# Internet de las Cosas (IoT)

## Regulación federal de Estados Unidos y del Estado de California

**Autores**

Raimundo Roberts M.
rroberts@bcn.cl

Christine Weidenslaufer
cweidenslaufer@bcn.cl

Nº SUP: 130569

**Resumen**

Con un crecimiento de miles de millones de dispositivos conectados cada año, la Internet de las Cosas (IoT, por sus siglas en inglés) es hoy más que el uso de objetos cotidianos conectados entre sí y a Internet.

Actualmente, la IoT, o Internet Industrial de las Cosas es uno de los dos principales segmentos del mercado mundial de estas tecnologías, enfocadas en el monitoreo y conexión de grandes equipos industriales, mientras que el segundo segmento es el dedicado a las “Smart cities”, conectando sistemas que influyen en la vida de grandes grupos de población.

Sin embargo, a pesar de su desarrollo global, la Unión Internacional de Telecomunicaciones (ITU) aun no ha logrado un consenso amplio para estándares globales que aseguren que estas tecnologías no sólo sean seguras para las personas sino también para la ciberseguridad.

Estados Unidos (a nivel federal) y el estado de California han publicado recientemente legislaciones para su regulación, las que se describen en este informe.

Por último, la Unión Europea, desde 2005 está desarrollando iniciativas para el fomento de la nueva Sociedad de la Información, con programas de investigación y normativa sectorial sobre protección de datos, cibercriminalidad y “comunidades conectadas”, entre otras, pero no se regula de forma explícita la IoT.

## Introducción

El siguiente informe describe y resume información sobre Internet de las Cosas y su regulación en el estado de California y en la legislación federal de Estados Unidos.

Las traducciones son propias.

## Antecedentes

La Internet de las Cosas (IoT, por sus siglas en inglés) es, en simple, el nombre de un conjunto de tecnologías que permiten incorporar información y comunicar esta información en objetos comunes (desde electrodomésticos hasta dispositivos médicos, deportivos, vestimenta, etc.) conectándolos a Internet y generando valor a los usuarios finales[1].

Por otro lado, la ITU, también lo entiende como "una infraestructura global para la sociedad de la información, que permite servicios avanzados mediante la interconexión (física y virtual) de elementos basados en tecnologías de la información y la comunicación interoperables existentes y en evolución"[2]. Desde 2005[3] la ITU ha estado trabajando en la elaboración de estándares globales que permitan el correcto funcionamiento de los dispositivos, sistemas y mecanismos que se requieren para la IoT, esto es, identificadores individuales de objetos, sistemas de identificación por radiofrecuencia, protocolos de control dentro de redes simples y de conexión a Internet, etc. En la IoT, "cada "cosa" debe ser identificada por un identificador único global o local para poder acceder a ella", y hay algunas situaciones especiales en las que estas "cosas" no necesitan identificadores globales y únicos, pero tienen que ser únicos en un entorno local[4].

Lo anterior supone una serie de desafíos, tanto técnicos como regulatorios y de seguridad, a medida que aumenta la demanda por objetos conectados. Según Kumar, a 2010 había 12.5 mil millones de dispositivos conectados en áreas tan diversas como transporte, retail, educación, salud, construcción y agricultura, entre otros[5], y se calcula que a 2018 ya eran 22 mil millones[6].

A ese año los dos segmentos más grandes del mercado mundial de IoT eran "Internet industrial de las cosas" (IIoT[7]), la que "está diseñada para 'cosas' más grandes que los teléfonos inteligentes y los dispositivos inalámbricos. Su objetivo es conectar activos industriales, como motores, redes eléctricas y sensores a la nube a través de una red"[8] y "Smart cities", donde las tecnologías de IoT dan la capacidad de "monitorear, administrar y controlar dispositivos de forma remota, y de crear nuevos conocimientos e información procesable a partir de flujos masivos de datos en tiempo real. Las principales características de una ciudad inteligente incluyen un alto grado de integración de la tecnología de la información y una aplicación integral de los recursos de información[9]".

[1] Weber, R. (2016).
[2] ITU (2012).
[3] ITU (2005).
[4] ITU (2017a).
[5] Kumar (N/D).
[6] Statista (2019).
[7] Boyes (2018).
[8] Boyes (2018).
[9] Tai-hoon *et. al*. (2017).

Se trata del uso de la IoT no sólo para conectar un refrigerador al teléfono celular, sino de su aplicación a niveles que alcanzan ciudades enteras o servicios que abastecen a grandes grupos de población. Incluso, una encuesta realizada a agencias federales de Estados Unidos mostró que de 56 agencias (que respondieron a la consulta, de un total de 90), 42 informaron que utilizan IoT para, entre otros, controlar o monitorear dispositivos o sistemas remotos (como boyas marinas), controlar el acceso a instalaciones o rastrear activos físicos, entre otros[10].

En la Unión Europea[11], desde 2005 está desarrollando iniciativas para el fomento de la nueva Sociedad de la Información, con programas de investigación y normativa sectorial sobre protección de datos, cibercriminalidad y "comunidades conectadas", entre otras, pero no se regula de forma explícita la IoT.

Actualmente, la Comisión Europea está desarrollando la "Política Europea de Internet de las cosas[12]", la cual se enfoca en la promoción científica y económica de la IoT, así como en el estudio de efectos jurídicos y sociales de la aplicación de estas tecnologías en el espacio europeo. Sin embargo, hasta la actualidad no se ha logrado consensuar estándares globales que agrupen las distintas aristas asociadas a la IoT, un trabajo en la ITU ha estado trabajando durante las últimas décadas y hasta la actualidad[13].

Sólo en lo relativo a la ciberseguridad, la revista Forbes (en febrero de 2021) citaba un informe que indica que las amenazas informáticas superan la centena mensual en un hogar promedio de Estados Unidos, incluyendo equipos como tabletas, celulares o computadores, para destacar que los dispositivos de IoT, con menos memoria y capacidad de almacenamiento, tienen menos recursos contra los ataques informáticos[14].

Una argumentación similar es la que advierte la Europol[15]. La entidad señala que, entre las superficies de ataque a las que se enfrentan las aplicaciones web están "la memoria física y la interfaz de un dispositivo (por ejemplo, el puerto USB), el firmware, el almacenamiento local de datos, el mecanismo de actualización, los servicios de red, la interfaz de la nube, la aplicación móvil y las API (interfaces de programas de aplicación) de terceros". Esto significa que cualquier dispositivo orientado a Internet "puede convertirse en el objetivo de un ataque utilizando una variedad de puntos de entrada diferentes", lo que en el caso de los dispositivos de IoT se amplifica, dado que estos entornos "son difíciles de gestionar, controlar y proteger, teniendo en cuenta además que muchos dispositivos de la IO no tienen características de seguridad integradas".

Así, la búsqueda de capacidades de protección frente a brechas de seguridad que aseguren los beneficios que se obtienen de estas tecnologías (que van desde la automatización del hogar hasta la recogida automática de datos marítimos o de vehículos de carga, por ejemplo) es hoy una de las principales tareas regulatorias en el mundo, en materia de tecnologías.

[10] GAO (2020).
[11] BBVA (2018).
[12] Comisión Europea (2020).
[13] ITU (2017b).
[14] Brooks, Ch. (2021).
[15] Europol (2016).

## I. Estados Unidos de Norteamérica EE.UU. (normativa federal)

En diciembre de 2020 se promulgó la Ley de mejora de la seguridad cibernética de IoT (*IoT Cybersecurity Improvement Act*)[16] de los EE. UU. (en adelante, la Ley), la cual describe los requisitos de seguridad que deben cumplir en el futuro los dispositivos de propiedad o controlados por el gobierno federal que estén conectados a sus sistemas informáticos[17].

Esta normativa responde a la vulnerabilidad de los dispositivos de IoT frente a los ataques digitales y la necesidad de protección de datos confidenciales[18]. Su alcance se extiende más allá de las agencias gubernamentales, e incluye a los fabricantes que crean dispositivos de IoT federales y a cualquier contratista del gobierno que utilice dispositivos de IoT

La Ley define la Internet de las Cosas (IoT) como la "extensión de la conectividad a Internet en dispositivos físicos y objetos cotidianos"[19].[20].

Si bien la definición de la Ley excluye expresamente los dispositivos de TI convencionales (por ejemplo, computadoras, laptops, tabletas y teléfonos inteligentes), se extiende a una variedad de sensores, actuadores y procesadores utilizados por el gobierno federal. Así, señala el estudio jurídico Gibson Dunn, las agencias federales habrían informado que utilizan dispositivos de IoT para controlar o monitorear equipos, rastrear activos físicos, brindar vigilancia, recopilar datos ambientales, monitorear la salud y la biometría y para muchos otros propósitos[21].

Para lograr sus objetivos, la Ley entrega diversos roles a una serie de agencias federales. Por una parte, requiere al Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST) la creación de directrices y estándares para la gestión de los dispositivos de IoT federales por parte de las agencias federales para el día 4 de marzo de 2021[22]. Estas directrices deben abordar los riesgos de ciberseguridad únicos que pueden tener los dispositivos de IoT y establecer estándares mínimos de seguridad para estos. El NIST también debe revisar y actualizar sus estándares cada cinco años para mantenerse al día respecto de nuevas preocupaciones en relación a datos.

Al formular estas directrices, el NIST debe considerar sus esfuerzos actuales con respecto a la seguridad de los dispositivos de IoT, así como las normas, pautas y mejores prácticas relevantes desarrolladas por el sector privado, agencias y asociaciones público-privadas[23].

El NIST también es instruido por la Ley para trabajar con el Departamento de Seguridad Nacional (*Department of Homeland Security*, DHS), expertos de la industria del sector privado e investigadores en materia de seguridad para determinar la mejor manera de informar las vulnerabilidades de seguridad presentes en los dispositivos IoT y cómo solucionar estos problemas. Por otra parte, requiere a la Oficina

[16] Public Law No: 116-207 (12/04/2020), llamada "Internet of Things Cybersecurity Improvement Act of 2020" o "The IoT Cybersecurity Improvement Act of 2020". Codificada en el US Code
[17] Gibson Dunn (2021).
[18] JD Supra (2021).
[19] Gibson Dunn (2021).
[20] JD Supra (2021).
[21] Gibson Dunn (2021).
[22] Sección 4(a)(1).
[23] Sección 4(a)(2)–(3).

de Administración y Presupuesto (*Office of Management and Budget,* OMB) y al DHS crear nuevas políticas y procedimientos que se alineen con los estándares y pautas del NIST. Esto debe completarse a más tardar 180 días después de que el NIST publique sus directrices. El DHS y la OMB también deberán trabajar con otras agencias federales y contratistas sobre cómo manejar las debilidades de seguridad y cómo seguir suficientemente las reglas del NIST[24].

Poco después de la aprobación de la Ley en diciembre de 2020, el NIST publicó borradores que discutían los requisitos de seguridad adecuados para los dispositivos de IoT. Los borradores fueron sujetos a comentarios públicos hasta el 26 de febrero de 2021[25]. Después de eso, señala la página web de información jurídica JD Supra, las partes interesadas deben mantenerse informadas de cualquier cambio en los borradores y revisar los estándares y directrices finales del NIST para garantizar su cumplimiento[26].

Asimismo, el NIST también debe establecer directrices para recibir, informar y difundir información sobre vulnerabilidades de seguridad y su resolución antes del 2 de junio de 2021[27]. Por último, a partir del 5 de diciembre de 2022, todas las agencias gubernamentales no podrán renovar los contratos de adquisición con empresas cuyos dispositivos de IoT no cumplan con los estándares y directrices del NIST[28].

## II. California, EE.UU. (normativa estadual)

El 1 de enero de 2020 entró en vigencia en el estado de California una ley[29] de privacidad específica[30], que regula los dispositivos conectados a Internet de las Cosas (*Internet of Things*, IoT), promulgada en 2018.

La ley de IoT de California requiere que los fabricantes de dispositivos conectados equipen el dispositivo con una o más características de seguridad razonable que[31]:

- Sea(n) apropiada(s) a la naturaleza y función del dispositivo;
- Sea(n) apropiada(s) a la información que el dispositivo puede recopilar, contener o transmitir; y,
- Sea(n) diseñada(s) para proteger el dispositivo, y cualquier información contenida en el mismo, del acceso, destrucción, uso, modificación o divulgación no autorizados.

Para estos efectos, se define “fabricante” a la persona que fabrica, o contrata a otra persona para fabricar en su nombre, dispositivos conectados que se venden u ofrecen para la venta en California. Por su parte, se define “dispositivo conectado” como cualquier dispositivo u otro objeto físico que sea capaz de

[24] Secciones 4(b)(1)–(2) y 4(b)(1).
[25] Gibson Dunn (2021).
[26] JD Supra (2021).
[27] Sección 5(a).
[28] Sección 7(a)(1) y 7(d).
[29] La norma (*SB-327 Information privacy: connected devices*) fue incorporada a la Parte 4 de la División 3 del Código Civil de California (*Title 1.81.26. Security of Connected Devices*).
[30] También está vigente una norma general que regula la privacidad de los consumidores (*California Consumer Privacy Act, CCPA*).
[31] Sección 1798.91.04.

conectarse a Internet, directa o indirectamente, y al que se le asigne una dirección de Protocolo de Internet (dirección IP) o una dirección Bluetooth[32].

Por último, para definir qué se considera una "característica de seguridad razonable", la ley establece que debe cumplirse alguno de los siguientes requisitos[33]:

(1) La contraseña preprogramada es única para cada dispositivo fabricado; o
(2) El dispositivo contiene una característica de seguridad que requiere un uso para generar un nuevo medio de autenticación, antes de que se otorgue acceso al dispositivo por primera vez.

Actualmente, solo los estados de California y Oregon[34] (en términos similares) requieren a los fabricantes incorporar características de seguridad razonables para los dispositivos de IoT. En la práctica, como señala el sitio web de información jurídica *National Law Review*, estas medidas de seguridad significan que los dispositivos conectados serán menos vulnerables a ataques, pues no funcionarán con la contraseña predeterminada "genérica" establecida por un fabricante[35].

## Referencias

BBVA (2018). Hora de regular el Internet de las Cosas en la UE. Noviembre, 2018,. Disponible en: https://www.bbva.com/es/hora-regular-internet-las-cosas-la-ue/ (mayo, 2021).

Boyes, H., *et. al* (2018) "The industrial internet of things (IIoT): An analysis framework", Volume 101, Octubre 2018, P.1-12, Computers in Industry. Disponible en: https://www.sciencedirect.com/science/article/pii/S0166361517307285 (Mayo, 2021).

Brooks, Ch. (2021). Cybersecurity Threats: The Daunting Challenge of Securing the Internet of Things", Forbes, 7 de febrero, 2021. Disponible en: https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/?sh=16fcf62c5d50 (mayo, 2021).

Comisión Europea (2020). Política europea de Internet de las cosas. Mayo, 2020. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/iot-policy (mayo, 2021).

Europol (2016). Cybersecurity and the Internet of Things – a Law Enforcement Perspective. European Cybercrime Centre. Abril, 2016. Disponible en: https://cybersummit.info/sites/cybersummit.info/files/Cybersecurity_and_the_Internet_of_Things_-_a_Law_Enforcement_Perspective.pdf (mayo, 2021).

Gibson Dunn (2021). New Federal Law for IoT Cybersecurity Requires the Development of Standards and Guidelines Throughout 2021. 17 de febrero, 2021. Disponible en:

[32] Sección 1798.91.05.
[33] Sección 1798.91.04.
[34] En Oregon, el proyecto de ley aprobado por la asamblea legislativa estadual es HB 2395, de 2019. Otros estados que estarían discutiendo en sus legislaturas esta materia son Nueva York, Illinois y Maryland (Gibson Dunn, cita [32]).
[35] National Law Review (2020).

https://www.gibsondunn.com/new-federal-law-for-iot-cybersecurity-requires-the-development-of-standards-and-guidelines-throughout-2021/ (mayo, 2021).

International Telecommunication Union (2017a). Series X: Data Networks, Open System Communications and Security. ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things. Disponible en: http://handle.itu.int/11.1002/1000/13411 (mayo, 2021).

-- (2017b). SG20: Internet of things (IoT) and smart cities and communities (SC&C). Disponible en: https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx (mayo, 2021).

-- (2012). Visión general de la Internet de las cosas. ITU-T Y.4000/Y.2060 (06/2012). Disponible en: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=es (mayo, 2021).

-- (2005). The Internet of Things. Internet Reports. Disponible en: https://www.itu.int/osg/spu/publications/internetofthings/ (mayo, 2021).

JD Supra (2021). How Far Does the New Federal IoT Law Reach? 10 de Marzo 10, 2021. Disponible en: https://www.jdsupra.com/legalnews/how-far-does-the-new-federal-iot-law-5837222/ (mayo, 2021).

Kumar, R. “Key Aspects of Cybersecurity in the context of Internet of Things (IOT)”, ITU. Disponible en: http://bcn.cl/2pme0 (mayo, 2021).

National Law Review (2009). IoT Manufacturers – What You Need to Know About California’s IoT Law. Vol. X, N. 28. 28 de enero, 2020. Disponible en: https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law (mayo, 2021).

Statista (2019). Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030. Mayo 2019. Disponible en: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/ (mayo, 2021).

Tai-hoon, K., Ramos, C., Mohammed, S. (2017). Smart City and IoT. Future Generation Computer Systems, Vol. 76, 2017, pp. 159-162. Disponible en: https://doi.org/10.1016/j.future.2017.03.034 (mayo, 2021).

U.S. Government Accountability Office, GAO (2020). Internet of Things: Information on Use by Federal Agencies. GAO-20-577. Agosto, 2020. Liberado al público en Septiembre, 2020. Disponible en: https://www.gao.gov/products/gao-20-577 (mayo, 2021).

Weber, R. (2016). Governance of the Internet of Things—From Infancy to First Attempts of Implementation? Laws 2016, 5, 28; Disponible en: https://doi.org/10.3390/laws5030028 (mayo, 2021).

**Normativa**

Nacional:

Chile:

- Ley N° 18.168, Ley General de Telecomunicaciones. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=29591 (mayo, 2021).

EE.UU. (federal).

- Internet of Things Cybersecurity Improvement Act of 2020. Disponible en: https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf (mayo, 2021).

California, EE.UU.:
- Código Civil de California (Part 4, Division 3, Title 1.81.26. Security of Connected Devices). Disponible en: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (mayo, 2021).
- Proyecto de ley "SB-327 Information privacy: connected devices" [California]. Disponible en: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (mayo, 2021).
- Proyecto de ley "HB 2395 Relating to security measures required for devices that connect to the Internet" [Oregon]. Disponible en: https://olis.leg.state.or.us/liz/2019R1/Measures/Overview/HB2395 (mayo, 2021).

**Nota aclaratoria**

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.