servicios, no impone al consumidor obligación alguna, a menos que haya aceptado en forma inequívoca las condiciones ofrecidas por el proveedor», es decir, se exige que exista una consentimiento expreso por parte del consumidor.

conforme la legislación vigente; no tener políticas claras y transparentes en materia de privacidad y datos personales; comunicar a terceros los datos personales sin autorización o conocimiento del titular; darle un uso a los datos distinto de la finalidad para el cual fueron recabados, falta de información a los consumidores, entre otros. Lo anterior, no sólo constituye una vulneración a los derechos de privacidad y protección de datos personales, sino que junto con ello no se cumple uno de los requisitos básicos para el asentamiento y crecimiento de esta tecnología, como ya se mencionara anteriormente en este artículo.

SOLUCIONES

MODELOS DE PROTECCIÓN

Se han planteado en la literatura diversos modelos de protección frente a la amenaza que genera la IoT a la privacidad y a la protección de datos personales, los que consideran uno o más de los siguientes elementos:

a) Legislación: Ya sea local o regional que reconoce el derecho fundamental a la privacidad y a la protección de datos personales, creando el marco regulatorio y normativo que establece los requisitos para que un tratamiento de datos personales se considere legítimo.

A este respecto, las preguntas que se debieran resolver si se considera necesario contar con legislación en la materia, serían las siguientes: ¿Es necesaria una ley orgánica en materia de protección de datos personales, ya sea internacional o nacional, o basta con leyes sectoriales que regulan los diversos mercados? Si la legislación ya existe, ¿es necesaria una nueva legislación para la IoT, o es suficiente con la ya existente? Y si es necesaria una nueva legislación, ¿qué tipo de ley y con qué alcance se necesita? (Weber y Weber, 2010).

b) Autorregulación: Existe autorregulación cuando los sujetos destinados a cumplir con las normas o reglas las dictan y se obligan a cumplirlas. La autorregulación no estará acompañada de legislación cuando se estructura exclusivamente en base a un modelo de control social, en el cual la sociedad sanciona a los autorregulados cuando no cumplen las normas autoimpuestas, mediante su exclusión del mercado o disminución de ventas. La autorregulación también puede ir acompañada de la legislación, en aquellos casos en que ésta la contemple como una vía

para promocionar el cumplimiento de la norma, o bien cuando los mismos sujetos normados encuentran en la autorregulación una vía efectiva para evitar la sobrerregulación.[30]

c) Gobierno y legislación internacional o global: Dada la naturaleza supranacional de la IoT, que se basa en internet y utiliza intensamente los servicios en la nube, se ha planteado la conveniencia de contar con un gobierno y legislación internacional que regule y dicte las normas que los actores IoT deberán cumplir (Weber y Weber, 2010; Federal Trade Commission, 2015).

d) Tecnología: Como indican Jing Zhang y Liuqui Ye (2010), los nuevos problemas causados por la tecnología aún dependen de la misma tecnología, por lo que las amenazas de la IoT requieren de nueva ciencia y tecnología para resolverlas. Estos autores plantean que la actual tecnología de la protección a la privacidad personal formada en la era de internet y en otras áreas tiene un cierto grado de desarrollo, que provee una base sólida para asegurar la protección de la privacidad en la era de la IoT.

PROPUESTA DE MODELO DE PROTECCIÓN

Para enfrentar la problemática planteada, se debiera no sólo pensar en buscar una solución desde la legislación, sino más bien buscar una forma de resolver el asunto sistémicamente, es decir, integrando las diversas herramientas disponibles (técnicas, legislativas, económicas y sociales) con el objeto de ir utilizándolas selectiva pero conjuntamente para abordar las falencias detectadas, como se grafica en la figura 4.

Estas herramientas debieran ser utilizadas durante todas las fases del tratamiento de datos personales[31] y estar presentes desde que se recaban

30. La Federal Trade Commission recomienda adoptar la autorregulación en el ámbito de la IoT; a este respecto se indica en el informe que la autorregulación y las mejores prácticas de negocio —que son tecnológicamente neutrales— junto con la educación del consumidor sirven como marco preferente para proteger la privacidad del consumidor y la seguridad, al mismo tiempo que mejoran la innovación, la inversión, la competencia y la libre flujo de información esencial para la internet de las cosas.

31. Toch, Wang y Faith (2012) establecen, en cambio, que según las diversas fases (recolección de datos, análisis de los datos, distribución de los datos) se deben tomar diversas medidas, ya que cada una de dichas fases implica retos distintos para la privacidad.

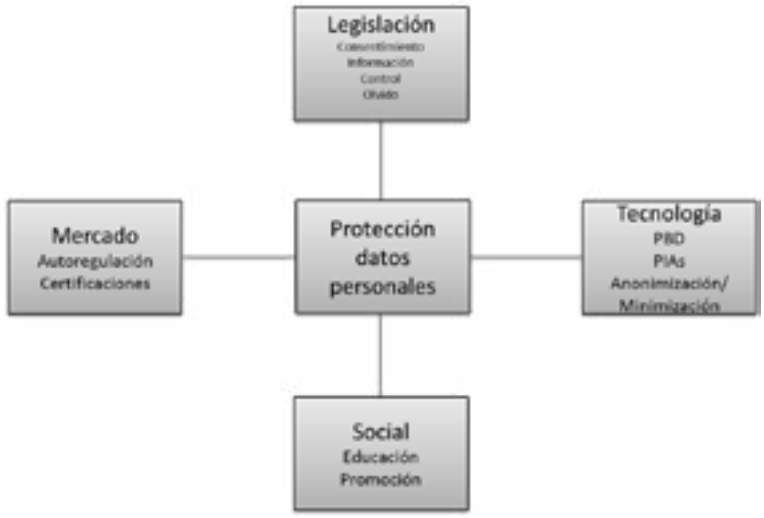

Figura 4.

los datos (International Conference of Data Protection an Privacy Commissioners, 2014).

La legislación

La legislación respecto de la IoT debiera cumplir con un objetivo que a primera vista podría entenderse como contradictorio: a saber, promover esta tecnología junto con proteger la privacidad de las personas. Creemos, en todo caso, que no existe tal contradicción, ya que para que exista un mercado sano y confiable en cualquier ámbito, y sobre todo teniendo presente el empoderamiento actual de los consumidores, es necesario que tales consumidores estén debidamente informados y en posesión de sus derechos.[32]

En esta materia, la normativa europea de protección de datos per-

32. En este sentido, el Parlamento Europeo ha indicado: «Una de las condiciones previas para la promoción de la tecnología es la de establecer normas jurídicas que refuercen el respeto de los valores fundamentales, así como la protección de los datos personales y la vida privada». Y también: «El desarrollo de nuevas aplicaciones y el propio funcionamiento y el potencial comercial de internet de los objetos estarán estrechamente ligados a la confianza que los consumidores europeos depositen en el sistema, [...] la confianza se obtiene cuando se aclaran las dudas sobre las posibles amenazas para la intimidad y la salud» (Parlamento Europeo, 2010).

sonales —que actualmente se encuentra en revisión— y los principios que la informan, constituyen un referente que es reconocido por toda la literatura. Excede el alcance de este trabajo referirse en detalle a la referida normativa y sus principios, no obstante lo cual sí se considera necesario y oportuno profundizar en la correcta aplicación de la norma y principios aplicables, respecto de los siguientes aspectos: consentimiento del titular de datos, información al titular de datos, control del titular de datos, y derecho al olvido.

a) Consentimiento del titular de los datos. El principio del consentimiento es uno de los más importantes en materia protección de datos personales. En base a él se establece que la regla general es que el titular de los datos debe prestar su consentimiento para que se pueda legítimamente efectuar tratamiento de su información personal, y las excepciones a este principio deben ser establecidas por una norma legal.[33] La exigencia de este consentimiento es la base sobre la cual se estructura el derecho a la autodeterminación informativa, el que busca que el tratamiento de datos se efectúe a partir de una decisión libre y voluntaria de las personas (Gozaini, 2001; Jervis, 2006). Lo anterior es, asimismo, reconocido en el ámbito de la IoT por la WP29 al indicar que el consentimiento es el primer principio legal que debe ser seguido por los proveedores de la IoT.[34]

Este principio recibe reconocimiento con mayor o menor fuerza en todas las legislaciones protectoras de datos, como, asimismo, en las declaraciones de organismos internacionales sobre los principios rectores que deben estar presentes en materia de tratamiento de datos personales.

A este respecto, este artículo plantea que el consentimiento debiera caracterizarse por ser:

- manifiesto, es decir, debe ser expreso, no puede presumirse o ser tácito;[35]

33. La importancia y cantidad de excepciones legales a la regla general del consentimiento del titular de los datos que se contienen en las distintas legislaciones, es un tema central que debe considerarse cuando se efectúe un análisis *in extenso* de este principio, cosa que escapa al objeto de este documento.

34. Véase para un estudio detallado de los requisitos del consentimiento en materia de datos personales, Article 29 Working Party (2011a).

35. No es consentimiento el basado en la inacción o el silencio del titular de datos.

- libre o exento de vicios del consentimiento, de manera que no exista error, engaño, intimidación o consecuencias negativas importantes para el interesado si no consiente;
- específico, ya que no caben consentimientos generales para efectuar tratamiento de datos, sin determinación exacta de la finalidad;
- informado respecto de las características principales del tratamiento;
- previo al tratamiento de datos consentido; y,
- revocable, el titular de datos debe poder dejar sin efecto su autorización, y una vez revocada se deben eliminar los registros respectivos.

Cabe agregar que en el ámbito de la IoT, dada la relevancia que revisten actividades como la personalización, el perfilamiento, el cruce de datos que generan nueva información respecto de la cual el titular de los datos no ha dado su consentimiento, es aconsejable establecer un sistema que permita fácilmente, tanto a los proveedores de la IoT como a los respectivos titulares, recabar y otorgar, respectivamente nuevos consentimientos una vez que vayan surgiendo nuevos datos. Por otra parte, este consentimiento debe ser entregado con las características ya revisadas tanto respecto del tratamiento inicial, como de eventuales cesiones o comunicaciones a terceros.

b) Información al titular de los datos. La legislación se debe preocupar de que la información llegue a los titulares de datos y que ésta sea de calidad, de manera de garantizarles la toma de decisiones informadas sobre el tratamiento de sus datos personales. Lo anterior requiere el uso de un lenguaje apropiado para que los titulares de datos entiendan lo que están consintiendo y con qué fines; el uso de un lenguaje legal o extremadamente técnico no cumple este requisito. Asimismo, la información debe ser clara y suficientemente visible para que no pueda ser pasada por alto, debe ser entregada realmente a los titulares de datos y no dejarla sólo disponible en algún lugar. Por otra parte, no basta con

Sobre todo en el ámbito de las aplicaciones, se debe considerar que no es válido el uso de casillas ya marcadas o tickeadas o la configuración del navegador de internet que establecen de forma predeterminada la autorización para recopilar datos personales.

sólo informar al momento de recabar los datos de la finalidad del tratamiento y si se cederán tales datos, como lo hace la legislación chilena, se debiera, asimismo, indicar si tal información llevará a tomar decisiones automatizadas, si se efectuará cruce de datos, si se efectuará perfilamiento o personalización.

Para disminuir la asimetría de información es además necesario que exista, por parte de los responsables del tratamiento de información, deberes activos de entrega de información, es decir, que no sólo estén obligados a informar al titular de datos cuando éste les requiera información acerca del tratamiento que de sus datos efectúan, sino que también se impongan la obligación de informar públicamente, por ejemplo, en los sitios web, si tratan datos personales, de qué tipo, con qué finalidad específica, por cuánto tiempo, si los datos se ceden a terceros, y a quiénes. Asimismo, se debiera generar un registro público de entidades, tanto públicas como privadas, que efectúan tratamiento de datos personales.

c) Control del titular de los datos. La legislación debiera entregar al titular de los datos las herramientas necesarias para que pueda ejercer un control real sobre su información personal. Como se ha indicado, ese control se concreta, por una parte, mediante la exigencia de consentimiento del titular de los datos para su tratamiento, el que debe cumplir con los requisitos ya revisados, y con excepciones al consentimiento específicas y fundamentadas (no abiertas, como ocurre con el concepto de fuente accesible al público que existe actualmente en la legislación chilena) y, por otra parte, mediante el otorgamiento de derechos subjetivos al titular de los datos, que le permitan a éste velar por el cuidado de la calidad de los datos, mediante el ejercicio de los derechos de modificación, oposición, eliminación, bloqueo de datos, cuando los datos de que se traten ya no den cuanta de la realidad[36].

d) Derecho al olvido. Mediante sentencia del Tribunal Europeo[37] en

36. En ese sentido se ha pronunciado el WP29, al indicar: «Aunque el consentimiento cumple un rol otorgando control a los titulares de datos, no es la única manera de hacerlo. La Directiva prevé otros medios de control, en particular, el derecho a oponerse, aunque éste es un instrumento diferente para ser ejercido en una etapa diferente del proceso, es decir, después de que el procesamiento se ha iniciado y se basa en un fundamento jurídico diferente» (Article 29 Working Party, 2011a).

37. Sentencia del fecha 13 de mayo de 2014 del Tribunal de Justicia de la Unión Europea.

el juicio de Google Inc. España contra la Agencia de Protección de Datos Española, ante el conflicto de derechos fundamentales que se produjo entre un sujeto que exigía que no se informara su nombre en las búsquedas efectuadas a través de Google, y esta empresa que indicaba que tenía el derecho a hacerlo, se falló indicando que el titular de los datos personales tiene el derecho de solicitar que la información no se ponga a disposición del público en general mediante su inclusión en lista de resultados, y que estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona.

El derecho al olvido que nace de la relación de los derechos de supresión, bloqueo y oposición, ya reconocidos en las legislaciones protectoras de datos, busca que los sujetos tengan la facultad de exigir que sus datos personales sean completamente eliminados de cualquier tipo de registro, de manera tal que ya no se pueda efectuar una vinculación a ninguno de ellos.

El reconocimiento de este derecho es especialmente relevante en el ámbito de la IoT dado que existen diversos proveedores de esta tecnología y que la información personal mayoritariamente se transmite por internet, estableciéndose la obligación para el responsable del tratamiento de informar a los terceros que eventualmente traten dicha información de la circunstancia del ejercicio del derecho al olvido.[38]

Otro argumento por el cual se hace necesario que las legislaciones establezcan expresamente este derecho, es que el costo de almacenar información decrece en forma continua, por lo que una vez que la información es generada, probablemente será retenida indefinidamente, no existiendo incentivos a su eliminación.[39]

De este modo, se concluye que si un sistema normativo cuenta con una legislación protectora de datos personales que regule al menos los

38. El Reglamento Europeo de Protección de Datos Personales, que se está discutiendo por estos días, reconoce explícitamente el derecho al olvido.

39. En el ámbito de la IoT, una Comisión de la Unión Europea dentro de las líneas de acción para el plan europeo de IoT, ya mencionaba el «silencio de los chips», como un derecho de las personas de desconectarse de su ambiente de red en cualquier momento (European Economic and Social Committee, 2009).

elementos señalados anteriormente, no requiere de una modificación para adecuarse a los impactos de la IoT; si, por el contrario, tal legislación no existe o es insuficiente en su regulación en los aspectos anteriores, sí será necesaria su adecuación.

La tecnología

Existen diversas medidas tecnológicas que se pueden adoptar con el objeto de proteger la privacidad y los datos personales en el ámbito de la IoT. A continuación se presentan tres de ellas, a saber: privacidad por diseño/defecto, evaluaciones de impacto en la privacidad, y la anonimización/minimización.

a) Privacidad por diseño/defecto (PbD, *Privacy by design/default)*. La Comisión Europea ha definido a la privacidad por diseño como la aplicación, teniendo en cuenta el estado de la técnica y el costo de dicha aplicación, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, de las medidas y los procedimientos técnicos y de organización adecuados para que el tratamiento satisfaga los requisitos de la Directiva 95/46/CE y garantice la protección de los derechos del interesado (Comisión Europea, 2014a).

De su parte, la creadora del concepto, Ann Cavoukian (2011), indica que la PbD promueve la visión de que la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; sino que su aseguramiento debe convertirse en el modo de operación predeterminado de una organización. El PbD se extiende a aplicaciones que engloban: 1) sistemas de tecnologías de la información; 2) prácticas de negocios responsables; y, 3) diseño físico e infraestructura en red. Se establece como principio que todos los actores de la IoT ganan con la PbD, ya que de una parte se asegura la privacidad y se obtiene control sobre la información propia, y de la otra los proveedores IoT obtienen una ventaja competitiva sostenible.

Finalmente, la protección de datos por defecto, íntimamente vinculada con la minimización de datos, es la aplicación de mecanismos para garantizar que, por defecto, sólo se sometan a tratamiento los datos personales necesarios para cada objetivo específico del tratamiento y, especialmente, que no se recojan ni conserven más del mínimo necesario para esos fines, tanto en términos de cantidad de datos como de tiempo

de almacenamiento (Comisión Europea, 2014a). De esta manera, no se requiere que los titulares de datos ejecuten alguna acción o solicitud en resguardo de sus derechos de protección de datos personales; el sistema opera sólo respetando tales derechos. Este sistema se caracteriza por satisfacerse por defecto.

b) Evaluaciones de Impacto en la Privacidad (PIA, *Privacy Impact Assessments*).[40] Se trata de procesos en razón de los cuales un consciente y sistemático esfuerzo es realizado para evaluar los impactos en la privacidad y protección de datos de —en este caso— la IoT, con el objeto de tomar las acciones apropiadas para prevenir o al menos minimizar esos impactos (Article 29 Working Party, 2011b). Estos procesos se debieran ejecutar antes del lanzamiento de cualquier nueva aplicación IoT. Se establecen objetivos y riesgos que deben ser analizados, los que en el caso de la IoT son, por ejemplo, los presentados en las tablas 1 y 2.

c) Anonimización/minimización. En razón de la anonimización, allí donde no es necesario tratar datos personales (esto es, que identifican o hacen identificable a una persona), se debe efectuar disociación de datos, ya sea que se recojan disociados o se disocien con posterioridad. La minimización de datos en la IoT, según la Federal Trade Commission (2015) puede ayudar a proteger contra dos riesgos relacionados con la privacidad. En primer lugar, la recolección y retención de grandes cantidades de datos aumenta los daños potenciales asociados con una violación de datos, tanto con respecto a los datos almacenados en el propio dispositivo, así como en la nube, ya que grandes cantidades de datos son un objetivo más atractivo para los que quieran apropiarse de ellos en forma indebida. En segundo lugar, si una empresa recoge y retiene grandes cantidades de datos, existe un mayor riesgo de que los datos serán utilizados de una forma que se aparta de las expectativas razonables de los consumidores.

En este mismo sentido se ha pronunciado el WP29 al indicar que muchos de los actores de la IoT sólo necesitan datos agregados o esta-

40. La Comisión Europea (2014b) ha definido a la PIA como un proceso sistemático para evaluar el impacto potencial de los riesgos cuando las operaciones de tratamiento puedan suponer riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance u objetivos, que debe llevar a cabo el responsable o el encargado del tratamiento, o el encargado que actúa por cuenta del responsable.

Tabla 1.

Objetivos	Alcance
Calidad de los datos	Minimización de datos, especificación de la finalidad, calidad de los datos son objetivos clave que necesitan ser asegurados.
Legitimidad del tratamiento de datos	Legitimidad se debe asegurar con la autorización legal o convencional del tratamiento.
Cumplimento del ejercicio de los derechos subjetivos del titular de los datos	Se debe asegurar que es posible ejercer derechos de acceso, modificación, suspensión o cancelación de datos.
Asegurar confidencialidad y seguridad del procesamiento	Se debe prevenir accesos no autorizados, registros de procesamiento de datos, seguridad de redes y transporte y prevenir pérdida accidental de datos.

Tabla 2.

Riesgos	Alcance
Finalidad del tratamiento	La finalidad del tratamiento no ha sido especificada y documentada, o están siendo usados más datos que los requeridos para el cumplimiento de la finalidad declarada o se está efectuando un cruce de información más allá de lo necesario para cumplir con la finalidad.
Información	La información entregada al titular de los datos no es completa, o el procesamiento de datos no es transparente o la información entregada no es oportuna. Se toman decisiones automatizadas basadas en datos personales, pero el titular de los datos no es informado sobre la lógica de la decisión.
Consentimiento	Consentimiento no ha sido obtenido, o lo ha sido bajo amenaza o en desventaja.
Derechos subjetivos	No se dan las condiciones para que el titular de los datos ejerza sus derechos subjetivos.
Tratamiento de datos ilegítimo	Tratamiento de datos es efectuado en incumplimiento de normas legales.

dísticos y no tienen necesidad de recolectar datos en bruto a través de los dispositivos IoT. Los actores deben eliminar los datos tan pronto hayan extraído la data necesaria para su procesamiento. Como principio, la eliminación debiera ocurrir en el punto más cercano a la recogida del dato en bruto, esto es, en el mismo dispositivo después del procesamiento (Article 29 Working Party, 2014). El Parlamento Europeo ha efectuado a este respecto dos solicitudes: que se adopte como principio general que las tecnologías IoT deben ser diseñadas para recoger y utilizar solamente la cantidad mínima indispensable de datos necesarios para cumplir su función e impedir que se recojan datos adicionales, y que una parte significativa de los datos compartidos por la IoT se conviertan en anónimos antes de ser transmitidos (Parlamento Europeo, 2010).

El mercado

Como ya se mencionara, las personas son actores de este mercado o ecosistema y, por otro lado, los proveedores IoT. Considerando lo señalado anteriormente respecto a la caracterización de los proveedores IoT, se concluye que en su mayoría se trata de responsables de tratamiento de datos personales, conforme las definiciones legales existentes en la materia,[41] por lo que están limitados a cumplir las obligaciones[42] y asumir las responsabilidades que las legislaciones establecen para ellos por tener dichas calidades.

El modelo de protección que se plantea propone que además de dichas obligaciones y responsabilidades, estos actores ejecuten, desde su rol en el mercado y en su propio interés, las medidas técnicas planteadas en el acápite anterior, junto con la creación de códigos de conducta o autorregulatorios[43] que materialicen —a través de medidas concretas y autoimpuestas— sus obligaciones y responsabilidades legales junto con

41. Conforme el artículo 2 letra m) de la Ley 19.628 es responsable del registro o banco de datos la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. De su parte, el artículo 2 letra d) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece que el responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho nacional o comunitario.

42. Podemos citar como las principales obligaciones legales impuestas a los responsables de tratamiento de datos personales las siguientes: seguridad, debido cuidado, calidad de los datos, tratamiento conforme al fin, secreto o confidencialidad, notificación.

43. Alberto Cerda Silva (2006) define a los códigos de conducta o deontológicos como normas de comportamiento adoptadas por los propios destinatarios de sus previsiones. Se trata de una expresión de autorregulación, si bien, a la vez, cumple un rol de control de las operaciones que reglamenta; junto con familiarizar a sus destinatarios con la legislación y reglamentos vigentes, contribuye a adecuar sus disposiciones a un contexto determinado, y en cuanto tal, induce al respeto de la ley y permite cerciorarse del encuadre de las operaciones con el régimen legal aplicable.

las referidas medidas técnicas, asumiendo de esta forma acciones en orden de mitigar la ocurrencia de las malas prácticas mencionadas en el capítulo anterior.

A este respecto, resulta interesante referirse a algunas de las medidas que, conforme el WP29, deben tomar los actores IoT en materia de privacidad y protección de datos personales (Article 29 Working Party, 2014):

Fabricantes de dispositivos:

- Deben informar a los usuarios sobre el tipo de datos que son recogidos y cómo van a ser tratados y cruzados.
- Deben comunicar a todos los demás actores involucrados tan pronto un titular revoca su consentimiento o se opone al tratamiento de datos.
- Deben proporcionar opciones granulares cuando conceden acceso a las aplicaciones a los titulares de datos, de una manera similar al «no molestar» en los teléfonos inteligentes, los dispositivos IoT deberían ofrecer una opción de «no recoger» datos personales para programar o desactivar rápidamente sensores.
- Para cumplir con la transparencia y el control del usuario, deben proporcionar herramientas para a leer, editar y modificar localmente los datos antes de que sean transferidos a cualquier controlador de datos. Además, los datos personales tratados por un dispositivo deben ser almacenados en un formato que permita la portabilidad de datos.
- Los usuarios deben contar con herramientas que les permitan exportar fácilmente sus datos en un formato estructurado y de uso común y amigable.
- Los dispositivos IoT pueden ser compartidos por varios titulares de los datos o incluso arrendados, por lo que deben estar configurados para distinguir entre diferentes personas que utilizan el mismo dispositivo de modo que no puedan conocer las actividades de la otra.
- Deben permitir el control y procesamiento de entidades locales (los llamados *proxies* de privacidad personal) que permiten a los

usuarios tener una idea clara de los datos recogidos por sus dispositivos y facilitar el almacenamiento y el procesamiento local sin tener que transmitir los datos al fabricante del dispositivo.

Proveedores de plataforma:

- Deben promover formatos de datos claros y fáciles de entender, portátiles e interoperables, con el objeto tanto de facilitar las transferencias de datos entre distintas partes como de ayudar a los titulares de datos a entender qué datos personales realmente se están recolectando por los dispositivos IoT.
- Deben promover los formatos de datos que contengan el menor número de identificadores personales como sea posible con el fin de facilitar la anonimización adecuada de los datos.
- Deben trabajar en estándares certificados que establezcan la línea base para las garantías de seguridad y privacidad de los titulares de datos.
- Deben desarrollar protocolos de encriptación y comunicación adaptadas a las especificidades de la IoT, garantizando confidencialidad, integridad, autenticación y control de acceso.

Desarrolladores de aplicaciones:

- Los avisos o advertencias deben ser diseñados para recordar a los usuarios con frecuencia que los sensores están recogiendo datos. Cuando el desarrollador de la aplicación no tiene un acceso directo al dispositivo, la aplicación debe enviar periódicamente una notificación al usuario para hacerle saber que todavía está grabando datos.
- Las aplicaciones deben facilitar el ejercicio por parte del titular de los datos de los derechos de acceso, modificación y eliminación de datos personales recolectados por el dispositivo IoT.
- Deben proporcionar las herramientas para que los titulares de datos puedan exportar los datos personales tanto en bruto como agregados en un formato estándar y utilizable.
- Deben prestar especial atención a los tipos de datos que son procesados y a la posibilidad de deducir datos personales sensibles de ellos.

- Deben aplicar el principio de minimización de los datos. Cuando el propósito se puede lograr utilizando los datos agregados, los desarrolladores no deben acceder a los datos en bruto. De manera más general, los desarrolladores deben seguir un enfoque de privacidad por diseño y minimizar la cantidad de datos recopilados a la necesaria para prestar el servicio.

Integradores

Además de cada una de las medidas que eventualmente le correspondan a los integradores cuando asumen el rol de los otros actores del mercado, a ellos les corresponderá, especialmente:

- El consentimiento para el uso de un dispositivo IoT y el tratamiento de datos resultante debe ser informado y libremente otorgado. Los usuarios no deben ser penalizados económicamente o afectar el acceso a las capacidades de sus dispositivos IoT si deciden no utilizar el dispositivo o un servicio específico de él.
- El titular de los datos personales que se están procesando en el contexto de una relación contractual con el usuario de un dispositivo IoT (por ejemplo, un hotel, una compañía de seguros de salud o un arrendador de autos) debe estar en condiciones de administrar el dispositivo. Independientemente de la existencia de cualquier relación contractual, los titulares de datos personales deben poder ejercer sus derechos de acceso y oposición.

En esta parte, finalmente se discutirá acerca de las entidades de certificación de cumplimiento de protección de datos personales. Se trata de entidades que pueden ser privadas o públicas y que lo que buscan es certificar, mediante la realización de auditorías, que un determinado proveedor IoT cumple con proteger la privacidad y los datos personales. Si se cumplen con estas certificaciones el proveedor contará con un certificado o sello que lo acreditará ante el mercado y, en consecuencia, ante los titulares de datos como uno que se preocupa de los derechos de tales titulares.

Actualmente se está tramitando un proyecto de ley[44] que propuso la existencia de estas entidades certificadoras y que nos parece interesante de rescatar considerando que el modelo propuesto en este artículo requiere, como ya se mencionó, de la ejecución de diversas medidas, las cuales no sólo vienen de la mano de legislación sancionatoria:

- Creación de instrumentos que facilitan el cumplimiento de la ley, por la vía de incentivar la autorregulación, inversión en modelos de prevención de cumplimiento y otros instrumentos que permiten rebajas de sanciones, de manera de centrarse en la prevención y promoción de instrumentos eficaces y eficientes para lograr los propósitos de la legislación, antes que descansar exclusivamente en la imposición de sanciones para quienes infrinjan la ley.
- Así se establece una atenuante especial por prevención de infracciones, si se acredita haber cumplido diligentemente los deberes de dirección y supervisión para la protección de los datos personales bajo responsabilidad o tratamiento del responsable de la base de datos.
- Para dicho objeto, se considera que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión de la infracción, se ha adoptado la implementación de un modelo de organización, administración y supervisión para prevenir la infracción cometida, certificado por una empresa certificadora de cumplimiento.
- Estos certificados indicarán niveles de cumplimiento normativo de acuerdo a la clasificación que se determine reglamentariamente y podrán ser expedidos por una empresa certificadora de cumpli-

44. Boletín 8143-03, proyecto de ley que introduce modificaciones a la Ley 19.628 sobre Protección de la Vida Privada. Dicho proyecto de ley que fue iniciado por mensaje presidencial en el gobierno de Sebastián Piñera, se encuentra actualmente sin avances en su tramitación y no se espera que éstos ocurran. En cualquier caso la existencia de estas empresas certificadoras había sido rechazada en el primer trámite constitucional en la Cámara de Diputados por la Comisión de Economía, Fomento y Desarrollo. Lamentablemente, al día de hoy se sigue esperando el envío por parte del gobierno actual mediante mensaje del proyecto de ley que vendría a enmendar las falencias de nuestra legislación en materia de protección de datos personales.

miento, la que podrá ser una empresa de auditoría externa, sociedad clasificadora de riesgo u otra entidad acreditada por el Servicio Nacional del Consumidor que pueda cumplir esta labor.

- Finalmente, se ha considerado establecer un contrato con cláusulas dirigidas entre la empresa certificadora de cumplimiento y el responsable del tratamiento de datos que requiere los servicios de la primera, para contar con un modelo de prevención de infracciones, denominado «contrato de certificación», en el que se especificarán todos los derechos y obligaciones necesarios para cumplir con lo dispuesto en esta ley. Las cláusulas dirigidas se refieren a que las empresas certificadoras serán responsables de culpa levísima respecto de las obligaciones establecidas en la presente ley. Además, los contratos no podrán contener cláusulas de exención de responsabilidad para la certificadora respecto de infracciones en que se incurra aun cuando exista calificación de compatibilidad con el nivel de cumplimiento señalado en el inciso anterior.

Sociales

Dentro del modelo, cumple un rol fundamental la educación que se le entregue a los titulares de datos respecto a esta tecnología, a cuáles son sus derechos en materia de protección de datos personales y cómo ejercerlos dentro de este ámbito. Sin embargo, lo anterior no es suficiente, ya que también resulta necesario que exista ante los proveedores de esta tecnología una promoción constante respecto de la importancia que tiene el respeto de los derechos a la privacidad y a la protección de datos personales. Lo anterior debiera ejecutarse no sólo por el Estado, sino que también por las diversas organizaciones no gubernamentales que se ocupan de estos temas.

CONCLUSIONES

Este artículo conceptualiza y caracteriza a la IoT como una tecnología relativamente nueva, respecto de la cual, dada su complejidad derivada de los diversos actores y elementos que conforman su ecosistema y por la enorme cantidad de datos personales que maneja, puede constituir

una amenaza a la privacidad y a la protección de datos personales. Esta amenaza, sin embargo, no es nueva, ya que abarca problemáticas que ya han sido detectadas y discutidas ampliamente en el ámbito de la protección de los derechos referidos; no obstante, se comprueba que estos problemas se profundizan en la IoT por su propias características. En este orden de cosas, se enuncian como las amenazas más importantes las siguientes: asimetría de información, ausencia de control sobre la información personal, consentimiento inexistente o ineficaz, y las malas prácticas de los actores de la IoT.

Para mitigar o anular la posibilidad de que tales amenazas se concreten, se han esbozado por la literatura diversos modelos de protección que fueron revisados en este artículo, ninguno de los cuales logra a nuestro entender que los derechos a la privacidad y a la protección de los datos personales sean realmente amparados. Por esta razón, se elabora un modelo de protección que enmienda las actuales falencias ya que utiliza diversas herramientas en forma conjunta, de manera tal que éstas sean usadas selectiva pero conjuntamente, cuando corresponda, según la amenaza a la cual están destinadas a neutralizar.

Se propone que la legislación debiera promover la tecnología IoT creando confianza en los usuarios y consumidores respecto al amparo efectivo de sus derechos a la privacidad y protección de datos personales, mediante la exigencia de un consentimiento al tratamiento de datos personales manifiesto, libre, específico, informado, previo y revocable; estableciendo deberes de información a los proveedores; entregando control efectivo al titular de los datos mediante una regulación adecuada del consentimiento y asegurando el ejercicio de los derechos de oposición, modificación, eliminación o bloqueo de datos cuando los datos personales ya no sean de calidad, y finalmente instaurando en forma expresa el derecho al olvido.

En segundo lugar, la tecnología cumple un rol esencial en este modelo, ya que ella permite que los servicios IoT desde su conceptualización y creación respeten la privacidad y la protección de datos personales —privacidad por diseño/defecto—, lo que, junto con otras herramientas como la anonimización y minimización, facilita que la legitimidad en el tratamiento de datos esté presente en todas sus etapas.

En tercer lugar, el mercado debe intervenir a través de sus diversos actores, creando condiciones técnicas y normativas, como la autorre-

gulación y los códigos de conducta, junto con entidades certificadoras del cumplimiento que incentiven el respeto por la privacidad de los consumidores.

Finalmente, considerando el aspecto social, es relevante que exista educación continua a los titulares de datos personales respecto a sus derechos y las nuevas tecnologías y de promoción ante los proveedores de la IoT sobre los beneficios de respetar tales derechos.

REFERENCIAS

36th International Conference of Data Protection and Privacy Commissioners (2014). «Declaración de Mauricio sobre Internet de las Cosas». Balaclava.

Article 29 Working Party (2011a). «Opinion 15/2011 on the definition of consent». Disponible en <http://bit.ly/1JgiypF>.

—. (2011b). «Privacy and data protection impact assesments framework for RFID applications». Disponible en <http://bit.ly/20cLSS5>.

—. (2014). «Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos». Disponible en <http://bit.ly/1T2cH9G>.

Atzori, Luigi, Antonio Iera y Giacomo Morabito (2010). «The internet of things: A survey». *Computer Networks*, 54: 2787-2805.

Cavoukian, Ann (2011). «7 foundational principles of privacy by design». Information and Privacy Commissioner of Ontario. Ontario.

Cazila, Juan y Roberto Junco (2014). «El internet de las cosas. Una nueva manera de relacionarnos con nuestro entorno». Disponible en <http://bit.ly/1SoZQPz>.

Cerda Silva, Alberto (2006). «Algunas consideraciones sobre los códigos de conducta en la protección de datos personales». *Revista Chilena de Derecho Informático*, 2: 121-132.

Chow, Chi-Yin y Mohamed F. Mokbel (2009). «Privacy in location-based services: a system architecture perspective». *SIGSPATIAL Special*: 23-27.

Comisión Europea (2014a). «Recomendación 2014/724/UE de la Comisión relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente». Diario Oficial de la Unión Europea del 18 de octubre de 2014. Disponible en <http://bit.ly/1QjiNjl>.

—. (2014b). «Definition of a research and innovation policy leveraging cloud computing an IoT combination». Report. Bruselas.

—. (2015a). «Digital agenda for Europe. The internet of things». Disponible en <http://bit.ly/236YNYj>.

—. (2015b). «A digital single market strategy for Europe. Analysis and evidence». Disponible en <http://bit.ly/1ZHaIYh>.

De Filippi, Primavera (2014). «Big data, big responsabilities». *Internet Policy Review*, 3: 1-12.

Electronic Privacy Information Center (2015). Disponible en <http://bit.ly/1Zs8XxT>.

Escribano, Bianca (2014). «Olswang». Disponible en <http://bit.ly/236YBrO>.

European Economic and Social Committee (2009). «Internet of things. An action plan for Europe». Disponible en <http://bit.ly/1QcmoQc>.

Federal Trade Commission (2015). Disponible en <http://1.usa.gov/1Spomxo>.

Gambi Moreira, Ennio (2004). «Análisis de la ley 19.812 y régimen jurídico del *scoring* crediticio o modelo de calificación financiera». *Revista Chilena de Derecho Informático*, 4: 131-148.

Gozaini, Osvaldo (2001). *Hábeas data. Protección de datos personales. Doctrina y jurisprudencia*. Buenos Aires: Rubinzal-Culzoni.

Herrán, Ana (2002). *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Madrid: Dykinson.

IDC y TXT (2014). «Definition of a research and innovation policy leveraging cloud computing and IoT combination». Disponible en <http://bit.ly/1NiYX2Y>.

IDC (2015). Noticias. Disponible en <http://bit.ly/1RWQg4N>.

International Telecommunication Union (2005). «ITU Internet Reports 2005: The internet of things».

—. (2014). Terms and definitions.

—. (2015). «GSR Discussion Paper. Regulation and the internet of things». Disponible en <http://bit.ly/1ZE616U>.

Jervis, Paula (2006). *La regulación del mercado de datos personales en Chile*. Tesis para optar al grado de Magíster en Derecho. Santiago: Facultad de Derecho, Universidad de Chile.

Parlamento Europeo (2010). «Resolución del Parlamento Eu-

ropeo, de 15 de junio de 2010, sobre la Internet de los Objetos (2009/2224(INI))».

Perera, Charith (2014). «Context aware computing for the internet of things: A survey». *IEEE Communications Surveys & Tutorials*, 16 (1): 414-454.

Perera, Charith, Rajiv Ranjan, Lizhe Wang, Samee U. Khan, y Albert Y. Zomoya (2015). «Big data privacy in the internet of things era». *IT Professional*, 17 (3): 32-39.

Senado (1998). «Diario sesiones del Senado. Sesión 18, tomo 2034».

Solove, Daniel (2002). «Conceptualizing privacy». *California Law Review*, 90: 1087-1155.

Solove, Daniel y Paul M. Schwartz (2009). *Privacy, information and technology*. Nueva York: Wolters Kluwer.

Swire, Peter (1997). «Markets, self-regulation, and government enforcement in the protection of personal information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce». Disponible en <http://ssrn.com/abstract=11472>.

Toch, Eran, Yang Wang y Cranor Lorrie Faith (2012). «Personalization and privacy: A survey of privacy risks and remedies in personalization-based system». User Model User-Adap Inter: 203-220.

Warren, Samuel y Louis Brandeis (1890). «The right to privacy». En *El derecho a la intimidad*. Traducción al castellano de Benigno Pendás y Pilar Baselga (1995). Madrid: Civitas.

Weber, Rolf (2009). «Internet of things. Need for a new legal environment?». *Computer Law & Security Review*, 522-527.

Weber, Rolf y Romana Weber (2010). *Internet of things. Legal perspectives*. Zürich: Springer.

Zhang, Jing, y Liuqi Ye (2010). «The internet of things and personal privacy protection». En *International Conference of Logistics Engineering and Management* (pp. 2895-2901). *Virginia: American Society of Civil Engineers*.

Ziegeldorf, Henrik Jan, Oscar García Morchon y Klaus Wehrle (2013). «Privacy in the internet of things: Threats and challenges». *Security and Communications Networks*: 2728-2742.

SOBRE LA AUTORA

Paula Jervis Ortiz es abogada. Licenciada en Ciencias Jurídicas y Sociales de la Universidad de Chile, Magíster en Derecho, con mención en Derecho Económico por la misma universidad y Magíster en Derecho de la Empresa por la Pontificia Universidad Católica de Chile. Su correo electrónico es <paulajervisortiz@gmail.com>. Su dirección postal es Alsacia 150, Las Condes, Región Metropolitana.

Este trabajo fue recibido el 30 de octubre de 2015 y aprobado el 14 de diciembre de 2015.