EN LETRA - año VI, números 11-12 (2019)
pp. 139-164

(DES)VENTAJAS DE LA PRIMERA LEGISLACIÓN SOBRE INTERNET DE LAS COSAS

Adriana Margarita PORCELLI*

Fecha de recepción: 21 de diciembre de 2018
Fecha de aprobación: 31 de mayo de 2019

Resumen

Durante las últimas décadas Internet ha evolucionado tan velozmente que abarca aspectos antes inimaginables. Computadoras, impresoras, celulares, tablets, televisores inteligentes, luces, automóviles, electrodomésticos y hasta la cerradura de las casas se pueden manejar a distancia para confort del consumidor. Pero también acarrea sus riesgos y las personas pueden ser víctimas de todo tipo de delitos. En consecuencia es necesario el dictado de normas que proporcionen mayor seguridad al manejo de los dispositivos conectados a la Red. El presente trabajo consiste en definir el ecosistema denominado Internet de las Cosas y analizar la Ley de California N° 327 *Information privacy: connected devices*. A tales efectos, comprende dos partes: la primera que delimita el marco conceptual-tecnológico y la segunda que examina los diferentes principios adoptados en la Ley N° 327 *Information privacy: connected devices*, y a la vez presenta sus más duras críticas así como los argumentos en su defensa.

* Abogada y procuradora graduada de la Universidad de Buenos Aires (UBA – Argentina). Magister en Relaciones Internacionales (Universidad Maimónides - Argentina). Diploma en Derechos Económicos, Sociales y Culturales (Universidad de la Patagonia San Juan Bosco - Argentina). Profesora Adjunta Ordinaria de la Universidad Nacional de Luján (UNL – Argentina). Miembro del Comité de Bioética. Correo electrónico de contacto: adporcelli@yahoo.com.ar

Palabras Clave

Internet de las cosas – legislación – privacidad – ciberseguridad

(DES)ADVANTAGES OF THE FIRST LEGISLATION ON THE INTERNET OF THINGS

Abstract

During the last decades, Internet has evolved into something that unforseeable matters. Computers, printers, cell phones, tablets, smart televisions, lights, cars, appliances and even door locks can be remotely operated for the consumer's comfort, but they can also be the medium for all kinds of crimes. In effect, it is necessary to set standards for ensuring the secure use of these devices that are connected to the Network. The present work consists of defining the ecosystem called Internet of Things and California Law No. 327 Privacy of information: connected devices. For such purpose, it comprises two parts: the conceptual-technological framework is defined in the first one; and, secondly, the different principles adopted in the referred statute are analyzed.

Keywords

Internet of things – legislation – privacy – cybersecurity

1. Introducción

Los economistas afirman que la humanidad está en el preludio de la Cuarta Revolución Industrial, llamada también Industria 4.0,[1] continuadora de los otros tres procesos históricos transformadores**:** (a) la Primera Revolución Industrial (entre 1760 y 1830) marcó la transición de la producción manual a la mecanizada, (b) la Segunda (alrededor de 1850) introdujo la electricidad y permitió la manufactura en masa, y (c) la Tercera (mediados del siglo XX), denominada la Revolución Digital, basada en el uso de tecnologías de información para automatizar aún más la producción. Esta Cuarta Revolución Industrial no se define por un conjunto de tecnologías emergentes en sí sino por

1 Este término fue utilizado por primera vez en la Feria de Hanover (Alemania) de 2011.

la completa digitalización de las cadenas de valor a través de la integración de tecnologías de procesamiento de datos, software inteligente y sensores. Recurriendo a Internet, a los sistemas ciberfísicos y a las redes virtuales con posibilidades de controlar objetos materiales, se pueden ir modernizando las plantas fabriles hasta transformarlas en fábricas inteligentes (PERASSO, 2016).

Dicho en forma más simple, una producción industrial en la que todos los productos y máquinas están interconectados entre sí digitalmente. Las nuevas tecnologías y enfoques están fusionando los mundos físico, digital y biológico de manera que transformarán a la humanidad en su esencia misma. En ello radica lo novedoso de esta nueva revolución que, a diferencia de las anteriores que se desarrollaron exclusivamente en el mundo físico, la conecta ese ámbito físico con el espacio digital, utilizando como medio de comunicación Internet (es decir, el Internet de las Cosas o "IOT", según las siglas del término en inglés [*Internet of Things*]) y como mensaje los propios metadatos o datos.

La digitalización está permeando la economía con tal intensidad que se dice que los datos son el nuevo petróleo[2], o que quien maneje los datos hoy maneja el mundo. Las empresas que gozan de mayor cotización en el mundo son empresas que ofrecen servicios gratuitos (por ejemplo, Google, Facebook, Twiter), pero nada en la Web es del todo anónimo ni gratuito. Cada vez que se ingresa en algún sitio se deja una marca, un rastro, un dato. Los datos son reproducibles tienen costos de transporte ínfimo e involucran aspectos de privacidad y seguridad. Al parecer los consumidores no evidencian el real poder de los datos ya que están dispuestos a entregarlos para recibir un servicio en línea, así como tampoco por parte de muchas empresas que no gestionan eficientemente la información que poseen. En realidad no son datos de la empresa sino de terceros que deben manejarlos de forma segura, vale decir tienen un deber de seguridad. A lo complejo del tema debe agregarse la necesidad de coordinación internacional al tratarse de asuntos que trascienden las fronteras nacionales. En 2017, cerca de 4.000 millones de personas -más de la mitad de la población mundial- utilizaba Internet y un 56% lo hacía con suscripciones a servicios móviles. Por otra parte, el 61% de dichas suscripciones operaban sobre redes 3G o 4G y durante el 2017 se descargaron 175.000 millones de aplicaciones y se usaban activamente

2 Según THE ECONOMIST (2017) "The world's most valuable resource is no longer oil, but data", consultado en [https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worldsmost-valuable-resource] el 03.08. 2018.

alrededor de 40 en cada teléfono inteligente. A principios de 2018 se registraban más de 5.000 millones de usuarios únicos de telefonía móvil, de los cuales 57% utilizaba teléfonos inteligentes. En enero de 2018, más de 3.000 millones de personas -el 42% de la población mundial- usaban mensualmente las redes sociales, especialmente mediante dispositivos móviles. En tanto, el uso de plataformas de comercio electrónico para comprar bienes de consumo creció hasta alcanzar los 1.800 millones de compradores -el 23% de la población mundial- en línea a nivel mundial. Entre las nuevas tecnologías que están impulsando la digitalización, la Internet de las Cosas es una de las que se prevé tendrá mayor impacto, tanto en el desarrollo de bienes y servicios para los consumidores como para usos productivos. (CEPAL, 2018).

Según estimaciones realizadas por la consultora GARTNER (2013), en 2020, el número de objetos conectados a Internet será más de 26.000 millones (excluyendo PCs, *tablets* y *smartphones*) y que la Internet de las Cosas aportará por sí un valor de 1,9 billones de euros a la economía mundial, demostrando la gran importancia estratégica que representará la economía digital en los próximos años. En sintonía, el estudio del MCKINSEY & COMPANY (2018), titulado *The Internet of Things: How to capture the value of IoT* una Internet de las cosas completamente conectada podría añadir hasta $11 billones a la economía global al año para el 2025 a través de diferentes entornos incluyendo fábricas, ciudades y ámbitos minoristas.

De lo anteriormente expuesto se puede deducir que Internet de las Cosas genera una enorme cantidad de datos transmitidos que son analizados a una velocidad antes inimaginable, realizando predicciones. Es destacable su valor en sectores claves como en el sanitario, en las *Smart Cities*, en el de la distribución, entre otros. Pero también conlleva importantes riesgos, como ser futuros usos no previstos en el momento de obtener la información y el consentimiento para ellos, la generación de perfiles, la manipulación, la monitorización de la conducta (*profiling*) y las valoraciones basadas en decisiones automatizadas que pueden perjudicar seriamente a las personas. Redes sociales como Facebook o Twitter permiten conocer los intereses de millones de personas en tiempo real, a qué estímulos responden, cuándo se conectan, qué compran, qué sitios visitan, con quiénes interactúa y más. Al cruzar esa enorme cantidad de datos con las que tienen (por ejemplo, las tarjetas de crédito o los resultados electorales), se puede medir casi todo. Los datos masivos que las personas entregan a los operadores globales (Google-Alphabet, Apple, Microsoft, Amazon y Facebook) reflejan toda su vida y adquieren dimensión económica al ser monetizados. Estas corporaciones están corriendo de lugar el eje de la

relación consumidor-producto, ahora los consumidores son una parte inescindible del producto.

Todas estas tecnologías, denominadas actualmente disruptivas, deben ser reguladas efectivamente por el derecho. En todos los países se evidencia una marcada tendencia a la formulación e implementación de estrategias digitales cada vez más integrales. La generación de agendas digitales fue estimulada por iniciativas internacionales, como las dos Cumbres Mundiales para la Sociedad de la Información (CMSI) de 2003 y 2005, la inclusión de las TICs en los Objetivos de Desarrollo Sostenible de las Naciones Unidas (ODS) en 2015, el Foro de la Cumbre Mundial de la Sociedad de la Información de 2018 "Aprovechando las TICs para construir Sociedades de la Información que alcancen los ODS" y la formulación de sucesivos planes regionales de acción sobre la Sociedad de la Información en América Latina y el Caribe, la última la VI Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Caribe de 2018 (eLAC 2020).

Por su parte, Europa comenzó con el abordaje de la problemática al adoptar las líneas maestras para el establecimiento de Políticas de Internet de las Cosas europeas. En marzo de 2015, la Comisión Europea publicó la "Alianza para la Innovación de Internet de las Cosas" para apoyar la creación de un ecosistema de Internet de las Cosas europeo innovador e impulsado por la industria. En mayo de 2015 adoptó la Estrategia del Mercado Único Digital y el 19 de abril de 2016 publicó el documento *Advancing the Internet of Things in Europe,* vale decir, Avanzando en la Internet de las Cosas en Europa".

Estados Unidos está mucho más avanzado en el tema legislativo y el 1 de agosto de 2017, el senador Mark Warner presentó una propuesta de ley *A Bill S.1961* intitulada *Internet of Things (IoT) Cybersecurity Improvement Act of 2017* con el objeto de establecer los estándares mínimos de seguridad que deben cumplir los dispositivos conectados a Internet adquiridos por las agencias federales, pero no para los electrónicos en general. En paralelo, el senador Roger Wicker introdujo, el 14 de diciembre de 2017, un proyecto de ley *A Bill S.2234*, *Internet of Things Consumer Tips to Improve Personal Security Act of 2017* y recientemente, 6 de julio de 2018, el senador Robert Latta presentó un proyecto de ley *H.R. 6032 State of Modern Application, Research, and Trends of IoT Act*. Pero ninguna de las iniciativas señaladas, hasta la fecha, se convirtió en ley. Por tanto, se destaca que el Gobernador del Estado de California, Jerry Brown, promulgó el 28 de septiembre de 2018, un proyecto de ley SB-327 *Information privacy: connected devices* que fue agregada a la Sección 1, Parte 4 de la División 3 del Código Civil, bajo el título *1.81.26. Security of Connected*

Devices, lo que convierte a California en el primer Estado con una ley de seguridad cibernética que cubre los dispositivos "inteligentes".

El presente trabajo consiste en definir y enumerar los componentes necesarios para el funcionamiento del ecosistema denominado Internet de las Cosas y analizar la Ley de California N° 327 *Information privacy: connected devices*. A tal efecto, este artículo comprende dos partes: la primera que delimita el marco conceptual-tecnológico y la segunda que examina los diferentes principios adoptados en la Ley N° 327 *Information privacy: connected devices*, y a la vez presenta sus más duras críticas así como los argumentos en su defensa.

2. Marco conceptual: Internet de las Cosas

La Internet de las Cosas parte de la base que no sólo las personas están conectadas sino también todo lo que pueda ser controlable desde el punto de vista electrónico: una casa, los electrodomésticos, las luces, la calefacción, los celulares o un auto, etc. Se fundamenta en la relación máquina-máquina (*machine to machine* o M2M), que implica el control de un dispositivo sobre otro, ambos conectados por Internet y sin la gestión de una persona. Según la Unión Internacional de Telecomunicaciones (UIT), se trata de una infraestructura mundial al servicio de la sociedad de la información, que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas gracias al interfuncionamiento de tecnologías de la información y la comunicación (existentes y en evolución) (CEPAL, 2016).

Conforme el "Dictamen 8/2014 sobre la evolución reciente de la Internet de los Objetos" del 16 de septiembre de 2014 y elaborado por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 -órgano consultivo de la Unión Europea- Internet de las Cosas comprende los sensores con capacidad de interacción entre ellos y con otros sistemas, que se incorporan a dispositivos de uso cotidiano de forma que recogen, tratan, almacenan y transfieren datos utilizando capacidades de interconexión en red, vale decir

con Internet.[3] Además identifica tres grandes bloques sobre los que se pueden desarrollar esa conexión:

a) Tecnología ponibles (*wearable computing*) son aquellos dispositivos que se han miniaturizado de tal manera que sean portables y ofrecen información sobre el entorno y las personas. El objetivo es que la tecnología sea imperceptible para el usuario final y que esté presente en su vida cotidiana sin tener que acudir a *tablets* y *smartphones* que son más pesados. Por ejemplo los *Google Glass* son una computadora ponible que incluye un pequeño dispositivo de visualización de cristal líquido. Se activa por la voz y los usuarios pueden desplazarse por los menús gracias a un teclado táctil situado en el lateral del dispositivo. Permite utilizar un número cada vez mayor de aplicaciones, tomar fotografías, grabar videoclips, cargar archivos en Internet, efectuar búsquedas en línea y enviar mensajes de correo electrónico. *Nike* fue una de las primeras empresas en adoptar esas tecnologías al introducir el dispositivo para la práctica deportiva *Nike+iPod* en 2006 (POOLE, 2014). Otro ejemplo destacable lo constituye la compañía británica *Intelligent Environments*, que desarrolló una plataforma virtual que se conecta a una pulsera que envía pequeñas descargas eléctricas (de 17 a 340 voltios) al usuario, cuando sus gastos superan lo deseado.[4]

b) Dispositivos que registran información sobre la actividad de las personas: en este grupo se ubican las informaciones sobre los lugares visitados, entre otros. Eso supone tener una radiografía que implica una vulnerabilidad para los individuos si es manejada de forma incorrecta. Un ejemplo es WAZE, una aplicación de tráfico gratis y colaborativa para smartphones que ayuda a esquivar atascos, a seleccionar el itinerario más conveniente.

3 El Grupo de Trabajo sobre Protección de Datos del Artículo 29 se creó en virtud del artículo 29 de la Directiva 95/46/CE. A partir del 25 de mayo del 2018 fue sustituido por el Consejo Europeo de Protección de Datos.

4 Más ejemplos se pueden consultar en INFOBAE (2016) "Polémico: una pulsera envía descargas eléctricas para fomentar el ahorro", consultado en [https://www.infobae.com/2016/05/23/1813599-polemico-una-pulsera-envia-descargas-electricas-fomentar-el-ahorro/] el 15.03. 2017

c) Domótica: por tal concepto se entiende al conjunto de tecnologías aplicadas al control y a la automatización inteligente de la vivienda, que permite una gestión eficiente del uso de la energía y aporta seguridad y confort, además de comunicación entre el usuario y el sistema (GALLEGO GÓMEZ y DE PABLOS HEREDERO, 2016). El primer ejemplo de domótica y control remoto automatizado es la instalación de controles de acceso digitales a la vivienda, cerraduras electrónicas que permiten controlar cuántas veces se ha abierto la puerta, comprobar si está bien cerrada (incluso estando a miles de kilómetros) o proporcionar acceso a cualquier persona en cualquier momento preciso.[5]

Así, cabe distinguir entre la Internet de las Cosas del consumidor (hogar inteligente, tecnologías ponibles) y la Internet de las Cosas de la producción, también denominada Internet Industrial. En el año 2017 se estimaba que a nivel mundial había alrededor de 8.000 millones de unidades instaladas de la Internet de las Cosas, de las cuales el 63% correspondía a soluciones de consumo personal (como domótica, tecnologías ponibles [*wearable technologies*] o autos conectados), en tanto que el restante 37% se repartía en soluciones transversales y para sectores específicos (GARTNER, 2017).

En base a lo expuesto, Internet de las Cosas crea de un mundo inteligente donde lo real, lo digital y lo virtual convergen para crear un entorno que proporciona más inteligencia a la energía, a la salud, al transporte, a las ciudades, a la industria, a los edificios y en muchas otras áreas de la vida diaria. Un ámbito en donde se interconectan millones de redes inteligentes que habilitan el acceso a la información no sólo en cualquier momento y lugar, sino también usando cualquier cosa y por parte de cualquier persona, a través de cualquier ruta, red, y cualquier servicio (COLINA, *et al*, 2015).

Fundamentalmente países como Alemania, Estados Unidos y China han implementado políticas para reorientar sectores productivos estratégicos hacia la industria 4.0. En la fábrica inteligente, el producto, al comunicarse con su entorno, puede reconfigurar la disposición de los sistemas de fabricación y adaptar los cambios en la producción de

5 Para ampliar en la temática, véase 20 MINUTOS (2016) "Domótica: cómo automatizar tu hogar para disfrutarlo más mientras ahorras tiempo y dinero", consultado en [https://blogs.20minutos.es/un-hogar-con-mucho-oficio/2016/11/03/domotica-como-automatizar-tu-hogar-para-disfrutarlo-mas-mientras-ahorras-tiempo-y-dinero/] el 15.03. 2017.

manera rentable y ha favorecido a la producción personalizada que satisface las necesidades heterogéneas de los clientes (CASALET, 2018).

Dentro del ecosistema de Internet de las Cosas se puede identificar los siguientes componentes:

a) Una Red de Sensores Inalámbricos (*wireless sensor network* [WSN]) es una red que se auto-configura, formada de pequeños nodos sensores que se comunican entre sí por señales de radio para percibir el mundo físico, son un puente entre el mundo físico y el virtual.

b) Módulos y tecnologías de comunicación: todos los aparatos que forman parte de la Internet de las Cosas deben estar conectados a una red de comunicaciones. Las cosas necesitan conversar entre sí y con Internet. Los módulos de comunicación son los componentes de los dispositivos responsables de la comunicación que proveen de conectividad conforme el sistema inalámbrico o el protocolo de comunicación por cable designado. La comunicación puede realizarse conforme la tecnología inalámbrica utilizada (como WiFi, Bluetooth y ZigBee), el sistema de conexión de celulares-actualmente con tecnologías de Cuarta Generación (4G), pero que se apresta a dar un paso más y llegar al estándar 5G y las tecnologías por cable, como Ethernet, utilizan el protocolo TCP/IP.

c) Procesamiento de Información Integrado: Los objetos inteligentes cuentan con una capacidad de procesador o microcontrolador y además capacidad de almacenamiento.

d) Geocalización: es la capacidad de los objetos inteligentes para obtener la ubicación física real de un objeto. La red de teléfono móvil o los sistemas de posicionamiento global (GPS) son tecnologías adecuadas para lograrlo, así como medidas de tiempo de ultrasonido, la identificación de radiofrecuencia y las tecnologías ópticas.

e) Interfaces de usuario: los objetos inteligentes pueden comunicarse con las personas de manera directa o indirectamente (por ejemplo a través de un *smartphone*), interfaces de usuario tangibles y métodos de reconocimiento de voz, imagen o gesto.

f) Fuente de alimentación: todo dispositivo electrónico requiere de energía eléctrica para funcionar.

Sin embargo, como las comunicaciones entre la unidad principal y sus módulos o entre los módulos entre sí se realiza, en la mayoría de los casos, utilizando un protocolo serial o estandarizado que es adoptado por la mayoría de las PCs y por los dispositivos electrónicos, la Internet de las Cosas necesita realizar algunos cambios en la conectividad de dispositivos, protocolos de comunicación y lenguajes de software para lograr la interoperatividad entre todos sus componentes. La generación de estándares implica que cada proveedor de tecnología debe cumplir con un protocolo de manera tal que su equipo sea compatible con los demás fabricados por otros prestadores para evitar las posiciones de dominio de mercado y de bloqueo del desarrollo. En este sentido, la Unión Internacional de las Telecomunicaciones ha formulado las Recomendaciones del Sector de Normalización de la UIT (UIT-T) para garantizar la interoperabilidad de las aplicaciones, los servicios y las plataformas de Internet de las Cosas.

El Protocolo de Internet (*Internet Protocol* [IP]), actualmente, está presente en todos los dispositivos capaces de enviar y recibir información digital, no solamente la Internet. Desde hace varios años, debido al crecimiento y al uso masivo que ha tenido la Web, se notó un agotamiento de las direcciones de la versión 4 (IPv4) ya que nunca fue diseñado para abarcar a tan alto número de dispositivos. Los esfuerzos llegaron hasta el punto de cambiar el protocolo de conexión IP de la versión 4 a la versión 6 (Ipv6), que conlleva una ampliación de la cantidad de direcciones disponibles a nivel mundial.

Ahora bien, previo al análisis de la ley del Estado de California, es necesario mencionar los riesgos derivados del presente ecosistema en cuanto a la privacidad, la protección de datos y la seguridad de la información (TEJERO LÓPEZ, 2014):

a) Efectividad en las medidas de seguridad: un limitante consiste en que no se las tienen en cuenta en la fase de diseño. Además la heterogeneidad de los dispositivos supone un gran problema en cuanto a proponer soluciones de tipo más universal y el aumento de recopilación de datos puede plantear problemas de autenticación y confianza en los objetos.

b) La proliferación de la gran cantidad de datos en los entornos de Internet de las Cosas facilita que puedan llegar a utilizarse para propósitos diferentes para los

que fueron recabados originalmente. No siempre las personas son conscientes de las capturas de la información, el tratamiento y/o la manipulación de esa información.

c) Riesgo de ataques maliciosos contra los dispositivos y sistemas: es difícil identificar los controles más apropiados para los sistemas dado la heterogeneidad de los objetos, además que todavía se desconoce su evolución futura.

d) *Lock-in* del usuario: significa que los usuarios se queden cooptados por un proveedor específico de servicios y les resulte difícil migrar a otros proveedores, provocado por la no homogenización de los dispositivos y tecnologías de comunicación.

e) Pérdida del control por el usuario*:* uno de los principales objetivos de la Internet de las Cosas consiste en dotar de cierta autonomía a los objetos y permitirles tomar decisiones de forma automática. Es necesario saber acotarlo y controlarlo adecuadamente para que no suponga riesgos o afecte a sus usuarios.

f) Legislación aplicable: el vacío legal es un riesgo colateral a todos estos avances digitales y tecnológicos, porque ni los gobiernos ni entes reguladores van al paso de los cambios. Dado el carácter global de Internet, otro problema es que los individuos y empresas se enfrentan a una serie de leyes de protección de datos nacionales que ofrecen distintos niveles de protección.[6] En enero de 2018, Microsoft publicó su libro *The Future Computed: Artificial Intelligence y and Its Role in Society*, en el que se plantea que si, bien la Inteligencia Artificial ayudará a resolver los grandes problemas sociales, es necesaria la formulación de una legislación moderna, la observancia de principios éticos sólidos, la capacitación para nuevas habilidades e incluso las reformas del mercado laboral. A medida que las computadoras se comportan más como los humanos, las ciencias sociales y las humanidades se volverán aún más importantes. Si la Inteligencia Artificial quiere alcanzar su potencial para servir a los humanos, entonces cada ingeniero tendrá

que aprender más sobre las ciencias sociales y cada especialidad en las ciencias sociales necesitará aprender más sobre ingeniería.

3. Primera legislación sobre Internet de las Cosas

La Senadora de Santa Bárbara, Hannah-Beth Jackson, presentó ante el Senado del Estado de California un proyecto 327, titulado *Information privacy: connected devices* (2017-2018) (03.02.2017). Posteriormente fue enmendado por la autora, continuó con el tratamiento legislativo y después de las tres lecturas obligatorias fue promulgado por el Gobernador Jerry Brown y archivado en la Secretaría del Estado (29.09.2018). De esta forma, se transformó en ley (*act*) y se agregó a la Sección 1, Parte 4 de la División 3 del Código Civil californiano, bajo el título *1.81.26. Security of Connected Devices*.[7]

Como requisito para su entrada en vigencia, en la Sección 2, establece que es necesario que el proyecto de la Asamblea N° 1906, titulado *Information privacy: connected devices. (2017-2018)*, presentado por la asambleísta Jacqui Irwin, de Thousand Oaks (enero de 2018), también se promulgue y entre en vigencia. Justamente ese mismo día (28.09.2018), ambos proyectos fueron promulgados por el Gobernador. El proyecto 327 es anterior, pero al ser enmendado es casi un espejo del proyecto 1906. Sin embargo, la posterior aplicación de ambas leyes es diferida al 1° de enero del 2020. La razón es otorgarles tiempo a los fabricantes de dispositivos conectados a Internet para que puedan adecuar sus productos a la nueva normativa.

Entre los fundamentos esgrimidos por la Senadora Jackson a favor de la promulgación de este proyecto de ley se destaca que los dispositivos de uso de los consumidores que se conectan a Internet van mucho más allá de la PC de escritorio tradicional para incluir una amplia variedad de productos electrónicos de consumo, como microondas, refrigeradores y juguetes para niños. Si bien estas capacidades pueden aumentar la funcionalidad del producto, muchos consumidores no están informados sobre

7 Para ampliar la historia sobre el tratamiento legislativo, consultar CALIFORNIA LEGISLATIVE INFORMATION (2018): *Bill History. SB-327 Information privacy: connected devices. (2017-2018)* consultado en [https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB327] el 3.12. 2018.

las consecuencias de poseer dispositivos conectados. Los consumidores pueden comprar un dispositivo sin darse cuenta hasta mucho tiempo después que hayan comenzado a usarlo en su hogar cómo utiliza Internet, qué tipos de información recopila y cómo se utiliza esa información. Algunos juguetes conectados a la Red, por ejemplo, piden a los niños que proporcionen datos personales verbalmente, incluidos los nombres de sus padres, el nombre de su escuela y el lugar donde viven, y se reservan explícitamente el derecho de realizar marketing directo hacia los menores. Continúa señalando que un número alarmante de estos dispositivos conectados a Internet carecen incluso de las funciones de seguridad más básicas, lo que los hace vulnerables a la piratería y a los ataques cibernéticos coordinados. Por ello se afirma la necesidad de la ley ya que crea un requisito de seguridad para los dispositivos conectados a Internet que pueden evolucionar a medida que la tecnología evoluciona. Requiere que los fabricantes equipen sus dispositivos con razonables y adecuadas características de seguridad a la naturaleza e información que recopila. También requiere que los fabricantes diseñen dispositivos conectados con indicadores visuales, auditivos u otros para mostrar cuándo están recolectando información, para obtener el consentimiento del usuario cuando la recopilación de información se extiende más allá de lo que es necesario y para notificar a los consumidores cualquier actualización o parche en la seguridad.

Con respecto a los consumidores, les permite tomar decisiones informadas al exigirles, a los vendedores, que revelen en el punto de venta, si el dispositivo es capaz de recopilar información personal o confidencial, dónde se puede encontrar la política de privacidad del dispositivo y cómo obtener actualizaciones de seguridad para el mismo.

Conforme *Common Sense Kids Action*,[8] patrocinador de la actual ley, el garantizar que los dispositivos conectados cumplan con los estándares de seguridad básicos ayudará a las familias a tomar decisiones informadas sobre estos dispositivos y sobre la información

8 *Common Sense Kids Action* es una organización nacional norteamericana sin fines de lucro líder con más de una década de experiencia ayudando a niños y familias a tener acceso a servicios de educación y salud infantil de alta calidad y asequibles; que todos los niños tengan experiencias de aprendizaje digital de vanguardia; que sus datos en línea están protegidos; y que tengan la oportunidad de crecer con suficientes oportunidades económicas y educativas para ayudarles a tener éxito en la vida.

que recopilan y comparten. El objetivo es asegurarse que las familias sepan qué información pueden recolectar los dispositivos que compran y quien tiene el control.

Por su parte, el Comité Judicial del Senado enumera varias leyes que refuerzan y que cambian con dicha normativa. En primer lugar, la Constitución de California, en cuyo artículo I Sección 1, se establece que todas las personas son por naturaleza libres e independientes y tienen derechos inalienables. Entre estos están disfrutar y defender la vida y la libertad, adquirir, poseer y proteger bienes, y buscar y obtener seguridad, felicidad y privacidad. La jurisprudencia existente permite a una persona interponer una acción por agravio por una invasión de la privacidad y establece que para presentar una demanda por violación del derecho constitucional a la privacidad, el demandante debe establecer los siguientes tres elementos: 1) un interés legalmente protegido a la privacidad; 2) una expectativa razonable de privacidad en esas circunstancias; y 3) que la conducta del acusado constituya una invasión grave de la privacidad.[9] En cuanto al interés a la privacidad legalmente reconocido, dicha jurisprudencia, establece que son generalmente de dos clases: intereses en excluir la difusión o el uso indebido de información sensible y confidencial (privacidad informativa), e intereses en la toma de decisiones personales íntimas o en la realización de actividades personales sin observación, intrusión o interferencia (autonomía de privacidad).

Conforme el Código Civil de California, Sección 1708.8, un individuo es responsable de una invasión a la privacidad cuando intente capturar, de una manera ofensiva, cualquier tipo de imagen visual, grabación de sonido u otra impresión física de otra persona involucrada en una relación privada y personal o actividad familiar, mediante el uso de cualquier dispositivo, independientemente de si esta imagen, grabación de sonido u otra impresión física no se podrían haber logrado sin que se usara el mismo. Y en la Sección 1798.81.5(b) se requiere que una empresa que posee licencias o mantiene información personal sobre un residente de California debe implementar y mantener procedimientos y prácticas de seguridad razonables y adecuadas a la naturaleza de la información, para

9 Superior Court of California *in re* "Hill v. National Collegiate Athletic Assn", sentencia del 28.01.1994. [N. del E.: consultado en {https://law.justia.com/cases/california/supreme-court/4th/7/1.html} el 27.12.2019]

proteger la información personal del acceso no autorizado, de la destrucción, del uso, la modificación, o revelación.

Según el Código de Negocios y Profesiones de California (Sección 22948.20), una persona o entidad no debe proporcionar la operatoria de una función de reconocimiento de voz sin informar, durante la configuración inicial o la instalación de un televisor conectado (ya sea al usuario o a la persona designada por él) la configuración o instalación inicial de la televisión conectada. Cualquier grabación real de la palabra recopilada a través de la operatoria de una función de reconocimiento de voz por el fabricante de un televisor conectado o de un tercero con el fin de mejorar la función de reconocimiento de voz no se venderá ni utilizará con fines publicitarios.

Por su parte, el Código Penal, en la Sección 637.5(a)(1), dispone que ninguna persona que posea, controle, opere o administre una empresa de televisión satelital o por cable, o que arrende canales en un sistema satelital o de cable, podrá utilizar cualquier dispositivo electrónico para grabar, transmitir u observar eventos o escuchar, registrar, o monitorear cualquier conversación que tenga lugar dentro de la residencia, o lugar de trabajo del suscriptor, sin obtener el consentimiento expreso por escrito del mismo. En la Sección 637.5(a)(2) se establece que ninguna empresa de televisión satelital o por cable podrá proporcionar información individual identificable con respecto a cualquiera de sus suscriptores (incluidos los hábitos de visualización de televisión, las opciones de compra, los intereses, las opiniones, los usos de energía, la información médica del suscriptor, datos o información bancaria, o cualquier otra información personal o privada) sin el consentimiento expreso por escrito del suscriptor. En la Sección 637.5(b) se especifica que las respuestas de visualización de los suscriptores individuales u otra información identificable individualmente derivada de los suscriptores pueden ser retenidas y utilizadas por una empresa de televisión por cable o satélite solo en la medida en que sea razonablemente necesario para fines de facturación y prácticas comerciales internas y para monitorear la recepción no autorizada de servicios. Finalmente, la Sección 637.5(d) se especifica que cualquier información de un suscriptor individualmente identificable recopilada por una empresa de televisión por satélite o por cable debe estar disponible para su examen dentro de los treinta (30) días posteriores a la recepción de la solicitud por un suscriptor para examinar la información en las instalaciones de la empresa.

En cuanto al fondo del tema, dicho Comité avanza en la historia de Internet de las Cosas y destaca que, actualmente todo, desde tostadoras y muñecas, hasta automóviles y

televisores, están conectados a Internet, reuniendo y aplicando una amplia gama de información. Esta tecnología tiene posibilidades ilimitadas. Ha revolucionado las capacidades de los dispositivos médicos y ha facilitado las compras. Los expertos de la industria prevén una expansión dramática en los próximos años con artículos para el hogar, como refrigeradores, lavadoras, lavavajillas y termostatos. Muchos de estos dispositivos recopilan una gran cantidad de información personal e íntima. Si no se asegura adecuadamente, esta inmensa cantidad de información privada puede ser vulnerable a las violaciones y puede ser hackeados directamente permitiendo a extraños realizar una vigilancia subrepticia en los hogares o comunicarse directamente a través de ellos. Quizás lo más perturbador, sea que los consumidores ni siquiera están al tanto de las completas capacidades de estos productos o de la información que se recopila. El Director del FBI expresó su preocupación sobre en tremendo daño que pueden generar los "ejércitos de zombis" creados por los dispositivos de Internet de las Cosas. Finaliza resaltando las bondades del proyecto de ley para abordar estas innovaciones y sus riesgos concomitantes, ya que establece requisitos relacionados con la seguridad de dichos dispositivos y la divulgación de sus capacidades (SENATE JUDICIARY COMMITTEE, 2017).

Dicha Ley se incorporó al Código Civil de California en la División 3 (Obligaciones), Parte 4 (Obligaciones Derivadas de Transacciones Particulares) bajo el Título 1.81.26. Seguridad de la Dispositivos Conectados (*Security of Connected Devices*). Su ámbito de aplicación tiene efectos extraterritoriales, ya que abarca a todos aquellos fabricantes de dispositivos conectados a la Web que vendan en California, aunque la fabricación se produzca fuera de dicho Estado, y establece estándares de ciberseguridad para dispositivos conectados a la web, desde termostatos hasta cámaras web y automóviles.

a) En primer lugar, en el Título 1798.91.04.(a) se requiere que los fabricantes de dispositivos conectados a Internet (que vendan sus productos en California) los equipen con "una característica o características de seguridad razonables" diseñadas para evitar que cualquier intruso acceda a ellos, aunque no define exactamente cuáles deberían ser esas características. Lo que detalla es que la seguridad razonable debe ser:

    1) Adecuada a la naturaleza y función del dispositivo.

    2) Adecuada a la información que puede recopilar, contener o transmitir.

3) Diseñada para proteger el dispositivo y cualquier información contenida en el mismo contra el acceso, destrucción, uso, modificación o divulgación no autorizados.

b) A continuación, bajo el apartado b), se exige que todo dispositivo conectado fuera de una red de área local sea equipado con un medio de autenticación con una característica de seguridad razonable. Considera una característica de seguridad razonable si cumple cualquiera de los siguientes requisitos:

1) La contraseña preprogramada es única para cada dispositivo fabricado.

2) El dispositivo contiene una función de seguridad que requiere que un usuario genere un nuevo medio de autenticación antes de otorgarle acceso al dispositivo por primera vez.

Esto se debe a que muchas veces ha sido una práctica común del fabricante proporcionar dispositivos con contraseñas predeterminadas compartidas, lo que significa que se puede acceder fácilmente al dispositivo después de la instalación si el usuario final no establece una nueva contraseña.

En el artículo 1798.91.05. se establecen varias definiciones:

a) "Autenticación" significa un método para verificar la autoridad de un usuario, así como el proceso o dispositivo para acceder a los recursos en un sistema de información.

b) "Dispositivo conectado" se define como cualquier dispositivo u otro objeto físico que sea capaz de conectarse, directa o indirectamente, a Internet y que tenga asignada una dirección de Protocolo de Internet o una dirección de Bluetooth.

c) "Fabricante" es la persona que fabrica, o que subcontrata la fabricación en su nombre de los dispositivos conectados a la Web que se venden o que se ofrecen para la venta en California. Un contrato para fabricar en nombre de otra persona no incluye el contrato que tiene por objeto solo comprar un dispositivo conectado, incluso si esos dispositivos se renombran para el comprador.

d) "Función de seguridad" significa una característica de un dispositivo diseñado para proporcionar seguridad para ese dispositivo.

e) "Acceso, destrucción, uso, modificación o divulgación no autorizados" es acceso, destrucción, uso, modificación o divulgación que no está autorizado por el consumidor.

En el artículo 1798.91.06.(a) establece determinadas exclusiones o excepciones a la aplicación de los artículos precedentes:

a) Los fabricantes no tienen la obligación de proteger los programas de software que los usuarios pueden instalar en un dispositivo conectado.

b) No impone ninguna obligación a un proveedor de una tienda electrónica, puerta de enlace, mercado u otros medios de compra o descarga de software o aplicaciones, de controlar o hacer cumplir los establecidos en el Título.

c) Exime al fabricante de un dispositivo conectado de evitar que un usuario tenga control total sobre un dispositivo conectado, incluida la capacidad de modificar el software o el firmware que se ejecuta en el dispositivo a discreción del consumidor.

d) Tampoco se aplicara a ningún dispositivo conectado cuya funcionalidad esté sujeta a los requisitos de seguridad de acuerdo con la ley federal, los reglamentos o las directrices promulgadas por una agencia federal.

e) No establece ningún tipo de acción privada. El Fiscal General, un abogado de la ciudad, el abogado del condado o un fiscal de distrito tendrán la autoridad exclusiva para hacer cumplir la ley.

f) Los deberes y obligaciones impuestos son acumulativos con cualquier otro deber u obligación impuesto en virtud de otra ley, y no deben interpretarse en el sentido de eximir a ninguna parte de ningún deber u obligación impuesta en virtud de otra ley.

g) En ningún caso se limita la autoridad de una agencia federal para obtener información sobre el dispositivo conectado de un fabricante como lo autoriza la ley o de conformidad con una orden de un tribunal de jurisdicción competente.

h) Los proveedores de atención médica, socio comercial, plan de servicios de atención médica, contratista, empleador o cualquier otra persona sujeta a la Ley Federal de Portabilidad y Responsabilidad de Seguros de Salud de 1996 (Ley Pública 104-191) o la Ley de Confidencialidad de Información Médica no estarán sujetos a este título con respecto a cualquier actividad regulada por esos actos.

California continúa liderando en la promulgación de leyes de privacidad y seguridad. Esta ley se produce inmediatamente después de la promulgada Ley de Privacidad del Consumidor de California (CCPA), que también entrará en vigencia el 1 de enero de 2020 y que tienen efectos extraterritoriales.

4. Argumentos a favor y en contra de la reciente ley: luces y sombras

4.1. Argumentos en contra

Uno de sus acérrimos detractores es el experto en ciberseguridad Robert Graham. Sus afirmaciones son lapidarias en cuanto califica a la ley como "típicamente mala", basada en una comprensión superficial de la ciberseguridad y la piratería, que va a hacer poco para mejorar la seguridad, mientras que hace mucho para imponer costos y dañar la innovación. Se basa en el concepto erróneo de agregar características de seguridad, el objetivo de la ciberseguridad es eliminar "características inseguras", lo cual significa eliminar puertos de escucha. Agregar características es la típica "píldora mágica" o "bala de plata", sin embargo, según este especialista, no es la solución. Las funciones arbitrarias como *firewall* y antivirus solo aumentarán la superficie de ataque empeorando las cosas ya que no existe garantía que los proveedores suministren dichos parches o, peor aún, que los usuarios los apliquen. Generalmente, las personas se olvidan de los dispositivos una vez que están instalados ya que no son como los teléfonos y/o computadoras portátiles que notifican a los usuarios sobre la aplicación de parches. Frente al argumento que una buena solución para esto es la actualización automatizada, el especialista afirma que solo si se ignora la historia. Muchos

califican a *NotPetya*[10] como el peor y más costoso ciberataque de todos los tiempos y fue lanzado subvirtiendo un parche automatizado. Por ejemplo, el gusano *Mirai*[11] infectó menos de 200.000 dispositivos. Un hackeo de un pequeño proveedor de Internet de las Cosas puede obtener el control de más dispositivos que eso de una sola vez. Y sigue sumando críticas ya que afirma que la ley tiene como objetivo una característica insegura que debe eliminarse: las contraseñas codificadas. Un dispositivo no tiene una contraseña única, hay muchas cosas que pueden llamarse contraseñas. Un dispositivo típico de Internet de las Cosas tiene un sistema para crear cuentas en la interfaz de la administración web, un sistema de autenticación completamente separado para diferentes servicios como Telnet[12] y un sistema completamente diferente para cosas como las interfaces de depuración. Ese fue el real problema con los dispositivos infectados por *Mirai* ya que había diferentes sistemas de autenticación en la interfaz web y en otros servicios como Telnet. De cara al futuro, lo más importante para protegerse es el modo de "aislamiento" en el punto de acceso WiFi que evita que los dispositivos se comuniquen entre sí (o se infecten entre sí). Esto evita ataques de "sitio cruzado" en el hogar, es decir, que las laptops y/o computadoras de escritorio infectadas (que están mucho más amenazadas) se propaguen a los demás dispositivos. La ley establece el vago requisito que los dispositivos tengan características de seguridad "razonables" y "apropiadas", pero es imposible para una empresa saber lo que significan estas palabras y si cumplen con la ley. Al igual que otras leyes que utilizan estos términos, se interpretará en los tribunales. A medida que los defensores mejoran la seguridad, los atacantes cambian de táctica, por lo que lo "razonable" está cambiando constantemente. La seguridad lucha contra el sesgo de la retrospectiva, por lo que lo que es "razonable" y "apropiado" parece más obvio después que ocurren cosas en lugar de antes. Se va a cargar a los dispositivos con funciones de cifrado y antivirus que el público cree que son razonables pero que empeoran la seguridad. Por último, culmina su análisis, Mirai solo

10 Petya es un *malware* de tipo *ransomware* que en 2017 comenzó un ciberataque mundial. Se esparce como troyano usando el popular sistema de archivos en la nube Dropbox. Mientras la mayoría de los malware de secuestro de computadoras selecciona los archivos a encriptar, Petya aumenta el daño potencial al impedir el arranque de la computadora, pidiendo rescate y no se transmite por Internet sino por redes privadas.

11 Mirai es un malware de la familia de las botnets o robots informáticos destinado a infectar los equipos conformantes del Internet de las Cosas, en especial la infección de routers y cámaras IP

12 Telnet (*Telecommunication Network*) es el nombre de un protocolo de red que permite acceder a otra máquina para manejarla remotamente

tenía 200.000 dispositivos que estaban principalmente fuera de los Estados Unidos. Esta ley no aborda esta amenaza porque solo se aplica a los dispositivos de California, no a los comprados en Vietnam y Ucrania que, una vez que se infecten, inundarán los dispositivos de California. Si de alguna manera la ley influyera en la mejora general de la industria, aún estaría introduciendo costos innecesarios a 20 mil millones de dispositivos en un intento por limpiar el 0,001% de ellos (GRAHAM, 2018).

En igual sentido se expidió la Cámara de Comercio de California, que señaló que la Sección 1798.81.5(b) del Código Civil ya requería que los fabricantes implementasen protecciones de privacidad razonables y, por lo tanto, el requisito que los fabricantes equipen dispositivos con "características de seguridad razonables y apropiadas para la naturaleza del dispositivo" era innecesario. La Sección 1798.81.5(b) se aplica a la "información personal" que una empresa posee, licencia o mantiene, y se define como el nombre de usuario o la dirección de correo electrónico de una persona en combinación con la contraseña, la pregunta de seguridad o el nombre de una persona en combinación con un número de seguro social, número de licencia de conducir, número de cuenta o información médica. Otro argumento en contra es que colisiona una ley federal, la Ley de Protección de la Privacidad en Línea de los Niños, aunque no justifica ni aclara esa contradicción.

4.2. Argumentos a favor

Para sus defensores, si bien no desconocen que la ley es demasiado amplia, aducen a su favor que mejor eso que nada. Bruce Schneier, tecnólogo de seguridad en la Escuela Kennedy de Harvard, expresamente opina que probablemente la ley no va lo suficientemente lejos, pero esa no es razón para no aprobarla. Es una razón para seguir adelante y sienta las bases para una futura legislación de ciberseguridad más sólida a nivel estatal y federal. Después del ataque masivo de la botnet *Mirai* en 2016 se puso de relieve lo mal asegurados que están muchos de los dispositivos. En ese incidente, los piratas informáticos explotaron las debilidades de las cámaras web y otros dispositivos conectados y los utilizaron para lanzar ataques cibernéticos que derribaron a Netflix, Spotify y otros sitios web importantes durante horas. Esta ley busca abordar algunas de esas fallas, estableciendo estándares de ciberseguridad para dispositivos, que actualmente son inexistentes (HAWKINS, 2018).

Conforme el Comité de Reglas del Senado, Oficina de Análisis de la Sala del Senado, que toma como fuente los argumentos de *Common Sense Kids Action*, un ejemplo alarmante

de la posibilidad de abuso de la tecnología surgió en relación con las muñecas *My Friend Cayla*. Las muñecas de juguete estaban equipadas con tecnología *bluetooth* que les permitía acceder a Internet, lo cual les posibilitaba comunicarse con los niños. Las muñecas instaron a los niños a proporcionar verbalmente datos personales, incluidos los nombres de sus padres, de su escuela y el lugar donde vivían. Además, la tecnología *bluetooth* era vulnerable a los piratas informáticos pudiendo programar la muñeca con obscenidades o incluso hablar directamente con los niños a través de ella a una distancia de hasta cincuenta (50) pies.

Pero éste no fue un hecho aislado, es similar a muchas historias relacionadas con monitoreos de bebés que permiten a los piratas informáticos comunicarse a través de ellos. A principios del año 2017, se informó que los juguetes de *CloudPets* fueron hackeados de manera similar. También se han presentado demandas en los últimos años en respuesta a televisiones conectados a Internet. Las pantallas inteligentes producidas y vendidas por Vizio supuestamente rastreaban el historial de visualización de los usuarios sin el conocimiento y consentimiento de los clientes. Los televisores de Samsung también fueron el centro de atención después que se descubrió que su tecnología de reconocimiento de voz estaba grabando conversaciones personales y transmitiendo la información a terceros. Los investigadores también han concluido que miles de cámaras web inseguras fabricadas por la firma china de electrónica *Xiongmai* fueron tomadas por piratas informáticos y se convirtieron en un ejército de "botnets" que atacó e inhabilitó los sitios web más importantes, incluidos Twitter, Spotify, New York Times y Airbnb en octubre del 2016.

Según el SENATE RULES COMMITTEE. SENATE FLOOR ANALYSIS (2018), California reconoce al derecho a la privacidad como un derecho fundamental, y desafortunadamente, debido al tamaño de su economía y al gran número de consumidores, los datos recopilados y en poder de las empresas de California son a menudo blanco de los ciberdelincuentes. Los innumerables ejemplos de dispositivos conectados a Internet que se piratean junto con la creciente incidencia de violaciones de datos ponen de relieve la necesidad de abordar más a fondo los problemas de seguridad. Un hilo común entre estos ejemplos es la deficiencia de las características de seguridad de los dispositivos. También falta una notificación clara a los consumidores acerca de qué es capaz un dispositivo, qué información recopila, qué hace con esa información y cómo un consumidor puede controlar esas funcionalidades. El daño que puede resultar del robo de información personal y confidencial a través de las violaciones de datos, la vigilancia encubierta de las vidas de los usuarios o el pirateo directo de dispositivos domésticos amenaza con socavar la privacidad y la seguridad de los

consumidores de California. De esta manera, consideraron que la ley da un paso para abordar estos problemas; y que, si bien existen leyes que exigen que las empresas que poseen, licencian o mantienen información personal sobre un residente de California implementen y mantengan procedimientos y prácticas de seguridad razonables adecuados a la naturaleza de la información, así se hacen extensivos estos requisitos a los fabricantes de dispositivos conectados a Internet.

Como cierre de los argumentos en defensa de la ley, el Informe del Procurador General del 2014 sobre la violación de datos en California demostró que, en 2012, el 17% de las violaciones de datos registradas en los Estados Unidos se produjo en California, más que en cualquier otro Estado, y que el número de violaciones notificadas en California aumentó en 28% en 2013. (CALIFORNIA DEPARTMENT OF JUSTICE, 2014). Durante el período de cuatro años comprendido entre 2012 y 2015, el Fiscal General recibió informes sobre más de 657 violaciones, que afectaron a más de 49 millones de registros (CALIFORNIA DEPARTMENT OF JUSTICE, 2016).

5. Conclusiones

Internet es probablemente el mayor invento de la historia de la humanidad desde la rueda. Ha puesto al alcance de las computadoras de los celulares, *tablets*, televisores y demás electrodomésticos, más información que toda la contenida en la Biblioteca de Alejandría. Ha cambiado la forma de trabajar, de estudiar y hasta de relacionarnos con otros seres humanos de distintas culturas, religiones, razas o nacionalidades. Es la mayor herramienta de conocimiento diseñada y está presente en todas las actividades humanas. Nadie niega su potencial y el beneficio y confort que genera, pero también tiene su lado oscuro. Los videos, fotos, emails, conversaciones, cuentas bancarias y cualquier otro dato personal que se sube a la red, están expuesto a un número indeterminado de personas.

Actualmente, los hogares comienzan a equiparse con dispositivos "inteligentes". La tecnología que alguna vez estuvo limitada a computadoras o teléfonos celulares ahora está integrada en los aparatos y juguetes de uso cotidiano. Dadas las capacidades cada vez mayores de esta tecnología para recopilar y sintetizar información, la seguridad y la privacidad son de suma importancia. Los informes generalizados de fallas de seguridad, piratería y espionaje solo han enfatizado aún más la necesidad de protecciones jurídicas.

Si bien existen proyectos de leyes a nivel estadual y regional (como en la Unión Europea), la primera Ley sobre Internet de las Cosas fue recientemente promulgada, a fines de septiembre de 2018, por el Gobernador del Estado de California, marcando un importante hito jurídico en la regulación de esta nueva tecnología. Tanto sus detractores como sus defensores coinciden en su amplitud y generalidad, pero es de destacar que reviva el debate, propiciando su discusión a nivel nacional, regional e internacional y que sienta un punto de inflexión en la protección de los consumidores de los dispositivos conectados, quienes, en especial los niños, utilizan esos productos inocentemente y sin saber que indirectamente están transmitiendo toda su información a la nube. Lo que muchos no advierten es que detrás de esa nube hay personas y organizaciones dispuestas a utilizar para su provecho toda esa información (hackers, piratas informáticos, contrabandistas, ladrones y abusadores de menores) poniendo en riesgo la privacidad e integridad de las personas. En este sentido, esta ley exige a los fabricantes de tales dispositivos que alerten a los consumidores con señales auditivas y/o visuales cuando el mismo está transmitiendo información personal. Un consumidor informado y capacitado es más difícil de engañar, es una manera de empoderar al consumidor.

Generalmente el derecho se escribe después de los hechos, en este caso es necesario adelantarse a cualquier ciberataque y esta ley puede ser un punto de partida, en especial en Argentina, que todavía ni se presentó un proyecto de ley que abriera el debate.

El periodista de investigación y escritor español Antonio SALAS en *Los hombres que susurran a las máquinas* (2015) plantea el dilema de los televisores inteligentes, por ejemplo Samsung, que ya en su manual de instrucciones advierte que todas las palabras emitidas dentro del alcance del televisor formarán parte de los datos capturados y transmitidos a un tercero a través de su uso de la función reconocimiento de voz. Pero es difícil que en el comedor o en el dormitorio no hablemos de cuestiones familiares y confidenciales. Esta nueva tecnología vino para quedarse y cada vez irrumpe con mayor asiduidad en nuestra vida cotidiana, que no nos tome desprevenidos.

Referencias

CALIFORNIA DEPARTMENT OF JUSTICE (2014) *California Data Breach Report,* consultado en [https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf] el 11.12. 2018

— (2016) *California Data Breach Report,* consultado en [https://oag.ca.gov/breachreport2016] el 09.12.2018.

CALIFORNIA LEGISLATIVE INFORMATION (2018) *Bill History. SB-327 Information privacy: connected devices. (2017-2018)*, consultado en [https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB327] el 03.12.2018.

CASALET, M. (2018) *La digitalización industrial: un camino hacia la gobernanza colaborativa. Estudios de casos*. Santiago de Chile, Comisión Económica para América Latina y el Caribe (CEPAL).

COLINA, A., *et al* (2015) *Internet de las Cosas*. W.S. Science.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL) (2016) *La nueva revolución digital. De la Internet del consumo a la Internet de la producción*. Santiago de Chile, Naciones Unidas.

— (2018) *Datos, algoritmos y políticas. La redefinición del mundo digital*. Santiago de Chile, Naciones Unidas.

20 MINUTOS (2016) "Domótica: cómo automatizar tu hogar para disfrutarlo más mientras ahorras tiempo y dinero", consultado en [https://blogs.20minutos.es/un-hogar-con-mucho-oficio/2016/11/03/domotica-como-automatizar-tu-hogar-para-disfrutarlo-mas-mientras-ahorras-tiempo-y-dinero/] el 15.03.2017.

GALLEGO GÓMEZ, C. y DE PABLOS HEREDERO, C. (2016) "El impacto de un nuevo paradigma tecnológico-social: el Internet de las cosas y la capacidad de innovación", en *Harvard Deusto Business Research,* volumen V, número 2, pp. 149-161.

GARTNER (2013) "Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets", consultado en [http://www.gartner.com/newsroom/id/2621015] el 02.05.2017.

— (2017) "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017 up 31 Percent from 2016", consultado en [https://www.gartner.com/newsroom/id/3598917] el 02.05.2017.

GRAHAM, R. (2018) "California's Bad IoT Law", en *Errata Security*, consultado en [https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XBbQ-lwzbIV] el 12.12.2018.

HAWKINS, D. (2018) "The Cybersecurity 202: California's Internet of Things Cybersecurity Bill Could Lay Groundwork for Federal Action", en *The Washington Post*, consultado en [https://www.washingtonpost.com] el 14.12.2018.

MCKINSEY & COMPANY (2018) *The Internet of Things: How to Capture The Value of IoT*, consultado en [https://www.mckinsey.com] el 02.12.2018.

MICROSOFT (2018) *The Future Computed: Artificial Intelligence y and its Role in Society*. Redmond, Washington, Microsoft Corporation

INFOBAE (2016) "Polémico: una pulsera envía descargas eléctricas para fomentar el ahorro", consultado en [https://www.infobae.com/2016/05/23/1813599-polemico-una-pulsera-envia-descargas-electricas-fomentar-el-ahorro/] el 15.03.2017.

POOLE, E. (2014) "El mundo nuevo de la tecnología ponible: ¿Qué consecuencias tiene para la propiedad intelectual (P.I.)?", en *Revista de la Organización Mundial de la Propiedad Intelectual*, número 3, junio/2014, pp-9-16.

SALAS, A. (2015) *Los Hombres que Susurran a las Máquinas*. Madrid, Espasa.

TEJERO LÓPEZ, A. y MARTÍNEZ SALLES, I. (2014) *Seguridad en el Internet de las Cosas. Retos y oportunidades detectadas*. Madrid, Centro de Apoyo a la Innovación Tecnológica (CAIT), Universidad Politécnica de Madrid.

UNIÓN EUROPEA. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2014) "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos", adoptado el 16 de septiembre de 2014. *1471/14/ESWP 223*.

SENATE JUDICIARY COMMITTEE (2017) *Information privacy: connected devices,* consultado en [https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB327] el 05.12.2018.

SENATE RULES COMMITTEE. SENATE FLOOR ANALYSIS (2018) *SB-327 Information privacy: connected devices,* consultado en [https://leginfo.legislature.ca.gov] el 12.12. 2018.

THE ECONOMIST (2017) "The World's Most Valuable Resource Is No Longer Oil, But Data", consultado en [https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worldsmost-valuable-resource] el 03.08.2018.