www.upo.es/revistas/index.php/lex_social/index
enero - junio 2019
Vol. 9 núm 1/ 2019
Revista jurídica de los Derechos Sociales
Lex Social

# ALCANCES JURÍDICOS, TECNOLÓGICOS Y COMERCIALES DE LA PRIMERA LEGISLACIÓN SOBRE INTERNET DE LAS COSAS

## *LEGAL, TECHNOLOGICAL AND COMMERCIAL SCOPE OF THE FIRST LEGISLATION ON THE INTERNET OF THINGS*

*ADRIANA MARGARITA PORCELLI*

*Profesora Adjunta Ordinaria*
*Universidad Nacional De Luján*

Artículo recibido el 19 de diciembre de 2018
Artículo aceptado el 12 de enero de 2019

**RESUMEN**

Internet no sólo es solo un nuevo medio de comunicación sino que se está convirtiendo en una capa de realidad que interviene en los distintos tipos de relaciones humanas: comerciales, afectivas, políticas, académicas, laborales y culturales. Durante las últimas décadas ha evolucionado de forma tan veloz que abarca aspectos antes inimaginables. Computadoras, impresoras, celulares, tablets, televisores inteligentes, luces, electrodomésticos y hasta la cerradura de las casas se pueden conectar a Internet y ser manejados a distancia para confort del consumidor. Pero también acarrea sus riesgos, la Web no es ni será 100 por ciento segura y las personas pueden ser víctimas de todo tipo de delitos. En consecuencia es necesario el dictado de normas que protejan la información personal y proporcionen mayor seguridad en el manejo de los dispositivos conectados a la Red.

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 tales efectos, este artículo comprende dos partes: la primera que delimita el marco conceptual-

tecnológico, proporciona ejemplos de las diferentes tecnologías en la vida cotidiana y empresarial 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.

**PALABRAS CLAVE:** Internet de las cosas, legislación, California, privacidad, ciberseguridad.

**ABSTRACT**

The Internet isn´t only a new means of communication, it´s becoming a layer of reality that intervenes in the different types of human relationships: commercial, affective, political, academic, labor and cultural. During the last decades it has evolved so quickly that it covers previously unimaginable aspects. Computers, printers, cell phones, tablets, smart TVs, lights, appliances and even the lock of the houses can be connected to the Internet and be operated remotely for the comfort of the consumer. But it also carries its risks, the Web isn´t and will not be 100 percent safe and people can be victims of all types of crimes. Consequently, it´s necessary to dictate rules that protect personal information and provide greater security in the management of devices connected to the Network.

The present work consists in defining and enumerating the necessary components for the functioning of the ecosystem called Internet of Things and analyze the California Law N ° 327 Information privacy: connected devices. To this end, this article has two parts: the first one, which delimits the conceptual-technological framework, provides examples of different technologies in everyday and business life and the second examines the different principles adopted in Law No. 327 Information privacy: connected devices, and at the same time presents its harshest criticism as well as the arguments in its defense.

**KEY WORDS:** Internet of things, legislation, California, privacy, cybersecurity.

*SUMARIO*

## 1. Introducción

Los economistas afirman que la humanidad se encuentra en el preludio de la Cuarta Revolución Industrial, llamada también Industria 4.0 (término utilizado por primera vez en la Feria de Hanover, Alemania, en el año 2011), continuadora de los otros tres procesos históricos transformadores**:** la Primera Revolución Industrial (entre 1760 y 1830) marcó la transición de la producción manual a la mecanizada, la Segunda, alrededor de 1850, introdujo la electricidad y permitió la manufactura en masa y la Tercera, a 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 mismas, sino por 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[1].

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 novedosos de esta nueva revolución, que a diferencia de las anteriores que se desarrollaron exclusivamente en el mundo físico, la actual conecta ese ámbito físico con el espacio digital, utilizando como medio de comunicación Internet (Internet de las Cosas, IOT, siglas en inglés de *Internet of Things*) y como mensaje los propios metadatos o datos (*Big Data*).

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.

[1] Perasso (2016)

[2] Según "The world's most valuable resource is no longer oil, but data" (6 de mayo de 2017) *The Economist.* Londres, [Consultado el: 3/8/2018]. Disponible en https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worldsmost-valuable-resource.

En el entorno digital y las redes sociales, el internauta convierte sus amistades, deseos, intereses, emociones, preguntas y búsquedas en datos que luego son procesados para determinar patrones de consumo. A esta tarea se la denomina "*digital labor*" o "*trabajo digital*". 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 por ciento lo hacía con suscripciones a servicios móviles. Por otra parte, el 61 por ciento de dichas suscripciones operaban sobre redes 3G o 4G y durante el 2017 se descargaron 175.000 millones de aplicaciones y se usaban activamente 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 por ciento utilizaba teléfonos inteligentes. En enero de 2018, más de 3.000 millones de personas- el 42 por ciento 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 por ciento 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[3].

Según estimaciones realizadas por la consultora Gartner, en 2020, el número de objetos conectados a Internet será de más de 26.000 millones (excluyendo PCs, *tablets* y *Smartphone*) y que la Internet de las Cosas aportará por sí misma 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[4].

En sintonía, el estudio del *McKinsey Global Institute*, intitulado **"***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[5].

De lo anteriormente expuesto, se puede deducir que Internet de las Cosas genera una enorme cantidad de datos transmitidos o *Big Data*, que analizan grandes volúmenes de datos 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

[3] Comisión Económica para América Latina y el Caribe. CEPAL (2018)
[4] Gartner (2013)
[5] McKinsey & Company (2018)

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. El poder de los datos masivos combinados con inteligencia artificial ya ha demostrado que puede prever el comportamiento humano y modificarlo. 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 están empezando a hacer usados y más que usados, reutilizados, porque no solo se utilizan para el fin que fueron recolectados sino para los más variados propósitos.

Las principales cinco compañías que diseñan el nuevo paradigma de producción están redefiniendo los conceptos de valor y capital dominantes durante el siglo pasado. 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, debe 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).

En relación con las políticas y procedimientos para la investigación de vulnerabilidades relacionadas con la ciberseguridad e interconexión de un dispositivo a Internet, por lo general se basan en la Norma ISO 29147 *Information technology- Security techniques-Vulnerability disclosure* y cualquier otra norma estándar que la suceda.

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*, para que la Comisión Federal de Comercio desarrollara recursos de ciberseguridad en la educación y la concientización de los consumidores con respecto a la compra y el uso de dispositivos que forman parte de la Internet de las Cosas y otros fines. 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*, el cual al 29 de noviembre de 2018 tuvo dos leídas por parte del Senado, para encomendar al Secretario de Comercio a realizar un estudio y presentar al Congreso un informe sobre el estado de la industria de dispositivos conectados a Internet en los Estados Unidos.

Pero ninguna de las iniciativa señaladas *ut supra*, 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 *Title 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 tales efectos, este artículo comprende dos partes: la primera que delimita el marco conceptual-tecnológico, proporciona ejemplos de las diferentes tecnologías en la vida cotidiana y empresarial 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

### 2.1. 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, para citar algunos ejemplos. 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)[6].

Conforme el "Dictamen 8/2014 sobre la evolución reciente de la Internet de los Objetos", adoptado el 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[7].

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 se encuentre presente en su vida cotidiana, sin tener que acudir a *tablets* y *smartphones* que son más pesados. Por ejemplo las *Google Glass* que son una computadora ponible que incluye un pequeño dispositivo de visualización de cristal líquido. Se activa por medio de 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 y, entre otras cosas, se pueden 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, en 2006, el dispositivo para la práctica deportiva *Nike+iPod*. Desde entonces, su línea de productos se ha ampliado y ahora incluye aplicaciones para *iOS y Android*, un reloj multifuncional con GPS y la banda *Nike Fuel*. Otro ejemplo es *Mimo Baby*, la prenda de vestir inteligente para bebés fabricada por *Rest Devices* en Estados Unidos. Es un monitor ponible para bebés que permite que los padres controlen las estadísticas vitales del bebé como la respiración, el nivel de actividad y la temperatura de la piel. [8]

Otro ejemplo destacable lo constituye la compañía británica *Intelligent Environments* la cual desarrolló una plataforma virtual que se conecta a una pulsera que envía pequeñas

[6] Comisión Económica para América Latina y el Caribe. CEPAL (2016)
[7] Ver Unión Europea. Grupo de Trabajo sobre Protección de Datos del Artículo 29. "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos". Adoptado el 16 de septiembre de 2014. *1471/14/ESWP 223*. Este Grupo de trabajo 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.
[8] Poole, E. (2014)

descargas eléctricas (de 17 a 340 voltios) al usuario, cuando sus gastos superan lo deseado.[9]

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, pero a la vez **s**e recogen todos los datos de las personas, la velocidad, la forma de conducir, el tiempos de los trayectos. En Alemania produjo serios problemas legales porque cuando una persona veía el primer retén policial, informaba inmediatamente a las demás y los sospechosos, alertados, tomaban otra ruta.

c) Domótica: por tal concepto se entiende el 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.[10]

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.

Uno de los mayores ejemplos del ahorro son los modernos controles de calefacción. Consisten en un termostato inteligente que dota a la calefacción de un envidiable cerebro digital, conectado al *smartphone* o *tablet* mediante una aplicación que habilita manejarlo desde cualquier lugar y en cualquier momento. Permite comprobar y programar la temperatura, adecuarla al clima existente minuto a minuto -se conecta a la previsión del tiempo para ayudar a reducir el consumo cuando sale el sol- y revela el dinero gastado durante el día, semana o periodo temporal determinado. Otro ejemplo de ahorro es automatizar las luces de la casa, lo que permitirá programar su encendido o apagado ajustándolo al horario solar para no desperdiciar ni un vatio de potencia, además de encender y apagar las luces.[11]

[9]Estos ejemplos se pueden consultar en: "Polémico: una pulsera envía descargas eléctricas para fomentar el ahorro". (23 de mayo 23 de 2016). *Infobae*. [Consultado el: 15/3/2017] Disponible en: https://www.infobae.com/2016/05/23/1813599-polemico-una-pulsera-envia-descargas-electricas-fomentar-el-ahorro/

[10]Gallego Gómez, C. y de Pablos Heredero, C. (2016)

[11]Para ampliar en la temática, véase: "Domótica: cómo automatizar tu hogar para disfrutarlo más mientras ahorras tiempo y dinero" (3 de noviembre de 2016) *20 minutos*. [Consultado el: 15/3/2017] Disponible 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/

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, que considera tanto aplicaciones para industrias y procesos específicos (gestión, fabricación, comercialización, distribución y demás), como soluciones multisectoriales (tecnologías ponibles para el monitoreo de la salud, vehículos conectados, ciudades inteligentes y otros). Se prevé que los futuros avances se centren en aplicaciones para ciudades inteligentes y sectores industriales, en las que la creación de valor provendría de una mayor eficiencia energética, aumentos en la productividad del trabajo, reducción de costos de mantenimiento, optimización de la gestión de inventarios y mejoras en la seguridad de los trabajadores. 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 por ciento correspondía a soluciones de consumo personal, como domótica, tecnologías ponibles (*wearable technologies*) o autos conectados, en tanto que el restante 37 por ciento se repartía en soluciones transversales y para sectores específicos.[12]

Por ejemplo, la empresa coreana LG *Electronics* presentó, en septiembre del 2018, en el capítulo latinoamericano de su Innofest 2018**,** la tecnología *ThinQ* conforme la cual los dispositivos "aprenden" a medida que son utilizados y tienen conectividad abierta - mediante Google Assistant y Alexa, de Amazon- con teléfonos y otros dispositivos inteligentes. Los productos con inteligencia artificial presentados cuya comercialización en Argentina se prevé a fines de 2018, fueron:

a) la lavasecadora LG *TWIN Wash ThinQ* que se controla por la voz, aprende y recomienda ciclos de lavado de acuerdo con las prendas y con las preferencias del usuario, y avisa en caso que quede poco jabón. La heladera LG *InstaView ThinQ* cuenta con cámaras internas que permiten ver en tiempo real la mercadería en su interior, además posee un panel de cristal que con dos pequeños golpes se ilumina y permite ver el interior sin necesidad de abrir la puerta -una tecnología presente en otros modelos de la marca-, pero que también se transforma en una pantalla donde se puede visualizar recetas, hacer la lista de compras y comprar.

b) El *LG OLED TV AI ThinQ*, es una TV ultrafina que tiene Google Assistant incorporado, lo que permite controlarla mediante la voz en cinco idiomas (incluido el español) para chequear las tareas diarias, hacerle consultas (desde las condiciones meteorológicas, nombres de personajes hasta ordenar que exhiba fotos) o controlar otros dispositivos compatibles como aires acondicionados o lavarropas. También tiene un procesador alfa 9 que reduce el ruido en las imágenes, potencia los objetos, definiendo texturas y bordes, con colores más precisos.

[12] Gartner (7 de febrero de 2017) "Gartner says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016". [Consultado el: 2/5/2017] Disponible en: https://www.gartner.com/newsroom/id/3598917

En todos los dispositivos está presente la tecnología *Inverter*, que modula con precisión la operación de motores y compresores para aumentar significativamente la eficiencia y el rendimiento energético. Esta funcionalidad reduce el consumo de energía y ofrecen una garantía de 10 años.[13]

Fundamentalmente países como Alemania, Estados Unidos y China, han implementado políticas para reorientar sectores productivos estratégicos hacia la industria 4.0 o la manufactura inteligente articulando el mundo digital con el de las máquinas y el sistema industrial con el avance de la computación, facilitando la recolección de grandes volúmenes de datos a través de las máquinas. 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 manera rentable y ha favorecido a la producción personalizada que satisface las necesidades heterogéneas de los clientes. En la Unión Europea, se destaca el proyecto ATHENA (*Advanced Technologies for Interoperability of Heterogeneous Enterprise Networks and their Applications*) orientado a los sectores aeronáutico y automotriz, el SEINE (*Standards for the extended digital innovative Enterprise*) conducente a mejorar y estandarizar los intercambios de datos y procesos entre OEM (fabricante de equipos originales) y proveedores del sector aeronáutico.[14]

En China, los granjeros están conectando sus rebaños a Internet. Por ejemplo, las vacas usan collares con sensores inalámbricos que recolectan datos biométricos como la temperatura corporal y el ritmo cardíaco, los que se procesan para mejorar la producción de leche y reportan beneficios generales en un 50 por ciento anuales[15].

En base a lo expuesto *ut supra*, 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.[16] Para lograr dicha interconectividad es necesario que todos los objetos que diariamente se manipulan posean sensores capaces de detectarlos, identificarlos o ubicar su posición. Además una dirección IP que los convierta en objetos inteligentes capaces de comunicarse no sólo con otros objetos inteligentes, sino con seres humanos, utilizando un software adecuado y apoyándose en diferentes tecnologías, como por ejemplo identificadores de radiofrecuencia (*radio frecuency identification* RFID), tecnología Bluetooth, ZigBee (una

[13]Robledo (2018)
[14] Casalet, M (2018)
[15] Hu (2018)
[16] VV.AA. (2015)

de las más avanzadas tecnologías para integrar la casa automatizada y los artefactos inteligentes), WiFi o Internet móvil de los celulares.

Por tanto, la Internet de las Cosas no es solo la conectividad de elementos físicos, es un ecosistema compuesto de dispositivos, redes de comunicación, plataformas de software y aplicaciones. Dentro de ese ecosistema se puede identificar los siguientes componentes:

a) Una Red de Sensores Inalámbricos (WSN, siglás en inglés de *wireless sensor network*) 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. Estas redes son un puente entre el mundo físico y el mundo virtual. Los sensores pueden medir cualidades físicas, tales como la temperatura, humedad y convertirlas en una señal que puede ser leída e interpretada por el microcontrolador. Para que estos sensores sean únicos e identificables y puedan intercomunicarse se utilizan tecnologías como las de identificación por radiofrecuencia (RFID, siglas en inglés de *Radio Frequency Identification*) y comunicación de campo cercano (NFC, siglas en inglés de *Near Field Communication*) que tienen la habilidad de convertir casi cualquier cosa en un componente de la Internet de las Cosas. Esta red de sensores se extiende en una región con el objeto de recolectar datos a través de sus nodos en tiempo real. Algunos de los campos de aplicación se relacionan con el monitoreo ambiental: agricultura, salud y sistemas de seguridad.

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 con el resto de la plataforma de Internet de las Cosas. Proveen de conectividad conforme el sistema inalámbrico o el protocolo de comunicación por cable designado. Según el costo y el desempeño de las distintas tecnologías de conectividad, casi todas la comunicaciones entre esos dispositivos e Internet se realizan de dos formas: a) un nodo intermediario que conecta a Internet como una puerta de enlace (*Gateway*) en donde el aparato es comúnmente conectado a la computadora y envía datos usando, por ejemplo el puerto USB. La computadora recibe esos datos y utilizando el software apropiado, lo envía a la Red o b) esos dispositivos tienen una comunicación directa y permanente a Internet. Este último caso es mucho más sencillo ya que los aparatos pueden funcionar y comunicar los datos de manera más autónoma e inmediatamente. En ambos casos, 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, posiblemente antes de 2020- y las tecnologías por cable, como Ethernet, utilizan el protocolo TCP/IP. Los módulos seleccionados se caracterizan por tener interfaces especiales para conectarse directamente a microcontroladores y plataformas de código abierto como “Arduino”

c) Procesamiento de Información Integrado: Los objetos inteligentes cuentan con una capacidad de procesador o microcontrolador y además capacidad de almacenamiento. Estos recursos pueden utilizarse, por ejemplo, para procesar e interpretar información del sensor, o guardar productos en "memoria" de cómo se han utilizado.

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 sistema 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*. Del mismo modo, los llamados "paradigmas de interacción innovadores" son pertinentes, tales como 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, en los pequeños aparatos es producida por baterías temocúpulas y paneles fotovoltaicos.

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 Pc 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. Resulta importante trabajar en la promoción de estándares y en la interoperabilidad, en las capas de procesamiento inicial y preselección de datos, almacenamiento, integración, procesamiento y accionamiento de dispositivos sino también en materia de los formatos de los datos y los mecanismos de seguridad y protección de la privacidad, que deben ser evaluados con objetivos de estandarización e interoperabilidad con la mayor amplitud geográfica posible. 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 (IP, siglas de *Internet Protocol*) permite interconectar redes de datos de diferente tecnologías y se ha transformado en el estándar para todo tipo de comunicación digital. 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. Desde el año 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet, un cambio indispensable para el desarrollo de la Internet de las Cosas.

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

a) Efectividad en las medidas de seguridad: un limitante consiste en que no se las tienen en cuenta en la fase de diseño. Los dispositivos conectados a Internet no suelen disponer de recursos suficientes, memoria y procesamiento, como para implementar las protecciones necesarias de seguridad a posteriori, o al menos aplicar las medidas de seguridad tradicionales. 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 éstos 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 parte del 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. Las decisiones tomadas de forma automática por dispositivos y aplicaciones, basadas en el enorme conjunto de datos obtenidos podría llevar a la toma de decisiones en forma discriminatoria e incurrir en errores.

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. Es necesario prestar especial atención para obtener la

uniformidad en las legislaciones.[17] Contar con un marco regulatorio internacional resulta indispensable para responder a las amenazas de seguridad específicas y abordar inquietudes sociales respecto de Internet de las Cosas como es el caso de la privacidad, la confianza y la libertad de expresión.

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, habrá desafíos y oportunidades. Por ejemplo, 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. La capacitación para un mundo impulsado por Inteligencia Artificial implica más que ciencia, tecnología, ingeniería y matemática. A medida que las computadoras se comportan más como los humanos, las ciencias sociales y las humanidades se volverán aún más importantes. Los cursos de idiomas, arte, historia, economía, ética, filosofía, psicología y desarrollo humano pueden enseñar habilidades críticas, filosóficas y éticas que serán fundamentales para el desarrollo y la gestión de las soluciones de Inteligencia Artificial. 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.[18]

Es que el potencial de la Inteligencia Artificial puede llegar a supuestos inimaginables. El científico investigador de Google, Ian Goodfellow, desarrolló una innovadora técnica llamada redes generativas antagónicas (GAN, por sus siglas en inglés de *Generative Adversarial Nets*) que les permite a las máquinas generar contenido original y realista, casi como si fueran humanos. Y lo más impactante es que lo logran a través de entrenamiento no supervisado. Básicamente son dos redes que compiten entre ellas, y mientras compiten, están forzadas a mejorar y superarse. Una de ellas es el generador, que es el que crea las imágenes o cualquier otro dato y la otra es el discriminador, que mira una imagen y trata de adivinar si se trata de una imagen real que proviene de los datos o de una imagen falsa originada por el generador. Es un proceso donde cada una de las redes va mejorando y aprende de su oponente y el generador logra hacer imágenes que engañan al discriminador. En la actualidad este tipo de aprendizaje no supervisado es incipiente y se utiliza para diseñar coronas dentales y, en el futuro, se podría emplear para idear por completo una casa: desde el exterior y hasta sus interiores.[19] También el Fondo *Global Goods* está trabajando en un sistema de imágenes por ultrasonido dotado de Inteligencia Artificial que integra un ecógrafo con aprendizaje profundo capaz de detectar automáticamente un ataque de neumonía y su progresión o la respuesta a un tratamiento.[20]

[17] Tejero López (2014)
[18]Microsoft (2018)
[19] Jaimovich, D. (2018)
[20] Vecchione, M. (2018)

Durante los días 29 y 30 de mayo de 2018, Argentina fue sede del Primer Foro sobre Inteligencia Artificial, Internet de las Cosas y Ciudades Inteligentes de América Latina, organizado por la Unión Internacional de Telecomunicaciones (UIT) , el Ministerio de Modernización, Argentina , Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) , Comisión Económica de las Naciones Unidas para América Latina y el Caribe (CEPAL) , Organización de las Naciones Unidas para el Desarrollo Industrial (ONUDI) , Comisión Interamericana de Telecomunicaciones (CITEL) , Comisión Técnica Regional de Telecomunicaciones (COMTELCA) y Telecomunicaciones de América Latina (Asiet) . Las ciudades consumen la mayoría de los recursos del mundo y causan emisiones masivas de gases de efecto invernadero. En América Latina, albergan a casi el 80 por ciento de la población de la región, una cantidad que probablemente aumentará en el futuro. Esto la convierte en una de las regiones más urbanizadas del mundo. Por tanto, el Foro exploró el papel de las nuevas tecnologías, incluida la conectividad de alta velocidad, resistente y de baja latencia y tecnologías como la computación distribuida, Internet de las Cosas, el aprendizaje automático y la Inteligencia Artificial para abordar los desafíos urbanos y dar forma a ciudades más inteligentes y sostenibles. Como documento final, el Foro produjo la Declaración de Buenos Aires, a través de la cual los participantes pudieron realizar un llamado a la acción, que destaca el valor del análisis de datos en tiempo real (basándose en los datos generados por las tecnologías inteligentes) para apoyar una economía circular eficiente en el uso de los recursos. El procesamiento y la gestión de datos éticos, la construcción de la confianza entre los ciudadanos y los recolectores de datos, entre otros, también se reconocieron como fundamentales para lograr todo el potencial de la Inteligencia Artificial e Internet de las Cosas. La declaración señala además la importancia de las normas internacionales para apoyar la interconexión e interoperabilidad de los sistemas de las ciudades. La estandarización y la regulación serán una contribución esencial a las protecciones contra las amenazas de seguridad específicas de Internet de las Cosas. También se alienta a incorporar soluciones de la Inteligencia Artificial a los servicios públicos.[21]

## 2.2. Big Data

Durante el año 2005 se evidenció la gran cantidad de datos que generaban los usuarios a través de Facebook, YouTube y otros servicios online, tanto que, en diciembre de 2011, *Apache Software Foundation* desarrolló *Apache Hadoop (*y en el 2014 *Apache Spark)* un marco de código abierto creado específicamente para almacenar y analizar grandes conjuntos de datos. Estos marcos de código abierto desempeñaron un papel principal en

[21] Para ampliar información, véase: Primer Foro sobre Inteligencia Artificial e Internet de las Cosas en Ciudades Inteligentes y Sostenibles en América Latina. "Declaración de Buenos Aires. Inteligencia Artificial e Internet de las Cosas en Ciudades Inteligentes y Sostenibles en América Latina". 30 de mayo de 2018. *ITU Foro* [Consultado el: 5/8/ 2018] Disponible en: https://www.argentina.gob.ar/sites/default/files/buenosaires-declaration-spanish-final.pdf

el crecimiento del Big Data ya que resultaban más fáciles de usar y más barato de almacenar.

Las revelaciones de Edward Snowden, el uso opresivo de los datos por parte de los gobiernos para identificar y arrestar a personas inocentes y el poder creciente de algoritmos que permiten la discriminación contra los menos favorecidos, son indicadores suficientes del perjuicio que el Big Data puede ocasionar a las sociedades democráticas basadas en los derechos humanos. La discusión social sobre la forma en que un mundo impulsado por los datos debe configurarse apenas comienza, mientras que se sigue creando más y más datos todos los días, pero ahora los humanos no son los únicos que lo hacen. Con la llegada del Internet de las Cosas hay un mayor número de objetos y dispositivos conectados a Internet que generan datos sobre patrones de uso de los clientes y rendimiento de los productos. El Cloud Computing ha ampliado aún más las posibilidades del Big Data ya que ofrece una escalabilidad realmente elástica, donde los desarrolladores pueden simplemente agilizar clústeres ad hoc para probar un subconjunto de datos.[22]

De ahí que, las empresas deban iniciar la transición del *Business intelligence (*Inteligencia de negocios*),* donde se estudia un consumidor en pasado y sus consecuencias; a un *Business analytics* (Análisis de negocios), que se adelanta a las necesidades, analiza los datos en forma conjunta, establece relaciones y comparaciones entre variables para tratar de adelantarse al futuro y construye guías en tiempo real.[23]

En Argentina, la Secretaría de Tecnologías de la Información y las Comunicaciones, dependiente del Ministerio de Comunicaciones emitió, el 1 de junio de 2017, la Resolución N° 11/17 por medio de la cual se creó el "Observatorio Nacional de Big Data" a fin de "analizar la evolución del Big Data", al que define como: *a este conjunto de datos de gran volumen, alta velocidad y/o alta variedad de información, generados a través de la red y mediante el uso de dispositivos inteligentes, que demandan nuevas formas de procesamiento y que incidirán en la toma de decisiones y en la optimización de procesos, se le denomina Big Data.*[24]

Más allá de las definiciones existentes sobre el Big Data, *con dicho término se hace referencia al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo*[25].

[22] Oracle (s.f.)
[23] Rayón. (2015)
[24] El documento se puede consultar en: Argentina. Ministerio de Comunicaciones. Secretaría de Tecnologías de la Información y las Comunicaciones Resolución 11E-2017 Creación del Observatorio Nacional de Big Data. Boletín oficial de la República Argentina, 8 de junio de 2017. Id SAIJ: NV17171
[25]Agencia Española de Protección de Datos (AEPD) y a la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) (2017, p.3)

De estas definiciones se puede inferir que dicho concepto se refiere no sólo a los datos sino también a las instituciones y al ecosistema más amplio que lo produce y utiliza. Engloba infraestructuras, tecnologías y servicios creados para procesar enormes cantidades de datos estructurados, no estructurados o semi-estructurados.

Big Data se refiere al ecosistema creado por la aparición concomitante de "las 3C de Big Data."

La primera C representa las *crumbs* o pedazos de datos emitidos y recolectados de forma pasiva, subproducto de la interacción de las personas con y el uso de dispositivos digitales que proporciona una visión única sobre sus comportamientos y creencias;

La segunda C representa las Capacidades de Big Data, lo que también se conoce como *Big Data Analytics*; es decir, el conjunto de herramientas y métodos, hardware y software, know-how y habilidades necesarios para procesar y analizar este nuevo tipo de datos, incluyendo técnicas de visualización, aprendizaje estadístico automatizado (*machine learning*), algoritmos, etc.;

La tercera C representa las Comunidades de Big Data, y describe los diferentes actores involucrados en el ecosistema de Big Data, desde los generadores de datos hasta sus analistas y usuarios finales; es decir, potencialmente toda la población.

Este ecosistema puede ser descrito y analizado como un sistema complejo, es decir, uno donde existen bucles de retroalimentación entre sus diferentes partes. En los niveles más básicos, las nuevas empresas por ejemplo Twitter ayudan a generar nuevos tipos de datos que a su vez conducen al desarrollo de nuevos tipos de instrumentos analíticos, dando lugar a nuevos tipos de datos, y luego a nuevos actores que toman ventaja de estos nuevos datos y herramientas. Es posible que este nuevo ecosistema pueda convertirse en o ser parte de un fenómeno social más amplio. Presenta cualidades muy marcadas que lo diferencian de las fuentes convencionales de datos: son de gran volumen y pueden componerse de muchos tipos de fuentes generadoras. Por ejemplo, aunque los registros administrativos se componen de grandes cantidades de datos y hojas de cálculo extensas, si su velocidad no aumenta y si su recolección fuese diaria, no serán considerados como Big Data. Big Data no se trata de los datos ni de su tamaño, se trata de datos diferentes que pueden contener señales que no estaban disponibles hace unos pocos años y que los humanos todavía no saben cómo leer o usar y que no se ha solicitado de forma activa e intencional por estadísticos o investigadores. A diferencia de los datos recogidos a través de fuentes tradicionales con el objetivo de responder a una pregunta, Big Data podría dar respuestas a preguntas que ni siquiera han sido formuladas. Son datos nuevos y deben ser considerados como huellas digitales de acciones humanas generadas de forma pasiva por individuos.[26]

El objetivo de Big Data, al igual que los sistemas analíticos convencionales, es convertir el dato en información para la toma de decisiones en tiempo real. Entonces la cantidad de

[26] VV.AA. (2016)

datos no es lo importante sino lo que se puede hacer con ellos ya que se puede analizar para obtener ideas que conduzcan a mejores decisiones y movimientos de negocios estratégicos. La naturaleza compleja del Big Data se debe principalmente a la naturaleza no estructurada de gran parte de los datos generados por las tecnologías modernas, como los web logs, la identificación por radiofrecuencia (RFID), los sensores incorporados en dispositivos, la maquinaria, los vehículos, las búsquedas en Internet, las redes sociales como Facebook, computadoras portátiles, teléfonos inteligentes y otros teléfonos móviles, dispositivos GPS y registros de centros de llamadas.

Pero también se lo caracteriza con 5 v:

1) Volumen es la característica más ostensible y que se traduce en el propio nombre de *Big Data.* La mayoría de los especialistas coinciden en se refiere a conjuntos de datos que van desde 30-50 Terabytes a varios Petabytes.

2) Variedad tanto en la tipología de datos y sus fuentes, como en el tratamiento de éstos, que pasan a ser estructurados, semiestructurados y desestructurados, datos dinámicos o en continuo cambio. Esta variedad y volumen requieren un tratamiento diferente para poder convertirse en información.

3) Velocidad en la captura, movimiento y procesamiento de los datos, llegando a ser en tiempo real en algunos casos. La velocidad también es significativa, ya que el análisis de datos se expande en campos como el aprendizaje automático y la Inteligencia Artificial, donde los procesos analíticos imitan la percepción mediante la búsqueda y el uso de patrones en los datos recopilados. La potencia de cálculo necesaria para procesar rápidamente grandes volúmenes y variedades de datos puede sobrecargar un solo servidor. Por tanto se puede distribuir el trabajo en cientos o miles de servidores y operar de manera colaborativa.[27]

4) Veracidad en cuanto a la calidad de los datos.

5) Variabilidad referido al frecuente cambio del significado de los datos, provocando algunas inconsistencias, y

5) Valor en cuanto a los beneficios del Big Data. Hoy en día, el Big Data se ha convertido en un activo crucial. Gran parte del valor de las empresas tecnológicas procede de sus datos, que analizan constantemente para generar una mayor eficiencia y desarrollar nuevos productos. Recientes avances tecnológicos han reducido exponencialmente el coste del almacenamiento y la computación de datos, haciendo que tales tareas resulten más sencillas y económicas, facilitando la toma de decisiones empresariales más acertadas y precisas. Identificar el valor del Big Data no pasa solo por analizarlo. Se trata de todo un proceso de descubrimiento que requiere que los analistas, usuarios empresariales y ejecutivos identifiquen patrones, tomen decisiones informadas y predigan comportamientos.

[27]"Big Data" (s.f.)

Las fuentes de datos de Big Data son muy amplias, pudiendo provenir de: Internet y móviles, de Internet de las Cosas, recopilados por empresas especializadas y datos experimentales. Y los tipos de datos pueden ser: no estructurados (documentos, vídeos, audios), semi-estructurados (software, hojas de cálculo, informes) y estructurados (bases de datos).

Uno de las principales obstáculos es que no existen estándares de calidad de datos unificados. En 1987 la Organización Internacional de Normalización (ISO, siglas en inglés de *International Organization for Standardization*) publicó las normas ISO 9000 para garantizar la calidad de productos y servicios. Sin embargo, el estudio de los estándares de calidad de los datos no comenzó hasta los años noventa, y no fue hasta 2011 cuando publicó las normas de calidad de datos ISO 8000**.** Estas normas necesitan madurar y perfeccionarse. Además, la investigación sobre la calidad de datos de Big Data ha comenzado hace poco y no hay apenas resultados.

Otro concepto relacionado es el de *data lake* o lago de datos que es un repositorio de almacenamiento a gran escala de cualquier tipo de datos en bruto, en su formato nativo hasta que se necesiten, que además proporciona una gran potencia de cómputo o procesamiento y tiene la potencialidad de gestionar una cantidad prácticamente limitada de tareas concurrentes.

## 3. Regulación Jurídica de Internet de las Cosas. Sección 1 Título 1.81.26 (*Security of Connected Devices*) del Código Civil del Estado de California, Estados Unidos

La Senadora de Santa Bárbara, Hannah-Beth Jackson, presentó, el 3 de febrero de 2017, ante el Senado del Estado de California un proyecto de ley intitulado "*SB-327 Information privacy: connected devices*" (2017-2018)[28]. Posteriormente fue enmendado por la autora, continuó con el tratamiento legislativo y después de las tres lecturas obligatorias, el día 29 de septiembre del 2018, fue promulgado por el Gobernador Jerry Brown y archivado en la Secretaría del Estado. 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 *Title 1.81.26. Security of Connected Devices*[29].

Como requisito para su entrada en vigencia, en la Sección 2, establece que es necesario que el Proyecto de Ley de la Asamblea N° 1906 intitulado *AB-1906 Information privacy: connected devices. (2017-2018)*[30], presentado en enero del 2018 por la asambleísta Jacqui

[28] Las siglas SB significan *Senator Bill*

[29] Para ampliar la historia sobre el tratamiento legislativo, véase United States. California Legislative Information (2018) *SB-327 Information privacy: connected devices. (2017-2018)* [Consultado el: 3/12/2018] Disponible en: https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB327

[30] Las siglas SB significan *Assembly Bill*

Irwin, de Thousand Oaks, también se promulgue y entre en vigencia. Justamente ese mismo día, el 28 de septiembre de 2018, ambos Proyectos de Ley fueron promulgados por el Gobernador. El proyecto de Ley SB-327 es anterior, pero al ser enmendado es casi un espejo del proyecto AB-1906. Sin embargo, la posterior aplicación- de ambas leyes- es diferida al 1° de enero del año 2020. La razón es otorgarles tiempo a los fabricantes de dispositivos conectados a Internet para que puedan adecuar sus productos a la nueva normativa.

En síntesis, se requiere que los fabricantes de dispositivos conectados a Internet los equipen con funciones de seguridad razonables y notifiquen directamente a los consumidores sobre los parches y actualizaciones en la seguridad. También deben diseñar los dispositivos de manera tal que indiquen cuándo está recopilando información y que obtengan el consentimiento del consumidor antes de recopilar o transmitir información. Además obliga a aquellos que vendan u ofrezcan vender estos dispositivos a proporcionar un aviso de las funciones de recopilación de información del dispositivo en el punto de venta.

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 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 es necesaria esta 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 características de seguridad razonables y adecuadas a la naturaleza del mismo y a la 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*[31], patrocinador de la hoy ley, al 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 que recopilan y comparten. Es hora de asegurarse que las familias sepan qué información pueden recolectar los dispositivos que compran y quien tiene el control sobre la misma.

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, la cual, en el art. I Sección 1, establece que todas las personas son por naturaleza libres e independientes y tienen derechos inalienables. Entre estos se encuentran 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. (conforme el caso *Hill v. National Collegiate Athletic Assn*. 1994). 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) 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

[31] *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.

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, en la Sección 22948.20, establece que 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 parte del 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) establece que ninguna empresa de televisión satelital o por cable podrá proporcionar información individual identificable con respecto a cualquiera de sus suscriptores, incluidos, entre otros, 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) 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) 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 30 días posteriores a la recepción de la solicitud por parte de 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. Recuerda que Kevin Ashton fue ampliamente reconocido por haber acuñado la frase *"Internet of Things"* (IoT). El concepto surgió de su investigación en MIT sobre "empaquetado inteligente". La frase hace referencia a la tecnología que permite que una lista cada vez mayor de dispositivos se comunique de forma inalámbrica con otros. Dos décadas más tarde, el concepto es bien conocido y se ha hecho cada vez más popular en los últimos años. 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. El CEO de Cisco ha declarado que Internet de las Cosas generará 19 billones de dólares en ganancias. Sin embargo, trae consigo problemas de privacidad y seguridad. Las corporaciones están conectando rápidamente el mundo físico y reuniendo datos de todo. 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. Además, muchos de estos dispositivos pueden 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. Investigaciones recientes indican que la cantidad de dispositivos aumentará de 6.4 mil millones a fines del año pasado a 25 mil millones para 2020. Este increíble crecimiento enfatiza aún más la necesidad de abordar los problemas de seguridad y privacidad. 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. Requiere que los fabricantes se aseguren que estos dispositivos estén equipados con características de seguridad razonables para proteger tanto el dispositivo como la información recopilada. También exige que los fabricantes diseñen estos dispositivos para indicar claramente cuándo están recopilando información y obtener el consentimiento del consumidor antes de hacerlo. Y asigna responsabilidad a aquellos que venden estos dispositivos para proporcionar un aviso adecuado de las funciones de recopilación de información de los dispositivos[32].

Dicha Ley, que 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)*, es corta y simple. Es de destacar que 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.

[32] United States. Senate Judiciary Committee (2017).

En primer lugar, en el Título 1798.91.04. (a) 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.

A continuación, bajo el apartado b), 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 establecido 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 por este título 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 esta ley 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.[33]

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.

[33] United States. California State Legislature (2018) *Title 1.81.26. Security of Connected Devices.* California Legislative Information. [Consultado el 10/12/2018] Disponible en: *https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB327*

### 3.1. Argumentos a favor y en contra de la reciente ley. Luces y sombras

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. Es como hacer dieta, donde la gente insiste en que debe comer más verduras, lo que hace poco para solucionar el problema. La clave para una dieta es no comer más sino comer menos. Lo mismo ocurre con la ciberseguridad, donde el objetivo no es agregar "características de seguridad", sino eliminar "características inseguras". Para los dispositivos conectados a Internet eso 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. Algunos dispositivos de Internet de las Cosas no pueden ser parchados, y eso es un problema. Pero incluso si los dispositivos son parcheables en teoría, no hay 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"[34] como el peor y más costoso ciberataque de todos los tiempos y fue lanzado subvirtiendo un parche automatizado. Por ejemplo, el gusano Mirai[35] 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[36] 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

[34] 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.

[35] 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

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

sistemas de autenticación en la interfaz web y en otros servicios como Telnet. La mayoría de los dispositivos vulnerables a Mirai hicieron lo correcto en las interfaces web, vale decir, que el usuario creó nuevas contraseñas antes de operar. Simplemente hicieron lo incorrecto en otro lugar. Esta ley mira el pasado y no al futuro. 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, vale decir, evita que las laptops y/o computadoras de escritorio infectadas (que están mucho más amenazadas) se propaguen a los demás dispositivos. Pero los legisladores no piensan en términos de lo que conducirá a la mayor protección, piensan en términos de quién puede ser culpado. Culpar a los dispositivos por la debilidad moral de no hacer cosas "razonables" es satisfactorio, sin importar si es efectivo. La ley establece el vago requisito que los dispositivos tengan características de seguridad "razonables" y "apropiadas". Es imposible para una empresa saber lo que significan estas palabras, es imposible saber si cumplen con la ley. Al igual que otras leyes que utilizan estos términos, se interpretará en los tribunales. Pero la seguridad no es como otras cosas. En lugar de algo estático que puede resolverse una vez, siempre está cambiando ya que el adversario no es algo estático como el desgaste de las piezas de un automóvil, sino dinámico. 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. La realidad es que el problema se presentará constantemente ante los tribunales, ya que los atacantes cambian de táctica, lo que genera enormes costos. 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 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 por ciento de ellos. En resumen, esta ley se basa en una comprensión obviamente superficial del problema. De ninguna manera aborda las amenazas reales, pero al mismo tiempo, introduce enormes costos para los consumidores y la innovación. Debido a la tecnología cambiante con IPv4 vs. IPv6 y WiFi vs. 5G, tales leyes son innecesarias: la Internet de las Cosas del futuro será inherentemente mucho más segura que la seguridad del estilo Mirai del pasado.[37]

En igual sentido se expidió la Cámara de Comercio de California. Agrega, además, que la Sección 1798.81.5 (b) del Código Civil ya requiere que los fabricantes implementen protecciones de privacidad razonables y, por lo tanto, el requisito que los fabricantes

[37] Graham (2018)

equipen dispositivos con "características de seguridad razonables apropiadas para la naturaleza del dispositivo" es 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.

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[38].

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 de dientes azules 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 de dientes azules 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 50 pies.

Pero este 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. Se informó que los monitores para bebés fabricados con Foscam han sido particularmente susceptibles a la piratería, ya que los piratas informáticos hablaban a través de ellos con los niños y operaron la lente de la cámara para rastrear sus movimientos.

[38] Hawkins (2018)

A principios del año 2017, se informó que los juguetes de *CloudPets* fueron hackeados de manera similar. Los juguetes se conectan a las aplicaciones móviles y permiten a los miembros de la familia enviar mensajes a sus hijos. Sin embargo, la información se almacenó de forma insegura en la nube y un hacker reveló más de 820.000 cuentas, incluida información personal, fotos y grabaciones de voces de niños. 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 los de Twitter, Spotify, New York Times y Airbnb en octubre del 2016.

California reconoce que el derecho a la privacidad es un derecho fundamental, y lo ha consagrado junto con otros derechos fundamentales en el artículo I, sección 1 de su Constitución. Dada la ubicuidad de Internet de la Cosas y la profundidad de la información personal y sensible que se puede recopilar y almacenar, este derecho fundamental está cada vez más vulnerado. 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.

La privacidad y la seguridad a menudo llegan tarde en la carrera con el mercado y con la conectividad que se mueve desde las computadoras y teléfonos celulares a las tostadoras y ositos de peluche, poniendo en riesgo tanto a los adultos como a los niños. 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. Esta ley da un paso para abordar estos problemas. 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, esta ley hace extensivos estos requisitos a los fabricantes de dispositivos conectados a Internet.[39]

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 por ciento 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 por ciento en 2013.[40] 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.[41]

## 4. 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.

Las webcam, los micrófonos de las computadoras personales, los celulares, las luces, el aire acondicionado, el lavarropas, el automóvil, la cerradura de la puerta de casa y hasta la barredora se pueden activar a control remoto para ver, escuchar y transmitir datos personales en tiempo real.

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.

[39] United States. Senate Rules Committee. Senate Floor Analysis (2018)
[40] United States. California Department of Justice (2014)
[41] United States. California Department of Justice (2016)

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 su libro "Los Hombres que Susurran a las Máquinas" plantea, entre otros temas, 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.[42]

Esta nueva tecnología vino para quedarse y cada vez irrumpe con mayor asiduidad en nuestra vida cotidiana, que no nos tome desprevenidos.

## 5. Bibliografía


- Agencia Española de Protección de Datos (AEPD) y a la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum) (2017) Código de Buenas Prácticas en Protección de Datos para Proyectos Big Data. [Consultado el: 25/7/2018] Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf
- Argentina. Ministerio de Comunicaciones. Secretaría de Tecnologías de la Información y las Comunicaciones Resolución 11E-2017 Creación del Observatorio Nacional de Big Data. Boletín oficial de la República Argentina, 8 de junio de 2017. Id SAIJ: NV17171
- "Big Data" (s.f.) *SearchDataCenter*. [Consultado el: 30/7/2018] Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Big-data


[42] Salas (2015)

- Casalet, M (2018) “La digitalización industrial: un camino hacia la gobernanza colaborativa. Estudios de casos”. *Documentos de Proyectos* (LC/TS.2018/95). Santiago, Chile: Comisión Económica para América Latina y el Caribe (CEPAL), pp. 7-9
- 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, Chile: Naciones Unidas.
- Comisión Económica para América Latina y el Caribe. CEPAL (2018) *Datos, algoritmos y políticas. La redefinición del mundo digital*. Santiago, Chile: Naciones Unidas.
- “Domótica: cómo automatizar tu hogar para disfrutarlo más mientras ahorras tiempo y dinero” (3 de noviembre de 2016) *20 minutos*. [Consultado el: 15/3/2017] Disponible 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/
- 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.” *Harvard Deusto Business Research* Volumen V. Número 2, pp. 149-161.ISSN: 2254-6235.
- Gartner (11 de noviembre de 2013) “Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets”. *Gartner* [Consultado el: 2/5/2017] Disponible en: http://www.gartner.com/newsroom/id/2621015
- Gartner (7 de febrero de 2017) “Gartner says 8.4 billion connected ‘things’ will be in use in 2017, up 31 percent from 2016”. [Consultado el: 2/5/2017] Disponible en: https://www.gartner.com/newsroom/id/3598917
- Graham, R. (10 de septiembre de 2018) “California's bad IoT law”. *Errata Security*. [Consultado el: 12/12/2018] Disponible en: https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XBbQ-lwzbIV
- Hawkins, D. (17 de septiembre de 2018) “The Cybersecurity 202: California's Internet of Things cybersecurity bill could lay groundwork for federal action” *The Washington Post*. [Consultado el: 14/12/2018] Disponible en: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.22a787721195
- Hu, K. (9 de agosto de 2018) “La necesidad de reformular la Internet de las cosas”. *La Nación*, sección opinión. [Consultado el: 15/11/2018] Disponible en: https://www.nacion.com/opinion/columnistas/la-necesidad-de-reformular-la-internet-de-las/UH5K2L7BIJA53NVC7W7CJV3LXA/story/
- Jaimovich, D**.** (19 de septiembre de 2018) “Quién es el científico que lidera la revolución creativa de las máquinas” *Infobae*. Sección Tecno. [Consultado el: 12/11/2018] Disponible en: https://www.infobae.com/america/tecno/2018/09/19/quien-es-el-cientifico-que-lidera-la-revolucion-creativa-de-las-maquinas/

∗McKinsey & Company (2018) *The Internet of Things: How to capture the value of IoT*. [Consultado el: 2/12/2018] Disponible en: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20How%20to%20capture%20the%20value%20of%20IoT/How-to-capture-the-value-of-IoT.ashx
∗Microsoft (2018) *The Future Computed: Artificial Intelligence y and its Role in Society*. Redmond, Washington: Microsoft Corporation.
∗Oracle (s.f.) "¿Qué es Big Data? "[Consultado el: 16/8/ 2018] Disponible en https://www.oracle.com/mx/big-data/guide/what-is-big-data.html
∗Perasso, V. (12 de octubre de 2016) "Qué es la cuarta revolución industrial (y por qué debería preocuparnos)" BBC Mundo. [Consultado el: 9/10/2018] Disponible en: http://www.bbc.com/mundo/noticias-37631834.
∗"Polémico: una pulsera envía descargas eléctricas para fomentar el ahorro". (23 de mayo 23 de 2016). *Infobae*. [Consultado el: 15/3/2017] Disponible en: https://www.infobae.com/2016/05/23/1813599-polemico-una-pulsera-envia-descargas-electricas-fomentar-el-ahorro/
∗Poole, E. (2014) "El mundo nuevo de la tecnología ponible: ¿Qué consecuencias tiene para la propiedad intelectual (P.I.)?" *Revista de la Organización Mundial de la Propiedad Intelectual*. junio, número 3/2014.
∗Primer Foro sobre Inteligencia Artificial e Internet de las Cosas en Ciudades Inteligentes y Sostenibles en América Latina. "Declaración de Buenos Aires. Inteligencia Artificial e Internet de las Cosas en Ciudades Inteligentes y Sostenibles en América Latina". 30 de mayo de 2018. *ITU Foro.* [Consultado el: 5/8/ 2018] Disponible en: https://www.argentina.gob.ar/sites/default/files/buenosaires-declaration-spanish-final.pdf
∗Rayón, Á. (6 de diciembre del 2015) "Por qué hablamos del Business Analytics y no solo del Business Intelligence". *DeustoData*. [Consultado el: 9/7/ 2018] Disponible en: https://blogs.deusto.es/bigdata/por-que-hablamos-del-business-analytics-y-no-solo-de-business-intelligence/
∗Robledo, J. (19 de septiembre de 2018) "Inteligencia artificial, eficiencia energética y diseño: cómo son los electrodomésticos de alta gama que LG traerá a la Argentina en 2019" *Infobae*. Sección Tecno. [Consultado el: 12/11/2018] Disponible en: https://www.infobae.com/tecno/2018/09/19/inteligencia-artificial-eficiencia-energetica-y-diseno-como-son-los-electrodomesticos-de-alta-gama-que-lg-traera-a-la-argentina-en-2019/
∗Salas, A. (2015) *Los Hombres que Susurran a las Máquinas*. España: Espasa
∗Tejero López, A. (2014) "Seguridad en el Internet de las Cosas. Retos y oportunidades detectadas". Centro de Apoyo a la Innovación Tecnológica (CAIT), Universidad Politécnica de Madrid
∗"The world's most valuable resource is no longer oil, but data" (6 de mayo de 2017) *The Economist.* Londres, [Consultado el: 3/8/2018]. Disponible en

https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worldsmost-valuable-resource.

- Unión Europea. Grupo de Trabajo sobre Protección de Datos del Artículo 29. "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos". Adoptado el 16 de septiembre de 2014. *1471/14/ESWP 223*.
- United States. California Department of Justice (2014) *California Data Breach Report.* [Consultado el: 11/12/2018] Disponible en: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy /2014data_breach_rpt.pdf
- United States. California Department of Justice (2016) *California Data Breach Report.* [Consultado el: 9/12/2018] Disponible en: https://oag.ca.gov/breachreport2016
- United States. California Legislative Information (2018) *SB-327 Information privacy: connected devices. (2017-2018)* [Consultado el: 3/12/2018] Disponible en: https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180SB327
- United States. California State Legislature (2018) Title 1.81.26. Security of Connected Devices. California Legislative Information. [Consultado el 10/12/2018] Disponible en: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB327
- United States. Senate Judiciary Committee (2017). *Information privacy: connected devices*. California Legislative Information. [Consultado el: 5/12/2018] Disponible en: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB327
- United States. Senate Rules Committee. Senate Floor Analysis (2018). *SB-327 Information privacy: connected devices.* [Consultado el: 12/12/2018] Disponible en: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB327
- Vecchione, M. (2018)" La tecnología para el bien – Un enfoque novedoso" *ITUNews Magazine. Inteligencia Artificial para el Bien en el Mundo,* pp.11-15
- VV.AA. (2015) *Internet de las Cosas* (ed. Zennaro, M. y Pietrosemoli, E.) [Consultado el: 25/10/2018] Disponible en: http://www.nodo6.com/docu/InternetdelasCosas.pdf
- VV.AA. (2016) *Oportunidades y requerimientos para aprovechar el uso de Big Data para las estadísticas oficiales y los Objetivos de Desarrollo Sostenible en América Latina*. Data-Pop Alliance.