UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO ADMINISTRATIVO

"LA REGULACIÓN EN MÉXICO DEL INTERNET DE LAS COSAS ENFOCADAS AL HOGAR".

TESIS

QUE PARA OBTENER EL TÍTULO DE:

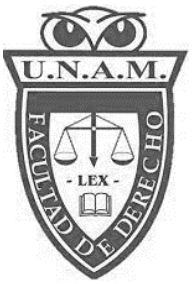
LICENCIADO EN DERECHO

PRESENTA

ALAN JESUARI MENDOZA PÉREZ

DIRECTOR DE TESIS:

DR. MARCO ANTONIO ZEIND CHÁVEZ



CIUDAD UNIVERSITARIA, CIUDAD DE MÉXICO, 2022

VNIVERSIDAD NACIONAL AVTONOMA DE MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO ADMINISTRATIVO
OFICIO No: FD/SDA/219/2022

M. EN C. IVONNE RAMÍREZ WENCE
DIRECTORA GENERAL DE ADMINISTRACIÓN ESCOLAR.
P R E S E N T E

Distinguida Señora Directora:

Me permito informar que la tesis para optar por el título de Licenciado en Derecho, elaborada en este Seminario por el pasante **ALAN JESUARI MENDOZA PÉREZ** con número de cuenta **313087101**, bajo la dirección del que suscribe, denominada **"LA REGULACIÓN EN MÉXICO DEL INTERNET DE LAS COSAS ENFOCADAS AL HOGAR",** satisface los requisitos establecidos por el Reglamento General de Exámenes Profesionales y de Grado de la UNAM, por lo que otorgo la aprobación correspondiente y autorizo su presentación al jurado recepcional en los términos del Reglamento de Exámenes Profesionales y de Grado de esta Universidad.

El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional.

Sin otro particular, le envío un cordial y respetuoso saludo.

"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., a 28 de octubre de 2022

DR. MARCO ANTONIO ZEIND CHÁVEZ
DIRECTOR DEL SEMINARIO DE DERECHO ADMINISTRATIVO

C.c.p. Secretaría de Exámenes Profesionales. - Presente

Agradezco a:
mis padres,
mis hermanos,
mis abuelos,
mis profesores y,
en especial a mí por haber terminado
la licenciatura.

GLOSARIO Y TÉRMINOS ABREVIADOS

App: aplicación móvil.

Arduino: es una plataforma de desarrollo basada en una placa electrónica de hardware libre que incorpora un microcontrolador reprogramable y una serie de pines hembra. Estos permiten establecer conexiones entre el microcontrolador y los diferentes sensores y actuadores de una manera muy sencilla.[1]

Big Data: conjunto de datos grande y complejo, así como a las técnicas de tratamiento específicas de ese gran volumen de información.[2]

***Bit*:** Binary Digit.

Cloud Computing: es la entrega de servicios informáticos, incluidos servidores, almacenamiento, bases de datos, redes, software, análisis e inteligencia, a través de Internet para ofrecer una innovación más rápida, recursos flexibles y economías de escala.[3]

***e-commerce*:** comercio electrónico.

HTML: HyperText Markup Language.

***IoT*:** Internet of Things o internet de las cosas

P&G: Procter & Gamble.

RAE: Real Academia Española

***Router*:** es un aparato que recibe y envía datos en redes informáticas.

***Smart Tv*:** Televisor inteligente.

***Software*:** conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.[4]

---

[1] Arduino, *¿Qué es Arduino?* Recuperado el 19 de julio de 2021, de: https://arduino.cl/que-es-arduino/

[2] IIC, *¿Qué es el Big Data?* Recuperado el 12 de enero de 2022, de: https://www.iic.uam.es/big-data/

[3] Microsoft, *Cloud Computing*. Recuperado el 22 de octubre de 2021, de: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

[4] Real Academia Española, *Significado de Software.* Recuperado el 19 de febrero de 2021, de: https://dle.rae.es/software

Streaming**:** es el medio por el cual pueden "enviar y recibir datos (como audio y video) en un flujo continuo a través de una red. Esto permite que la reproducción comience mientras se envía el resto de los datos".[5]

Smartphone**:** Teléfono inteligente.

Tablet: Tableta electrónica.

TCP/IP: son un conjunto de normas y procedimientos útiles para la transmisión de datos conocidos por el emisor y el receptor que conforman la arquitectura de cinco niveles. Es establecida por la aplicación, el transporte, el internet físico y la red, permitiendo la conexión de computadoras de marcas y tecnologías diferentes.[6]

URSSS: Unión de Repúblicas Socialistas Soviéticas.

Vacatio legis: periodo que transcurre desde que se publica una norma hasta que entra en vigor.

[5] AVG, *¿Qué es el streaming y cómo funciona?,* 2018, Recuperado el 19 de septiembre de 2021, de: https://www.avg.com/es/signal/what-is-streaming.

[6] Estrada Corona, Adrián, *Protocolos TCP/IP de Internet,* Revista Digital Universitaria, V, núm.8, 2004, pp. 1-7. Recuperado el 13 de noviembre de 2021, de: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf.

INTRODUCCIÓN

La tecnología se ha convertido día con día en parte fundamental de nuestra vida. Está presente en sistemas tan complicados como la geopolítica y la comunicación entre navíos, e incluso actúa de manera omnipresente en aspectos tan comunes como la comunicación por medio de celulares o tabletas electrónicas en la que es posible realizar actividades cercanas a una computadora portátil.

Sin embargo, a cada cierto tiempo, cada vez más corto, en algún lugar del planeta se van creando con más frecuencia dispositivos que interfieren en nuestra cotidianidad. Anteriormente, dichas creaciones no necesitaban de una conexión de internet, por lo que no nos ofrecían más que para lo que fueron creados ahora existen las bombillas inteligentes, los apagadores inteligentes, las televisiones inteligentes y refrigeradores que utilizan los productos en ellos para personalizar las preferencias de cualquier persona, así como notificar en caso de que se encuentre sin algún alimento común.

Debido a esta innovación en los artículos diseñados para el hogar, se necesita establecer una regulación jurídico-técnica que permita englobar todos los aspectos que involucran a la persona que usa estos dispositivos, además de aquellos que participan de forma directa.

Asimismo, por la facilidad con la que se producen hoy en día este tipo de objetos, los protocolos de seguridad con los que son fabricados no son los mejores. Estos varían dependiendo del proveedor o fabricantes, por lo que proporcionar los datos personales, incluso aquellos que se catalogan como sensibles, pone en riesgo nuestra seguridad y la de nuestros familiares. En muchos casos, la información se recopila aun cuando no la use el usuario original.

Teniendo en cuenta la relevancia que trae aparejada esta tecnología, así como las deficiencias en su regulación, el presente trabajo busca abordar desde el tema jurídico los aspectos notables que se deben tomar en cuenta al querer regular el internet de las cosas, en especial aquellas que están enfocadas al hogar.

Es por eso que, a lo largo del presente trabajo, se busca separar todo lo que involucra a este tipo de objetos, desde lo que se entiende por Internet hasta lo que ya se comprende como el internet de las cosas. De igual manera, se exponen los inicios de esta tecnología, además de los componentes mínimos que se deben saber sobre los dispositivos *IoT*.

Respecto a ello, se resalta que no se utilizaron sugerencias en cuanto al uso de protocolos informáticos. Esto se debe al constante cambio de la ciberseguridad de los diferentes objetos; es una cuestión que debe aplicarse conforme a la realidad que se vive y las situaciones tecnológicas con las que se cuentan al momento de querer regularlo. Es decir, el presente trabajo es en esencia un documento jurídico y resalta solamente los aspectos técnicos que se consideran necesarios para comprender el tema del documento.

CAPÍTULO 1. EL INTERNET

El Internet, hoy en día y en un mundo globalizado, es un elemento indispensable en la vida de las personas. El vínculo suele iniciar con la interacción directa de una persona con un dispositivo capaz de acceder a esa red o mediante la interacción entre artefactos que acceden al Internet (M2M) con la finalidad de satisfacer una necesidad.

Estas necesidades van desde consultar las noticias mediante una computadora o utilizar una *app* en un *smartphone* para acceder a algún servicio de *streaming*, hasta facilitar la producción de algún producto para el manejo de las máquinas de forma remota o para recabar datos que hagan más eficiente el proceso de producción.

Por lo tanto, el Internet es una red en la cual es indispensable estar conectados para poder interactuar con el mundo globalizado; no obstante, ¿qué tanto se conoce del Internet?

En los siguientes capítulos del presente tema, se analizará desde la creación del mismo hasta la importancia que tiene hasta la fecha.

1.1 Conceptos de Internet

Encontrar una definición o un concepto universal que trascienda en el tiempo no es posible. Desde su creación, el Internet ha cambiado y ha tenido diversos usos y alcances respecto a lo que conocemos de él, por lo que existen varias concepciones.

En particular, la RAE establece que el Internet es una “red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”. [7]

En cuanto a la doctrina, se pueden encontrar conceptualizaciones que devienen de un análisis técnico. Por ejemplo, para Rodríguez Ávila “el Internet no

[7] Real Academia Española, *Significado de Internet.* Recuperado el 19 de febrero de 2022, de: https://dle.rae.es/internet?m=form

es una simple red de ordenadores, sino una red de redes, es decir, un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma".[8]

Asimismo, dentro de la doctrina mexicana con enfoque jurídico, se encuentra el libro de la Dra. Clara Luz Álvarez *Telecomunicaciones y Radiodifusión en México*, donde se señala la siguiente definición:

"Internet es una colección de miles de redes enlazadas a través de una serie de protocolos técnicos comunes que hacen posible que los usuarios de cualquiera de esas redes se comuniquen con o usen los servicios de cualquiera de las demás redes."[9]

En ese sentido, el Internet se puede conceptualizar como un conjunto de redes conectadas entre sí que permite la comunicación entre los diferentes dispositivos con los que se puede acceder a este.

En el ámbito internacional, se encuentra un concepto de Internet que engloba todos los aspectos considerados para ese tiempo; fue el creado mediante acuerdo del Consejo Federal de Redes en el año de 1995. Sobre lo que es el Internet, se estableció lo siguiente:

> *"Internet" refers to the global information system that --*
> *1. is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;*
> *2. is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and*
> *3. provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein*". (Sistema de información global que,
>
> 1. está unido lógicamente por un espacio de direcciones único a nivel mundial basado en el Protocolo de Internet (IP) o sus posteriores extensiones/sucesiones.

[8] Rodríguez, Abel, *Iniciación a la red Internet. Concepto, funcionamiento, servicios y aplicaciones de Internet, Ideas propias*, España, Vigo, 2007, p. 2.
[9] Álvarez de Castilla, Clara Luz, *Telecomunicaciones y Radiodifusión en México*, Ciudad de México, Posgrado de Derecho de la UNAM, 2018, p. 57.

> 2. es capaz de soportar comunicaciones que utilizan el conjunto de Protocolos de Control de Transmisión y el Protocolo de Internet (TCP/IP) o sus extensiones/continuaciones y/u otros protocolos compatibles con IP.
> 3. proporciona, utiliza o hace accesibles, ya sea de forma pública o privada, servicios de alto nivel basados en la infraestructura de comunicaciones y afines descrita en el presente documento).[10]

Respecto a ello, al hacer una búsqueda de la definición de Internet en la legislación mexicana, se encuentra que la Ley Federal de Telecomunicaciones y Radiodifusión (LFTyR) vigente, en su artículo 3°, fracción XXXII, establece lo que se debe entender como Internet, señalando lo siguiente:

> (…) Internet: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única (…).[11]

Esta última concepción se usará en el presente trabajo como la única debido a que es la que se encuentra regulada en la legislación. De igual modo, es aquella que permitirá delimitar el objeto de forma más certera.

1.2 Revoluciones industriales importantes

Los cambios que han surgido a través del tiempo permiten que nuestra realidad vaya evolucionando de forma tan rápida. Esta es la forma en que se pueden resumir las diversas revoluciones que han afectado nuestra sociedad.

Las revoluciones industriales han permitido significativos cambios en la forma en que nos desarrollamos en el presente, de forma tal que nuestro futuro se encuentra supeditado a lo que hacemos y, ese es el impacto de las revoluciones

[10] Federal Networking Council, *Concepto de Internet,* (1995), Portal de internet de la Federal Networking Council. (con traducción propia). Recuperado el 02 de agosto de 2021, de: https://www.cs.columbia.edu/~hgs/internet/definition.html
[11] Ley Federal de Telecomunicaciones y Radiodifusión, *Artículo 3°, Fracción XXXII*, México, 2014. Recuperado el 17 de agosto de 2021, de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

industriales, cambios que aceleran las innovaciones en diferentes ámbitos de nuestra vida.

1.2.1 Situación Preindustrial

Uno de los aspectos que provocaba un lento desarrollo en la situación preindustrial, era la imposición de un sistema basado en la existencia de los señores feudales, quienes introducían la obligación de dar un tributo. Debido a ello, la producción se quedaba únicamente en el interior del feudo y la mayoría de los habitantes del territorio conservaban un estatus de siervo. A esto, se aunaba la existencia de una monarquía absoluta, encargada de cerrar aún más el intercambio de productos.

Por lo tanto, la economía regente en el mundo, previo a la entrada de esta Revolución Industrial, tomaba como base la agricultura y el sector artesanal. No obstante, lo producido en el sector agrícola era usado en su mayoría para el autoconsumo, causando así una producción muy baja de dichos frutos; esto limitaba el intercambio de productos y hacía un comercio ineficiente. En el caso del sector artesanal, los talleres eran pequeños; solamente trabajaban los maestros artesanos y uno o dos aprendices con una maquinaria precaria y escasa, provocando baja productividad.

De este modo, lo anterior hace que el intercambio de productos no sea tan eficiente para provocar un cambio en las ciudades; es decir, para hacerlas más desarrolladas a nivel industrial, educativo, comercial, científico, etcétera.

1.2.2 Primera Revolución Industrial

En Inglaterra, durante la mitad del siglo XVIII, se da el inicio de la transición de una economía agraria y artesanal a una mecanizada. La industria resalta como el gran estandarte del cambio; sin embargo, este movimiento no sólo afectó la economía de Europa, sino que se extendió a otros ámbitos como el cultural, social, científico y el político.

En este sentido, Gran Bretaña se convirtió en la nación más poderosa en ese momento debido a los movimientos industriales que dieron inicio allí, aunado a la astucia al momento de explotar los beneficios adquiridos al industrializar la nación y hacerla más desarrollada frente a las demás naciones.

1.2.2.1 Inicio de la Primera Revolución Industrial

Durante el siglo XVII se comenzó a dar lo que posteriormente daría inicio a la Revolución Industrial. Debido a la elevación de las relaciones económicas y la abundancia económica de algunas personas que obtenían un beneficio por la amplitud de las relaciones comerciales, las empresas tenían el potencial económico para planear e implementar mejores sistemas productivos, mejorando su tiempo y la calidad de producción.

No obstante, no fue sino hasta finales del siglo XVII y principios del siglo XVIII, cuando la población de Gran Bretaña comenzó a notar la importancia de mejorar la productividad con la intención de generar más ingresos y más beneficios para las personas que comprasen dichos productos.

- Características

En ese marco, se dio un crecimiento exponencial debido a que en las ciudades donde se encontraban personas con ingresos económicos altos se comenzó a atraer gente de otros poblados para tener más mano de obra y a su vez, más entes que generaran comercio a fin de cumplir con las necesidades básicas u objetos de adquisición por simple interés social. Además, las personas que buscaban trabajar en las fábricas se iban asentando en las ciudades que albergaban la cantidad más grande de fábricas, provocando que se fuera poblando la ciudad y aumentara la población que a la larga traería mano de obra para el futuro.

Esto condujo a grandes cambios a nivel social, pues se creó una clase social denominada con posterioridad como proletariado industrial, esto debido al trabajo que realizaban en las fábricas y a la relación de supra-subordinación que existía en dichos lugares.

Uno de los símbolos y uno de los mayores inventos creados en esa época, fue la máquina de vapor, la cual simbolizaría el inicio de una nueva época para el mundo.

1.2.3 Segunda Revolución Industrial

La Primera Revolución Industrial provocó que la industria no tuviera freno, por lo que los avances tecnológicos se dieron de forma progresiva. Eso causó que las condiciones de vida mejoraran y, por tanto, que las personas del campo quisieran mudarse hacia las ciudades, provocando a su vez un incremento en la mano de obra disponible.

En esta segunda etapa de la Revolución Industrial, ésta se expandió hasta otros continentes impulsando a países como Estados Unidos, Alemania y Japón. Sin embargo, la Gran Bretaña aún era conocida y respetada, no por los factores que lo hicieron en la Primera Revolución Industrial, sino porque se mantenía como una potencia marítima fuerte en cuanto al comercio y las fuerzas militares.

1.2.3.1 Inicio de la Segunda Revolución Industrial

Podemos establecer que esta etapa abarca desde el 1830 hasta 1914, fecha en la que comienza la Primera Guerra Mundial.

A este periodo de la historia también se le conoce como la era del Capitalismo Financiero, debido a que los Bancos tenían el protagonismo en esta época debido a la participación que tenían en las empresas industriales y su importancia para el crecimiento de ellas.

Sin embargo, aún con el crecimiento de industria del mundo, la Gran Bretaña perdió el puesto como nación líder en producción de hierro, innovación tecnológica, poderío económico e industrial y dejó el puesto a los países antes mencionados.

- Características

En esta época, el crecimiento de los países y naciones se dio en diferentes aspectos, tanto a nivel económico, social, cultural, tecnológico, etcétera.

En este sentido, el crecimiento que tuvo la agricultura se vio beneficiada por los diferentes aspectos que la engloban, siendo los más relevantes la mecanización y la utilización de fertilizantes artificiales.[12] Hay que señalar la rápida globalización de la especialización en la agricultura, al establecer en territorios de todo el mundo la producción distintiva, de forma tal que ciertas partes del mundo exportaban productos determinados para satisfacer la demanda de los países industrializados.

Algunos ejemplos son: Ganadería vacuna en EE.UU., y Argentina; Ganado Ovino en Australia; Agricultura de Plantación en países de América del Sur, Asia y África (fue desarrollado por empresas trasnacionales que tenían los recursos para cultivar y distribuir productos que en Europa son de lujo). [13]

Asimismo, a finales del siglo XIX se notaron cambios en el sector energético pues se amplió la gama de combustibles con el descubrimiento de la energía eléctrica y del petróleo.[14]

En el caso del petróleo, este repercutió en el sistema económico del mundo. Al no encontrarse en todos los lugares del mundo, especialmente en los países con un desarrollo industrial alto, se ampliaron las relaciones comerciales y políticas con la intención de obtener un recurso que no había en su territorio, y con un uso que cada vez iba al alza. Otro gran obstáculo era la prospección, extracción y refinación de este bien, por lo que sólo las grandes empresas pudieron explotar el petróleo, quedando en manos de muy pocos competidores toda la cadena de distribución del mismo.

Por lo tanto, los derivados del petróleo tuvieron un importante auge a causa de la invención y utilización de motores que necesitaban estos combustibles como

---

[12] IES Fray Pedro de Urbina, *La Segunda Revolución Industrial*, Departamento de Geografía e Historia. Recuperado el 14 de febrero de 2021, de: http*://www.iesfraypedro.com/files/sociales/segunda-industrial.pdf.*

[13] *Idem.*

[14] *Idem.*

lo hizo el motor de diésel, que era utilizado de forma masiva en la flota de guerra británica.

En el caso de la electricidad, esta tuvo gran impacto en las empresas que utilizaban el carbón para generar energía, puesto que ya no tenían la obligación de involucrarse directamente con las minas de carbón.

Otro de los sectores beneficiados vinculados a la minería, fueron la extracción y utilización del hierro, el cual tuvo un incremento enorme debido a que se necesitaba para la construcción de edificaciones o para los medios de transporte en esa época, o simplemente para su comercio con otras naciones. Esto dio como resultado que también mejorara la forma en que se producía y comerciaba el acero mediante la extracción del hierro; gracias a la innovación en la ciencia química, se pudieron hacer aleaciones que mejoraron la calidad del producto.

Sin embargo, el cambio más relevante fue la utilización de la mercadotecnia para la venta de productos a los consumidores de todo tipo. Se tuvo que recurrir al uso de imágenes para llegar a las personas que no sabían leer a fin de que ellos pudieran adquirir los productos ofrecidos.[15]

Con el tiempo, las formas de mercadotecnia se fueron desarrollando velozmente. Además de los carteles o afiches, surgió el uso de marcas y la venta por catálogo, métodos iniciados por los EE.UU. Sin embargo, allí no se detuvo; la publicidad también se hizo presente en los periódicos y revistas con la finalidad de llegar a más personas.

Como último punto, cabe destacar que la búsqueda de mejores condiciones de trabajo también tomó gran relevancia durante la época. En un futuro, esta serie de nuevas consideraciones iba a provocar un gran cambio en la perspectiva laboral.

En principio, la alta demanda de productos hacía que las empresas comenzaran a implementar un incremento de la producción, aumentando así las horas de trabajo y la mecanización del mismo, viendo al trabajador como un bien

[15] Miller, Ignacio David, *La Segunda Revolución Industrial*, Buenos Aires, Kapelusz, 2016, pp.15-26.

que tenían que explotar. Aunado a ello, se pensó en la forma de mejorar los sistemas productivos de las empresas, por lo que se crearon e implementaron métodos como el de Henry Ford y Frederick Taylor.

Estos fueron un éxito, en razón de que mejoraron la forma en que realizaban sus productos de comercio y, a su vez, se reducían costos debido al tiempo que invertían en crearlos. No obstante, dichos sistemas tenían contras que al principio no tuvieron tanta relevancia; sin embargo, años después causarían huelgas en las fábricas a fin de buscar mejoras en las condiciones de trabajo.

De este modo, los sistemas de producción que revolucionaron esta época consideraban al trabajador como un bien que se podía mecanizar para mejorar la cadena de producción y a su vez la cadena de distribución. Al ser condiciones desfavorables para los trabajadores, estos decidieron realizar diversos movimientos sociales para obtener lo que pedían, así como organizarse para realizar colectivos que los defendieran, lo que después se les denominaría sindicatos.

Esto causó una mejora en sus condiciones de trabajo y a la larga la implementación de los diferentes derechos laborales o derechos del trabajo que al día de hoy siguen vigentes.

1.2.4 Tercera Revolución Industrial

Después del avance tecnológico derivado de la Segunda Revolución Industrial, Estados Unidos, uno de los países con más índice de crecimiento, sufrió diversos obstáculos económicos que impidieron su crecimiento de forma exponencial, padeciendo un estancamiento secular en los años sesenta y setenta, lo que devino en diferentes recesiones económicas durante los años ochenta. Sin embargo, permitió que países como Japón comenzaran a sufrir un crecimiento tecnológico tan grande que los hizo posicionarse como potencia tecnológica.[16]

[16] Roel, Virgilio, *La Tercera Revolución Industrial y la Era del Conocimiento*, 3a. ed., Perú, Fondo Editorial UNMSM, 1998, p.17.

A esta época tecnológica también se le denominó Revolución de la Inteligencia o revolución científico-técnica.

1.2.4.1 Reconocimiento de la Tercera Revolución

El concepto de Tercera Revolución Industrial es acuñado por Jeremy Rifkin, quien en su obra *El fin del trabajo*, plantea la idea de que se está viviendo un momento de transformación rumbo a la ausencia del trabajo, en la que cada vez menos trabajadores producirían los bienes y servicios.

Rifkin establece que el empleo de energías renovables, la construcción de edificios que produzcan su propia energía, la transición del uso del hidrógeno como elemento de almacenaje energético y el uso de la tecnología del Internet, siendo el primero y este último los más relevantes, son los pilares de la Tercera Revolución Industrial.

Señala que el cambio climático, aumentado por la actividad industrial basada en combustibles de origen fósil, preocupa a los expertos debido a que se está al borde de una extinción masiva de la vida en el planeta. Una forma de revertir este suceso consiste en cambiar esta clase de combustibles por aquellos que no tuvieran un impacto negativo al ambiente.[17]

Además, el uso del internet para lograr innovación tecnológica que facilite la información y la comunicación entre las personas, ha incrementado de forma sustancial, fungiendo como enlace para el desarrollo de energías renovables.

Uno de los principales riesgos al usar las tecnologías de la información es la desigualdad al momento de acceder a ellas, derivado de los cambios socioeconómicos y políticos que sufre una sociedad al existir una Revolución Industrial, tal y como sucedió en las revoluciones industriales anteriores.

[17] Lastra Lastra, José Manuel, Rifkin, Jeremy, *La Tercera Revolución Industrial*, *Boletín Mexicano de Derecho Comparado*, Ciudad de México, v. 50, núm. 150, dic. 2017, pp. 1457-1462. Recuperado el 29 de agosto de 2021, de: *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332017000301457&lng=es&nrm=iso.*

1.2.5 Cuarta Revolución Industrial

Tal y como sucedió en las revoluciones industriales anteriores, en la Cuarta Revolución Industrial se están produciendo cambios políticos, económicos, sociales y culturales que causan cambios en la percepción que se tiene de la realidad.

1.2.5.1 Inicio de la Cuarta Revolución Industrial

La Cuarta Revolución Industrial se dio a principios de este siglo con la digitalización progresiva, esto significa la convergencia entre las diferentes tecnologías digitales, físicas y biológicas como la inteligencia artificial, la inteligencia aumentada, la robótica, la impresión 3D, la *cloud computing*, el *big data*, avances en el internet de las cosas o la nanotecnología.[18]

Actualmente, las computadoras y los robots realizan actividades de nuestra rutina de forma más eficiente y a un menor costo si se compara con las actividades que puede hacer una persona en determinado tiempo. Esto provoca que su uso en la industria sea de forma recurrente debido a que aumenta la productividad, siendo esto aprovechado por empresas trasnacionales y nacionales. [19]

Ante esto, surge la existencia de fábricas inteligentes que se adaptan eficientemente a los procesos productivos marcados por las necesidades de los consumidores y fabricantes. Un ejemplo de ello es el mantenimiento realizado por máquinas, ya sea que lo inicien o que los trabajadores reciban determinado tipo de asistencia por medio de sistemas inteligentes.

En conclusión, la Cuarta Revolución Industrial es el conjunto de cambios que se viven en la actualidad, esperando a que se cumplan las expectativas planteadas al principio; no obstante, los resultados se notarán una vez que se terminen estos

---

[18] Escudero Naón, Alexandro, *Redefinición del 'aprendizaje en red' en la cuarta revolución industrial,* en *Apertura (Guadalajara, Jal.),*Guadalajara, X, núm. 1, 2018, pp.149-163, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665618020180001001 49#B26.*

[19] Vila de Prado, Roberto, *Consecuencias económicas y sociales de la cuarta revolución industrial y estrategias pensadas para la adopción de la actividad económica, Revista Aportes de la Comunicación y la Cultura,* núm. 26, junio 2019, pp.89-108. Recuperado el 19 de agosto de 2021, de: *http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2306867120190001000 10*

cambios o, hasta que, aparezca un nuevo conjunto de pensamientos llevados a la realidad y cambien la percepción de la ya existente.

1.3 Orígenes del Internet

El Internet no tiene un comienzo tan comercial como se llega a pensar en la actualidad. El inicio de esta herramienta tecnológica se pierde en el tiempo debido a su uso común y renovación constante.

Tuvo su origen en los Estados Unidos de América durante la Guerra Fría, una época muy complicada para el mundo. Los avances tecnológicos tenían un fin bélico y de competencia con la URSS, por lo que el gobierno de los Estados Unidos realizó varias investigaciones que implicaban el estudio y la aplicación de diversas tecnologías para lograr la comunicación de sus fuerzas armadas. Por consiguiente, el inicio del Internet se dio como parte de proyectos de investigación realizados por la Red de la Agencia de Proyectos de Investigación Avanzada (ARPA por sus siglas en inglés) a cargo de la Armada de EE.UU.; en resumen, fue pensado para uso exclusivo de la milicia.

Una vez que su uso dejó de ser exclusivo para las Fuerzas Armadas, en el año de 1965 fue posible enlazar dos computadoras en diferentes territorios de los Estados Unidos de América. A pesar de ser un avance importante, se mostró que esta tecnología aún no tenía la suficiente capacidad de transferir datos; por ende, no era llamativa para las empresas.[20]

Llegado el año de 1969, varias universidades de EE.UU. pudieron conectarse entre ellas por medio de una red informática denominada ARPAnet, cuya red tenía como característica la ausencia de nodos centrales y de la cual formaban parte la Universidad de Utah, *Stanford Research Institute*, Universidad de

[20] Master Marketing, *¿Cuándo nació Internet? Historia y evolución,* 2019. Recuperado el 13 de marzo de 2021, de: *https://www.mastermarketing-valencia.com/marketing-digital/blog/internet-historia-evolucion/*

California, Santa Bárbara y la Universidad de California, Los Ángeles.[21] En años posteriores, el uso de ARPAnet fue únicamente para el almacenamiento de información y el envío y recepción de correos electrónicos.[22]

Para el año de 1982, ARPA declaró el protocolo TCP/IP (*Transfer Control Protocol/Internet Protocol*), una base para el intercambio de información entre los ordenadores, dando como resultado la primera definición de Internet: "conjunto de redes interconectadas mediante TCP/IP".[23]

Entre los años 1989 y 1990, Tim Berners Lee, un investigador del CERN (Organización Europea para la Investigación Nuclear), buscó facilitar el intercambio de información entre los investigadores, por lo que creó un *software* que permitió visualizar la información desde cualquier nodo de la red a través de *HTML,* un hipertexto que lograba adjuntar y/o utilizar imágenes, objetos y video. Con posterioridad, se le conocería como *World Wide Web* ("www", como se conoce en la actualidad) a la red de Internet.

1.3.1 Evolución del Internet

Aunque el internet ya se podía utilizar por personas que se dedicaban a realizar investigaciones o a impartir clases, aún faltaba que cualquier persona ajena a estos campos pudiera acceder a ella. Por ello, el siguiente paso fue lograr un acceso universal a esta tecnología.

En el año de 1993, ya con la apertura del Internet con fines comerciales, los colaboradores de Marc Andreesen, un ingeniero que trabajaba en la innovación del uso de Internet, ofertó a varias personas el navegador *Mosaiconline*, un navegador con fines académicos, con la finalidad de observar si lograba tener la atención de las personas y analizar su utilidad.

---

[21] Trigo Aranda, Vicente, *Historia y evolución de Internet*, *Manual formativo de ACTA*, núm.33, 2004, pp. 22-32. Recuperado el 22 de septiembre de 2021, de: *https://dialnet.unirioja.es/servlet/articulo?codigo=5098592*

[22] *Idem.*

[23] *Idem.*

En 1994, los colaboradores de Marc, en colaboración con el empresario James Clark, amplio creyente de la convergencia de los medios con la tecnología digital, se plantearon la idea de convertir *Mosaic* en una empresa que pudiera proveer a las personas un navegador que le hiciera competencia al en ese momento máximo proveedor, *Microsoft*.

Lograron lanzar *Netscape*, un adversario comercial para el que en ese momento era el mejor navegador de la época: *MSN.com*., el cual estaba instalado en todas las computadoras que tenían un *software* de *Microsoft*.

Navigator Netscape se convirtió en un éxito total. Lo llevó a generar ganancias tan desproporcionadas que desbancó a la empresa de Bill Gates (dueño y fundador de *Microsoft*) como el navegador más usado en esa época. Esto provocó una competencia por el mercado que ayudaría a la mejora tecnológica en este campo.

Mientras *Netscape* se ocupaba del manejo de sus finanzas, *Microsoft* se ocupaba de crear un navegador más eficiente y con una propuesta comercial mejor que la de su competidor principal. Para 1995 nace *Internet Explorer*, un navegador menos eficiente, pero con la ventaja de ser gratuito.

Bill Gates y su equipo pensaron que la mejor estrategia para hacer llegar a más hogares su navegador era regalarlo y preinstalarlo en los dispositivos que tuvieran un *software* de *Microsoft*, por lo que, al contrario de *Netscape*, llegó a más personas sin tener que pagar un precio por él.

Esto trajo la caída de *Netscape* y el posicionamiento de *Microsoft* en el mercado del Internet y de los navegadores. Lo que se traduce en un impacto enorme en el crecimiento del Internet desde la disputa entre estos dos proveedores de navegadores.

1.3.2 Buscadores

En el año de 1994, dos estudiantes de la universidad de Stanford, Jerry Yang y David Filo, crearon lo que más tarde sería el primer buscador; sin embargo, su invención se dio sin la intención de realizar un negocio. Comenzó con el objetivo de

almacenar las direcciones que les atraían; posteriormente, publicarían su catálogo para que las personas pudieran acceder de forma gratuita a los datos recopilados por ellos.[24]

Esto provocó que a diversas personas se les facilitara el contenido que querían consultar. Toda la información se encontraba a la mano y clasificada, causando que las personas que usaran esta herramienta quisieran la ampliación del contenido y se pudiera organizar una mayor cantidad de información.

Esta popularidad provocó que Jerry y David cambiaran el enfoque de lo que habían creado, mirándolo ahora como una oportunidad comercial y ya no solo de entretenimiento. Después de varios nombres sin un gran atractivo comercial, el nombre de *Yahoo* le dio esa distinción que tanto buscaban.

Tenía tanto éxito su navegador que, a causa de la popularidad y gran demanda de este, necesitaban dejar de usar el servidor de la Universidad debido a un eminente colapso. Se mudaron de Stanford y con ello en años posteriores *Yahoo* cayó en la bolsa; es decir, sus acciones cotizaban en el año 2002 alrededor de 15 dólares.

En la actualidad, *Yahoo* sigue existiendo. Sin embargo, ya no es el principal motor de búsqueda para las personas, siendo sustituido por otro que mejora las cualidades de búsqueda y de organización, así como la disponibilidad para obtener y publicar información.

La necesidad de mejorar las herramientas de búsqueda y ofrecer variedad en sus motores provocaron, entre otros motivos, que en el año de 1998 Larry Page y Sergey Brin crearan *Google*. Uno de los más grandes buscadores en la actualidad se mostró ante el mundo del Internet como un motor de búsqueda moderno al utilizar una nueva forma de clasificar las páginas web en función de su importancia.[25]

[24] Trigo Aranda, Vicente*, op.cit.*
[25] *Idem.*

No obstante, aunque los avances en el uso del Internet han sido enormes como lo fueron la creación de esos motores de búsqueda, no significa que los avances tecnológicos hayan causado únicamente beneficios.

Se ha dicho, dentro del mundo cibernético, que las personas desconocen más de lo que conocen del Internet; es decir, únicamente rasgan la superficie de todo lo que implica navegar. Para su explicación, estos espacios se pueden dividir en: *Surface Web* (Internet superficial), *Deep Web* (Internet profunda) y *Dark Web* (Internet oscuro).

Para ilustrar de mejor manera el alcance y contenido que hay en Internet, se utiliza la imagen de un iceberg; la intención es representar de forma más didáctica el alcance y el contenido que abarca el Internet. En la parte superior del iceberg se coloca la *Surface Web*, en la cual únicamente se encuentra toda aquella información que podemos obtener a través de los buscadores, por ejemplo: redes sociales (no implica su acceso), sitios de *e-commerce* como *Amazon* o *Linio*, portales de Internet comunes en los que encontramos información académica como *Scielo* o *Wikipedia*, así como sitios web que nos permiten acceder a contenido de video o audio como *YouTube* (de forma gratuita; es decir, sin suscripción).

Esto es así debido a dos de sus características principales:

a) Las páginas de Internet son indexadas por los buscadores; es decir, registran los sitios web que quieren que se puedan encontrar mediante el uso de este, provocando así su acceso público.
b) La carencia de una contraseña o un código para acceder a ellas.

En conclusión, los servicios antes mencionados se colocan dentro de la *Surface Web* pues es de fácil acceso para la mayoría de las personas con disponibilidad para conectarse a Internet. Además, es lo primero a lo que se tiene acceso al momento de navegar.

En la segunda sección del iceberg, la parte situada por debajo del agua, se encuentra la *Deep Web.* En esta parte reside toda aquella información a la que se

puede acceder únicamente entrando al sitio directamente y con contraseña o sin ella, siendo esta parte del 90% de todo el contenido disponible en Internet.

En la *Deep Web* no sólo se encuentra contenido conocido como ilícito, como páginas de internet para ver películas o descargar música, sino que se encuentran también aquellos sitios de uso común como el uso del correo electrónico, servicios de mensajería instantánea, uso de servicios de *streaming*, videoconferencias, banca en línea, *intranets* de gobiernos o empresas, entre otros.

Respecto a ello, el uso del contenido disponible en la *Deep Web* ha ido en aumento, tal y como lo muestra el 17° Estudio sobre los Hábitos de los Usuarios de Internet en México 2021, realizado por la Asociación de Internet en México.[26]

En la tercera sección del iceberg se encuentra la *Dark Web*, la cual es una pequeña parte de la *Deep Web* donde está todo ese contenido indexado a navegadores especializados, siendo estos de menor contenido que los navegadores más conocidos.

El uso de la *Dark Web* se debe principalmente al anonimato; la mayoría de los navegadores permiten desplazarse por estos sitios sin que se deje gran huella del paso de los usuarios.

Sin embargo, debido a la confidencialidad con la que se accede y se está en estos sitios, es factible que se encuentren sitios en los que se comparte contenido de forma ilícita. Por lo tanto, es posible encontrarse con personas que realicen actos ilegales como el robo de información o venta de armas de fuego, siendo además vulnerables a ataques cibernéticos.

[26] Asociación de Internet de México, *17° Estudio sobre los Hábitos de los Usuarios de Internet en México,* 2021, Recuperado el 14- de febrero- de 2022, de: *https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v16%20Publica.pdf.*

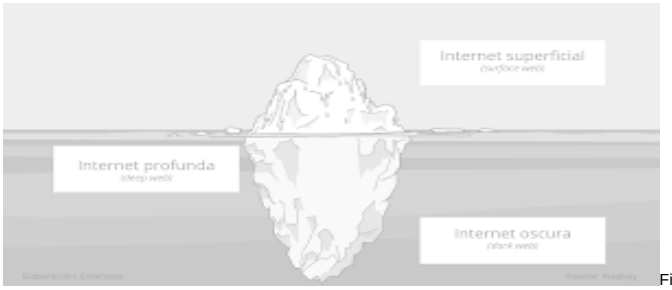


Figura 1.[27]

1.4 El Internet en la legislación mexicana

La legislación mexicana carece de una regulación específica del Internet. Al traspasar fronteras, se provocaría una invasión de facultades entre Estados si se intenta regular por un gobierno externo.

Además, regular el Internet de forma específica implicaría realizar una investigación tan amplia como el Internet mismo puesto que en la actualidad casi todo lo que nos rodea tiene que ver con el mundo digital. Sin embargo, eso no excluye que se intenten regular todas aquellas situaciones y hechos vinculados al Internet, como lo serían la defensa de los derechos humanos en el Internet, el acceso a Internet y el comercio electrónico.

1.4.1 El Internet como Derecho Humano en la constitución mexicana

Dentro de la legislación mexicana, la relación que guarda el Internet con los derechos humanos implica todo lo que tiene que ver con el acceso que tienen las personas a él.

De forma tal que, para darle la importancia que implica el acceso a Internet, se tuvieron que realizar ciertas modificaciones a los artículos constitucionales que involucraban los derechos a proteger para tener la posibilidad de acceder.

Es por ello que se reformaron los artículos 6°, 7°, 27 y 28 de la Constitución mexicana, derivado de la implementación de diversas reformas jurídicas en materia de telecomunicaciones para atender los diversos inconvenientes que implica combatir la brecha digital.

[27] **Figura 1.** *Imagen explicativa sobre los niveles que tiene el Internet*, 2019, Recuperada el 1 de octubre de 2021, de: *https://www.enterarse.com/20191011_0001-lo-mas-profundo-del-internet-que-son-la-deep-web-y-la-dark-web*

En el artículo 6° se establece el derecho de acceso a Internet como derecho fundamental que ejerce como mecanismo de entrada para ejercer los demás derechos.

El artículo antes mencionado, en conjunto con el artículo 7° del mismo ordenamiento, aborda temas sobre la libre manifestación de las ideas sin afectar a un tercero y/o sin perturbar el orden público, además de la búsqueda y recepción de información por cualquier medio incluyendo el entorno digital. En el apartado B de este mismo artículo, se establece el acceso a las diferentes tecnologías de la información a través de diversos mecanismos que permitan la inclusión digital bajo los estándares mínimos que garanticen estos derechos.

Asimismo, la relevancia del artículo 27 es la administración de las redes de telecomunicaciones y radiodifusión por parte del Estado.

Por último, el artículo 28 incluye cuestiones de competencia económica en materia de telecomunicaciones y radiodifusión, así como la creación de un ente con autonomía constitucional con la facultad de hacer lo necesario para disminuir la brecha digital; es decir, garantizar el acceso a estos medios de información.

1.4.2 El Internet como Derecho Humano en los tratados y convenios internacionales

En el año de 2006, la Asociación para el Progreso de las Comunicaciones elaboró una carta sobre derechos en Internet, sirviendo como precursor para considerar el acceso a Internet como derecho humano.

Por ello, en el año 2011, se declaró como derecho humano el acceso a Internet por parte de la Asamblea General de la ONU, iniciando así diversas reformas a los tratados internacionales en materia de Derechos Humanos.

Entre ellas se encuentra la resolución para la “promoción, protección y el disfrute de los derechos humanos en Internet”, expedida por el Consejo de Derechos Humanos para la protección del derecho de acceso a Internet como derecho humano. A la letra, establece lo siguiente:

(…) Observando que el ejercicio de los derechos humanos, en particular del derecho a la libertad de expresión, en Internet es una cuestión que reviste cada vez más interés e importancia debido a que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones, Tomando nota de los informes del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, presentados al Consejo de Derechos Humanos en su 17º período de sesiones y a la Asamblea General en su 66º período de sesiones, relativos a la libertad de expresión en Internet.

1. Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;

2. Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;

3. Exhorta a los Estados a que promuevan y faciliten el acceso a Internet y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;

4. Alienta a los procedimientos especiales a que tengan estas cuestiones en cuenta en sus mandatos actuales, según proceda;

5. Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede

ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo (…).[28]

La mayoría de los tratados internacionales en materia de Derechos Humanos que no consideran de forma explícita el acceso a Internet como un derecho, sí protegen los derechos relacionados a este último, como lo son el derecho de acceso a la información, derecho a la libertad de expresión y el derecho de asociación. Algunos de estos instrumentos son:

- Pacto Internacional de Derechos Civiles y Políticos (PIDCP).
- Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC).
- Declaración Universal de los Derechos Humanos (DUDH).
- Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos.

1.5 Instrumentos normativos que regulan diversos aspectos del Internet en México

En México, la mayoría de las disposiciones que existen respecto al Internet son las que se enfocan en las diferentes áreas de la vida donde esta herramienta es parte fundamental para su desarrollo, siendo reguladas por disposiciones de otras materias.

Sin embargo, también existen algunas disposiciones normativas que tratan de regular aspectos más concretos del Internet como su uso de forma genérica. Es decir, se enfocan en los aspectos técnicos y los derechos de forma general que se tienen al usar el Internet sin señalar algún uso en específico.

[28] Consejo de Derechos Humanos, 20º período de sesiones, Tema 3 de la agenda *Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales*, incluido el derecho al desarrollo del 29 de junio de 2012.

1.5.1 Ley Federal de Telecomunicaciones y Radiodifusión

La LFTyR fue publicada el 14 de julio de 2014 en el Diario Oficial de la Federación y entró en vigor el 13 de agosto del mismo año. Desde su entrada en vigor hasta la fecha de realización del presente trabajo han transcurrido siete años, dentro de los cuales el Internet era uno de los puntos importantes a tomar en cuenta.

La inclusión del Capítulo VI de la Ley antes referida hace referencia a la neutralidad de las redes, tema que involucra diversos derechos humanos como la no discriminación y la protección de datos personales, así como las características que deben cuidar los proveedores de este servicio para que el usuario pueda tener un acceso a Internet seguro.

Además, contiene el Título Noveno denominado “De los usuarios”, el cual es un apartado especial respecto a los derechos que tienen los usuarios al contratar servicios de telecomunicaciones o los derechos que se adquieren una vez contratado un servicio de telecomunicaciones. En el mismo capítulo se establecen los medios por los cuales se protegen estos derechos.

1.5.2 Lineamientos de Neutralidad de la Red

El Instituto Federal de Telecomunicaciones (IFT) tiene la obligación derivada del artículo 145 de la LFTyR y de la resolución con número de expediente 32/2019 emitida por el Segundo Tribunal Colegiado en el que ratifica la resolución emitida por el Juzgado Segundo de Distrito; se establece la obligación de expedir y publicar los lineamientos correspondientes (en materia de neutralidad de la red) a más tardar al concluir el segundo periodo trimestral del año 2021.

Es por eso que el 5 de julio de 2021 fueron publicados en el Diario Oficial de la Federación los “Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet”, los cuales son conocidos como lineamientos en materia de neutralidad de la red.

Estos lineamientos desarrollan a fondo lo establecido en el artículo 145 de la Ley mencionada en párrafos anteriores, siendo los temas de gestión de tráfico, administración de la red y de la transparencia de la información los más relevantes.

En el artículo 4° de dichos lineamientos se establece la obligación por parte de los Prestadores de Servicios de Internet de asegurarse que las políticas de gestión de tráfico y administración de red que implementen protejan la libre elección que tienen los usuarios para acceder a los contenidos sin limitaciones, así como mantener el derecho a la privacidad que se tiene respecto al contenido consultado.

En el artículo 5° se señala que los proveedores de servicios de Internet no podrán establecer políticas de gestión de tráfico que limiten, degraden, restrinjan, discriminen, obstaculicen el acceso a contenidos, salvo que sean de forma temporal y en los casos que pongan en riesgo la seguridad e integridad de la red.

Por último, se señala la obligación contenida en el artículo 12 de mantener actualizado el Código de Políticas de Gestión de Tráfico y Administración de Red, así como publicarlo de forma accesible para que los usuarios finales puedan consultarlo, estableciendo en él los derechos a proteger.

Al expedir los lineamientos antes mencionados se le da forma a la regulación de los diferentes temas que de forma periférica rodean el derecho de acceso a Internet. Para poder tener acceso al Internet, los derechos humanos que se ven involucrados deben estar protegidos por una disposición normativa más específica, estableciendo los alcances de éstos.

Asimismo, deben regularse las cuestiones técnicas necesarias para el fácil acceso a la red y así desvanecer la brecha digital existente en nuestro país.

1.6 Regulación del Internet por organismos internacionales

Existen diversos organismos internacionales que, mediante grupos de trabajo y la publicación de diversos estudios o disposiciones, han puesto las bases sobre las cuales se debe guiar la regulación de diversos aspectos que involucran al Internet.

A nivel regional, se encuentra la Comisión Interamericana de Telecomunicaciones (CITEL), la cual funciona como órgano asesor de la OEA en los asuntos relacionados con las Telecomunicaciones y las TIC. Esta última tiene como objetivo facilitar el desarrollo de las telecomunicaciones en la región de los estados americanos.

Su origen data desde 1993, mediante la resolución de la Asamblea General AG/RES. 1224 (XXIII-O/93), de conformidad con el artículo 51° de la carta de la OEA, la cual establece la obligación por parte de los Estados para fomentar la ciencia y la tecnología, así como estimular las actividades en el campo de dicha área con la finalidad de concertar la cooperación de esta materia, así como la ampliación de los conocimientos.

Algunos de los objetivos de este organismo son:[29]

a) Facilitar y promover, por todos los medios a su alcance, el desarrollo continuo de las telecomunicaciones/tecnologías de la información y la comunicación (TIC) (en adelante, telecomunicaciones/TIC) en el Hemisferio, en pro del desarrollo sostenible.

b) Promover y fomentar la existencia de telecomunicaciones/TIC apropiadas que contribuyan al proceso de desarrollo integral de la región, con especial atención a las zonas desatendidas.

c) Organizar, promover y evaluar la realización periódica de reuniones de técnicos y expertos para estudiar la planificación, financiamiento, construcción, operación, normalización, asistencia técnica, mantenimiento y otros asuntos relacionados con el uso y desarrollo de las telecomunicaciones/TIC en las Américas.

d) Promover la unificación de criterios y estándares técnicos para la instalación, operación y mantenimiento de los sistemas, a fin de obtener el máximo beneficio de las facilidades con que cuenta cada

[29] OEA, *Sobre la CITEL*. *Recuperado el 20 de agosto de 2022, de: https://www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/citel/About/Details/category/citel/about-citel*

país y la región en general, en el marco de normalización global de la Unión Internacional de Telecomunicaciones (UIT) y otras organizaciones de normalización pertinentes.

e) Promover y estudiar la asistencia técnica, de acuerdo con los gobiernos de los respectivos países, dando prioridad a las necesidades de los países en desarrollo.

f) Fomentar el mejoramiento y armonización de los procedimientos administrativos, financieros y operativos para la planificación, instalación, mejoramiento, mantenimiento y operación de las redes de telecomunicaciones de los Estados Miembros de la CITEL, en el marco de las recomendaciones de la UIT, así como de otras organizaciones internacionales y regionales, que promueven el acceso generalizado a los servicios, el uso de nuevas tecnologías, la creación de empleo y el despliegue de infraestructura en áreas desatendidas.

g) Recomendar estudios y promover la adopción de acuerdos oficiales entre los gobiernos de los Estados miembros de la Organización para la planificación, instalación, mantenimiento y operación de los sistemas de telecomunicaciones en el Hemisferio.

h) Promover y fomentar el estudio y difusión de los problemas relacionados con el impacto de las telecomunicaciones en el medio ambiente y el cambio climático y su relación con las TIC, de acuerdo con las políticas desarrolladas por la UIT y otros organismos con competencia en esta materia.

De los objetivos se puede desprender que las actividades se enfocan en el desarrollo, la promoción, la elaboración de estudios, proyectos y la promoción de acuerdos en donde la coordinación de Estados es fundamental para el acceso a las TIC y las telecomunicaciones; dichas actividades se enfocan en los miembros de la organización para el desarrollo de la región.

Dentro de sus principales funciones se encuentran las siguientes:[30]

a) Actuar como principal órgano asesor de la Organización en todos los asuntos relacionados con las telecomunicaciones/TIC en el Hemisferio.

b) Promover o realizar estudios y programas para el desarrollo ordenado de las redes de telecomunicaciones / TIC, utilizando los sistemas más adecuados y eficientes disponibles.

c) Elaborar estudios sobre políticas públicas en el área de las telecomunicaciones / TIC.

d) Revisar y evaluar la eficacia de la cooperación técnica con la UIT y otras organizaciones regionales e internacionales de manera continua.

En cuanto a la regulación del Internet, así como su acceso, la CITEL ha realizado, en participación conjunta con la UIT, diversas investigaciones que tienen como objetivo ofrecer una visión diferente de la región respecto a esta herramienta.

Por lo anterior, la CITEL es, junto con la UIT, un organismo especializado en materia de telecomunicaciones que tiene como objetivo promover el avance en esta tecnología para lograr un crecimiento económico de la región, lo cual favorecería a todos los actores que participan en la cadena de los dispositivos del *IoT*, así como del Internet por sí solo.

Dentro de esas investigaciones, se encuentra la realizada bajo el acuerdo PCC.I/DEC.258 (XXIX-16), denominada *South School on Internet Governance*, entre otras.

[30] *Idem*

CAPÍTULO 2. EL INTERNET DE LAS COSAS

2.1 Concepto de Internet de las cosas

El Internet de las cosas es conceptualizado por la UIT como "la Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras".[31]

Para la OCDE, el Internet de las cosas comprende a los dispositivos y objetos cuyo estado puede alterarse a través de Internet, con o sin la participación activa de las personas, permitiendo incluir dispositivos como teléfonos inteligentes (*smartphones*), tabletas electrónicas, *routers, laptops*, entre otros.[32]

Una conceptualización menos técnica del internet de las cosas es aquella que describe Andrés Moisés Barrio en su libro *El Internet de las cosas*. Barrio señala que el *IoT* es aquella tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico para proporcionar servicios de valor añadido a los usuarios finales.

Por consiguiente, el Internet de las cosas es entendido como la comunicación electrónica entre objetos cotidianos, dentro de la cual comparten información y datos específicos entre ellos y/o el mundo que los rodea. Barrio conceptualiza de forma más clara lo que se debe de entender por Internet de las cosas, siendo ésta la que se va a usar de forma recurrente en el presente trabajo.

2.2 Antecedentes del Internet de las cosas

En los años 70's, el departamento de Ciencias de la Computación de la Universidad de Carnegie Mellon conectó una máquina dispensadora de *Coca-Cola*

[31] ITU, Series Y, *Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Overview of the Internet of Things*, 2012, p.2. Recuperado el 2 de mayo de 2021, de: *https://www.itu.int/rec/T-REC-Y.*

[32] OCDE, *OECD Digital Economy,* Outlook, 2015, p. 61. Recuperado el 3 de mayo de 2021, de: https://www.oecd.org/digital/oecd-digital-economy-outlook-2015-9789264232440-en.htm

a la PDP-10, que era en ese entonces la computadora principal de la universidad, con la intención de controlar el estado de la máquina y el tiempo en el que han estado las botellas dentro de la máquina; por lo tanto, se lograba identificar la temperatura de las botellas y así poder tomar un envase frío.[33]

Posteriormente, los envases de *Coca-Cola* fueron renovados y, por ende, la máquina ya no podía analizar su temperatura pues uno de los elementos tomados en cuenta era el tamaño de los envases; de esta forma, fue desconectada de la red.[34]

Sin embargo, a estos dispositivos aún no se les conocía como objetos del Internet de las cosas puesto que el término no existía. Fueron objetos que sirvieron para dar una idea de lo que en un futuro sería la conexión de objetos comunes a la red.

Aunque ya había conexiones inalámbricas entre dispositivos, éstas atendían a los estándares de la industria para las cuales fueron hechas; utilizaban redes creadas para un propósito: la comunicación entre dispositivos.

No fue sino hasta la década de los 90's, durante la conferencia de INTEROP, cuando se presentó el primer dispositivo cotidiano conectado a una red de Internet. Una tostadora fue el primer objeto con este tipo de características; tenía la capacidad para conectarse a una red de Internet y mediante un control remoto encenderse y apagarse. No obstante, aún necesitaba la interacción de una persona debido a que no tenía la capacidad de colocar el pan por sí solo.

Al año siguiente se le colocó un brazo robótico a fin de poder colocar el pan dentro de la tostadora; también usaba la conexión a Internet para realizar esa función, por lo que en ese momento la tostadora era casi por completo un dispositivo con conexión sin la intervención de una persona.

Fue tiempo después cuando el concepto de Internet de las cosas fue usado por primera vez. Kevin Ashton, en una presentación para un proyecto de la empresa

[33] Carnegie Mellon University, *The "Only" Coke Machine on the Internet*, School of Computer Science. Recuperado el 31- de marzo- de 2021, de: https://www.cs.cmu.edu/~coke/history_long.txt
[34] *Idem*

P&G, en los años 90's, necesitaba un nombre llamativo para la presentación que incluyera la palabra Internet. Debía tener un enfoque muy cercano a lo que trataban de lograr, y así fue como surgió este término.[35]

La implementación de etiquetas de radiofrecuencia y sensores en los productos que intentaba comercializar *P&G* buscaba generar datos sobre la ubicación del producto, por lo que al mencionar el título de la presentación llamó la atención el encabezado. De este modo, aceptaron la propuesta y en días posteriores la empresa *Gillette* le ofreció financiar su investigación. [36]

Asimismo, a principios del nuevo siglo, *LG* anunció al mundo sus planes de producir y comercializar un refrigerador conectado a Internet. Su función consistía en hacer un registro de los objetos que almacenaba dentro de él; sin embargo, esta idea no obtuvo frutos al ser una opción demasiado costosa para satisfacer una necesidad que podía cumplir un refrigerador convencional.[37]

Por consiguiente, la conexión de los diversos objetos existentes no era de gran relevancia en esa época. El término del Internet de las cosas apenas era un concepto que se utilizó de forma local; es decir, para nombrar la idea que quería mostrar Kevin Ashton a una empresa. En resumen, aún no se logró impulsar la adopción de este término para todo objeto que se podía conectar a una red de Internet.

Sin embargo, el tema de los objetos conectados a Internet y la frecuencia con la que comenzaron a usarse estos productos propiciaron que en años posteriores la ITU, en el año 2005, emitiera su primer informe sobre el tema.

2.3 Regulación del Internet de las cosas

El uso de los dispositivos conectados a Internet no solamente es una tendencia que va al alza, es una temática del presente. Hoy en día, existen

[35] Elder, Jeff, *Kevin Ashton nombró El Internet de las Cosas*, 2019. Recuperado el 19 de octubre de 2021, de: https://blog.avast.com/es/kevin-ashton-named-the-internet-of-things.
[36] *Idem.*
[37] RYT9, *LG Introduced Internet Digital DIOS Refrigerator*, 2000. Recuperado el 20 de octubre de 2021, de: *https://www.ryt9.com/en/prg/23392*.

dispositivos pequeños de medición y automatización en una bombilla, un despertador o un refrigerador, con la intención de mantener todo conectado a Internet y facilitar la interacción en el mundo.

Debido al previsible aumento en el uso de estos dispositivos, se necesita establecer una regulación del Internet de las cosas. Es preciso tratar de abarcar un catálogo de los objetos que forman parte de este grupo, así como establecer reformas a la normatividad existente para que incluya de forma específica un catálogo de los objetos conectados a Internet o la creación de un dispositivo normativo que permita establecer de forma concentrada todos los puntos a tratar sobre el asunto.

A nivel internacional, se encuentran diversas regulaciones técnicas sobre el *IoT*, resaltando aquellas emitidas por la Unión Internacional de Telecomunicaciones y las realizadas por la Unión Europea u otras organizaciones o integraciones.

La ITU, en el año 2005, dio a conocer su primer informe sobre el Internet de las cosas[38]. Se abordaron temas como ¿qué es el Internet de las cosas?, la tecnología que usa para funcionar, así como las aplicaciones y las áreas de oportunidades a las que se puede tener acceso al hacer uso de esta tecnología.

A partir de la publicación de este estudio, la ITU mostró la intención de establecer los parámetros generales sobre los que se debían basar los demás países para considerar la regulación de los objetos conectados a Internet.

En el mismo año, la Unión Europea (UE) emitió un plan denominado "*i2010*: Una sociedad de la Información Europea para el crecimiento y el empleo", con el propósito de coordinar a los integrantes de la unión y afrontar los desafíos de la sociedad de la información[39] debido al incremento en el uso de esta tecnología en un futuro.

---

[38] International Telecommunication Union, *The Internet of Things*, 2005. Recuperado el 11 de noviembre de 2021, de: *https://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf*

[39] BBVA, *Hora de regular el Internet de las cosas en la UE*, 2018. Recuperado el 14 de noviembre de 2021, de: *https://www.bbva.com/es/hora-regular-internet-las-cosas-la-ue/*

Posteriormente, en el año 2012, bajo la recomendación ITU-T Y.2060, este organismo internacional muestra lo que se debe considerar por Internet de las cosas, sus alcances, sus características fundamentales, así como los requisitos de alto nivel del *IoT* y sus modelos de referencia.

Con esta recomendación, la ITU sienta las bases de lo que se debe considerar al momento de invertir, estudiar, regular o hacer uso de esta tecnología que va en ascenso en el mundo entero. A la actualidad, el Internet de las cosas forma parte de nuestra vida cotidiana.

A la fecha, la ITU ha promovido otras recomendaciones en materia de Internet de las cosas, las cuales ayudan a complementar la recomendación antes mencionada. Algunas de estas recomendaciones son:

- UIT-T Y.2069 (07/2012)

Esta recomendación especifica los términos y definiciones relativos al *IoT* con el fin de explicar y describir las actividades relacionadas con la misma. [40]

- UIT-T Y.2066 (06/2014)

Esta recomendación se basa en la visión que de forma general da la recomendación UIT-T Y.2060, basándose en el amplio uso de esta tecnología y de los actores que intervienen en la producción, venta y uso de éstos.

Estableciendo los requisitos no funcionales, requisitos del soporte de aplicaciones, requisitos de servicio, requisitos de comunicación, requisitos de los dispositivos, requisitos de gestión de datos y requisitos de seguridad y protección de la privacidad.[41]

- UIT-T Y.2074 (01/2015)

[40] UIT. Y.2060, *Visión general de la Internet de las cosas*, 2012. Recuperado el 14 de noviembre de 2021, de: *https://www.itu.int/rec/T-REC-Y.2060-201206-I/es.*
[41] UIT, *Requisitos comunes de la Internet de las cosas*, 2014. Recuperado el 14 de noviembre de 2021, de: *https://www.itu.int/ITUT/recommendations/rec.aspx?rec=12169&lang=es.*

Esta recomendación está enfocada a los requisitos que deben tener los dispositivos del *IoT* al momento de estar en situaciones de catástrofes, así como los requisitos para utilizar dichos dispositivos en esos hechos.[42]

- ITU-T Y.2076 (02/2016)

Esta recomendación especifica los requisitos semánticos y el marco del *IoT*, en la que se incluyen aspectos semánticos de estos servicios en distintos dominios de negocio, entre otros.[43]

- UIT-T Y.4113 (09/2016)

Esta recomendación está enfocada en las funciones de transporte de red, así como las funciones de soporte de servicios, con la implantación de medidores inteligentes y sensores.[44]

- ITU-T Y.4203 (02/2019)

Esta recomendación busca auxiliar en la representación de diferentes objetos físicos de manera eficaz y de manera homogénea en el mundo virtual para reflejar su relación. Así como, establecer los requisitos para la descripción de estos objetos. [45]

- ITU-T Y.4475 (08/2020)

Esta recomendación establece las bases de marco de *software* ligero, la cual se encarga de soportar las aplicaciones del Internet de las cosas que requieren procesamiento inteligente y permite su funcionamiento en dispositivos con recursos limitados. [46]

---

[42] *Idem.*
[43] *Idem.*
[44] UIT. Y.4113*, Requisitos de red para la Internet de las cosas*. Recuperado el 14 de noviembre de 2021, de: *https://www.itu.int/rec/T-REC-Y.2060-201206-I/es*.
[45] UIT. Y.4203, *Requirements of things description in the Internet of things.* Recuperado el 14 de noviembre de 2021, de: *https://www.itu.int/rec/T-REC-Y.2060-201206-I/es*
[46] UIT. Y.4475*, Lightweight intelligent software framework for Internet of things devices.* Recuperado el 14 de noviembre de 2021, de: *https://www.itu.int/rec/T-REC-Y.2060-201206-I/es.*

Esto deja ver un número considerable de recomendaciones emitidas por la UIT para la regulación de los diferentes aspectos que involucran al Internet de las cosas.

Sin embargo, no es el único organismo en el mundo que ha emitido lineamientos en esta materia. En el año 2018, la Organización Internacional de Normalización, en conjunto con la Comisión Electrotécnica Internacional, desarrollaron el primer estándar internacional sobre *IoT*, que proporciona una arquitectura de referencia del Internet de las cosas.

La ISO/IEC 30141, Internet de las Cosas (*IoT*) Arquitectura de Referencia, es una ISO que se encarga de establecer una estructura común para los diseñadores y desarrolladores de las aplicaciones de *IoT.* Mantiene la seguridad y protección de los datos, además de afrontar interrupciones por ciberataques o desastres naturales.

Como se puede observar, desde la publicación del estudio realizado por la ITU en materia del Internet de las cosas en 2005, los aparatos electrónicos conectados a Internet se volvieron parte de los asuntos de las agendas y estrategias de los Estados debido al incremento en el uso de esta tecnología.

No obstante, eso no quiere decir que existan disposiciones normativas internacionales con coercitividad que regulen el Internet de las cosas.

A la fecha, se conoce una regulación que de forma directa regula los diferentes aspectos del *IoT* y es de carácter local. Fue emitida en el estado de California de los Estados Unidos de América, uno de los países con mayor uso de dispositivos que se conectan a Internet.

De este modo, fue aprobada por el Estado de California la Ley No. 327 en el año de 2018, pero iniciaría su vigencia hasta el 1° de enero del año 2020, por lo que lleva en funciones cerca de dos años.

Esta ley tiene por origen la propuesta presentada por la Senadora Santa Bárbara Hannah-Beth el 3 de febrero de 2017 ante el Senado del Estado de California, y llevaba por nombre SB-327 *Information privacy: connected devices.*

Dicha propuesta fue subsanada con posterioridad por la Senadora antes mencionada. El 29 de septiembre del mismo año se agregó a la Sección 1, Parte 4 de la División 3 del Código Civil californiano, bajo la designación: *Title 1.81.26. Security of Connected Devices.*[47]

Sin embargo, de acuerdo con la legislación del estado de California, era necesario que el Proyecto de Ley de la Asamblea n°1906 intitulado AB-1906 *Information privacy connected devices*, presentada el mismo año por el legislador Jacqui Irwin, tuviera que ser aprobado primero. Esto se debe a que el proyecto SB-327 contenía aspectos que necesitaban ser aprobados con anterioridad para que esta propuesta tuviera el efecto legal y social que se tenía planeado, por lo que ambas fueron promulgadas el 28 de septiembre de 2018 por el gobernador del estado de California.[48]

Al momento de ser promulgada se estableció una *vacatio legis* con la intención de otorgarle a los fabricantes de dispositivos del *IoT* tiempo para adecuar sus productos a la normatividad que se acababa de promulgar.

Asimismo, esta ley tiene la intención de ampliar el margen que se tenía de los objetos conectados a Internet; es decir; no sólo aplicaba para las PC, siendo el dispositivo, junto con el teléfono inteligente, de los aparatos más conocidos que se conectan a Internet; se tomaban en cuenta otros aparatos como el microondas, los refrigeradores, relojes o incluso focos.

Por consiguiente, la ley tiene como finalidad crear requisitos de seguridad para los objetos del *IoT* dotando a sus equipos de métodos de seguridad adecuados para otorgar la mejor protección a favor de los usuarios. Además, señala que la construcción de estos dispositivos requiere que tengan indicadores visuales, auditivos u otros para mostrar el momento en que recolectan la información de los usuarios y así se logre obtener su consentimiento cuando la recopilación se extienda más de lo que se necesita.

---

[47] Porcelli, Adriana Margarita, *Un hito jurídico sobre Internet de las Cosas: la Ley de California n° 327 del año 2018 vigente a partir del 1 enero del 2020*, 2020. Recuperado el 20 de noviembre de 2021, de: *https://www.scielo.br/j/rdgv/a/NBksbsTGzh38X5NDLsWNntq/?lang=es.*
[48] *Idem.*

Lo que se busca al emitir esta ley, es que se vea reflejada la toma de decisiones de los usuarios. El consumidor se vuelve más consciente de sus elecciones al aceptar o rechazar que la compañía que les solicita la información privada pueda recabarla.

2.3.1 Regulación jurídica del Internet de las cosas en el derecho mexicano

Tal y como se abordó en el tema anterior, la regulación del *IoT* es un tema de suma importancia para el mundo actual debido al incremento en el uso de objetos que se conectan a Internet.

De acuerdo con los datos recabados en México por el Instituto Nacional de Estadística y Geografía (INEGI), mediante la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información (ENDUTIH) 2020, se revela que un televisor con acceso a Internet representa un 22.2% de los medios preferidos de los usuarios para conectarse. Se encuentra superado tan solo por la computadora portátil y los celulares inteligentes con 33.7% y 96%, respectivamente.[49]

Esto implica que un televisor inteligente forme parte del grupo de los dispositivos favoritos de las personas para conectarse, siendo las pantallas *Smart Tv* uno de los dispositivos pertenecientes al Internet de las cosas. Lo anterior muestra que se están dando pasos agigantados para que el uso de estos dispositivos forme parte de la vida cotidiana de los usuarios.

A la fecha, en México no existe regulación alguna que detalle lo que se debe entender por el Internet de las cosas. No existe la regulación general que deben tener estos dispositivos conectados a Internet, ya sea al momento del ensamblado o en las características del *software* donde se puede tener acceso a la información personal de quienes los usan.

[49] Instituto Nacional de Estadística y Geografía (INEGI), *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares ENDUTIH (2021),* Comunicado de Prensa núm. 350/22, 4 de julio, 2022, pp. 1-19. Recuperado el 24 de noviembre de 2021, de: *inegi.org.mx.*

Sin embargo, aunque pareciera que no existe un marco normativo que regule a los objetos del *IoT*, se ha utilizado la normatividad periférica a fin de no dejar de forma libre su fabricación y comercialización a los fabricantes y productores de los *softwares*. Se realiza mediante disposiciones normativas de carácter técnico y leyes que regulen la protección de datos personales o las telecomunicaciones de forma general.

Desde la reforma en materia de Telecomunicaciones llevada a cabo en 2013, hasta la fecha, se han tratado de regular los objetos del *IoT* abordando primero la definición o concepto de lo que se debe entender por el Internet de las cosas. Además, se han añadido las cuestiones sobre las que se debe poner atención al momento de considerar a un objeto dentro de las diversas categorías que existen.

A la fecha, existe únicamente un proyecto de norma mexicana[50] que aborda el *IoT*. Tiene la intención de regular el Internet de las cosas en México; sin embargo, no incluye aspectos relevantes o novedosos para su regulación debido a que es una réplica de la recomendación ITU-T Y.2060, en la cual se establece lo que se debe entender por el Internet de las cosas, así como los conocimientos básicos sobre el área.

La incorporación de este tema para su regulación al sistema jurídico como norma mexicana no tendría los alcances que se necesitan puesto que su consentido no es de regulación sino de la descripción. Las características de esta norma son de carácter voluntario y la única forma de comprobar su efectiva aplicación es mediante la certificación de organismos de normalización.

Su principal función es la de establecer los requisitos mínimos de calidad de los productos y servicios con la intención de proteger a los consumidores. Así, se constituye una referencia para determinar la calidad de los productos y servicios de los que se trate, de conformidad con el artículo 54 de la Ley Federal sobre Metrología y Normalización, misma que a la fecha se encuentra abrogada.

[50] El proyecto lleva por denominación PROY-NMX-I-320-NYCE-2018. Publicado el día 20 de junio de 2019. Recuperado el 27 de noviembre de 2021, de: https://www.dof.gob.mx/nota_detalle_popup.php?codigo=5566036

Es por eso que actualmente no existe una regulación del Internet de las cosas. Podrán existir guías sobre el tema que permitan abarcar de forma específica lo que implica la conexión de objetos a Internet, los datos que recaba y la seguridad que se debe mantener para no poner en peligro al usuario; no obstante, aún se carece de una norma sobre este tema.

2.4 Relación del Internet de las cosas con la ciberseguridad

Para establecer cuál de todos los asuntos de ciberseguridad involucran al *IoT* de forma directa, se tiene que establecer la conceptualización y/o definición de dicho término.

El IFT define a la ciberseguridad como el "conjunto de herramientas, políticas, conceptos, acciones, prácticas idóneas y tecnologías que pueden utilizarse para proteger a los usuarios, sus dispositivos y la información transmitida y/o almacenada, de los riesgos de seguridad que hay en el ciber entorno".[51]

Mientras que Cisco, de forma más concisa y de fácil entendimiento, considera que la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales.[52]

En el ámbito internacional, la ciberseguridad es un tema fundamental para el desarrollo de las personas en el mundo digital debido al incremento en el uso de las tecnologías digitales y a los riesgos que implica su uso.

Es por eso que la Unión Internacional de Telecomunicaciones (UIT), en el año de 2018, publicó la *Guía para desarrollar una estrategia nacional de ciberseguridad*, en la que se establecen "los principios a tener en cuenta al momento de elaborar las estrategias de ciberseguridad, así como la aplicación de mecanismos que permiten prevenir, combatir y mitigar las acciones dirigidas contra

[51] IFT, *Página principal de Usuarios*. Recuperado el 1 de diciembre de 2021, de: *http://www.ift.org.mx/usuarios-y-audiencias/ciberseguridad-0*
[52] CISCO, *¿Qué es la ciberseguridad?* Recuperado el 1 de diciembre de 2021, de: *https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html*

la confidencialidad, la integridad y la disponibilidad de los sistemas e infraestructuras de TIC, así como las amenazas contra los datos informáticos".[53]

En México existen varias instituciones públicas involucradas en el ámbito de la ciberseguridad: la CONDUSEF, en el caso de ciberseguridad en temas financieros, la Guardia Nacional, la Comisión Intersectorial para el desarrollo del Gobierno Electrónico (CIDGE), el IFT, entre otras.

Asimismo, en el año de 2018 se expidió el Plan de Acciones en Materia de Ciberseguridad a cargo de la Unidad de Política Regulatoria, la Coordinación General de Política del Usuario, la Unidad de Asuntos Jurídicos y la Unidad de Administración, unidades adscritas al IFT.

En este documento se establecen los principios básicos y las bases fundamentales de la Estrategia Nacional de Ciberseguridad, así como las acciones llevadas a cabo por el instituto antes mencionado.

2.4.1 Seguridad

En términos generales, la seguridad es la cualidad de estar seguro, que a su vez se traduce en la ausencia de riesgo. Por lo tanto, la seguridad aplicada al ámbito digital se encarga de proteger la información que contiene determinada infraestructura digital frente a posibles riesgos.

En consecuencia, es una prioridad garantizar la seguridad de los dispositivos o de los servicios conectados a una red de Internet teniendo en cuenta que pueden recibir ataques cibernéticos y poner en riesgo los datos personales de los usuarios. Esto sin ser necesario que un usuario conecte el dispositivo a una red de Internet o a un mismo dispositivo que tenga esa capacidad de forma intencionada, debido a que se pueden conectar de forma automática a otros dispositivos provocando un riesgo a la seguridad de los mismos.

[53] Instituto Federal de Telecomunicaciones*, Segundo informe de privacidad de la información de los usuarios en el uso de servicios digitales*, 2021. Recuperado el 1 de febrero de 2022, de: *ww.ift.org.mx/usuarios-y-audiencias/segundo-informe-de-privacidad-de-la-informacion-de-los-usuarios-en-el-uso-de-servicios-digitales.*

Lo anterior requiere una colaboración entre todas las partes que participen en el uso, distribución y regulación de los servicios y dispositivos del *IoT*.[54]

Respecto a ello, existen diversos aspectos de seguridad en el ámbito digital que involucran al Internet de las cosas. Son de suma importancia para el libre y seguro desarrollo de las personas mientras hacen uso de estas tecnologías.

Para mantener la seguridad en cualquier sistema, se necesita mantener en sintonía a las personas, los procesos y la tecnología usada.

a) La tecnología con la que se cuenta es fundamental para proporcionar las herramientas necesarias a fin de prevenir o protegerse de ataques tecnológicos. Tener actualizadas estas herramientas asisten tanto a los procesos como a los usuarios.

b) Las estructuras establecidas en las organizaciones, tanto públicas como privadas, proporcionan planes de acción tanto para la protección como para la resolución de cualquier ataque cibernético.

c) Debido a que las personas deben entender y llevar a cabo los procesos de forma correcta, son el eslabón débil en esta cadena de seguridad. Las deficiencias en la actualización de la seguridad en el medio digital provocan que no se conozcan ni los riesgos ni las medidas a realizar para prevenir un posible ataque.

2.4.2 Seguridad de la información

La seguridad de la información involucra tanto el almacenamiento como el tránsito de información entre los usuarios y los recolectores de información.

Asimismo, la protección de los datos es un tema que debe tratarse con mucha cautela puesto que para que sean protegidos los datos es necesaria una mayor regulación, y por ende una mayor injerencia de las entidades que regulen el debido cuidado de los datos que se comparten de forma digital.

---

[54] Rose, Karen*, La Internet de las Cosas—Una breve reseña. Problemas y desafíos de un mundo más conectado,* Suiza, Internet Society, 2015, p.68. Recuperado el 12 de diciembre de 2021, de: *https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf.*

De esta forma, se causa un giro en el manejo de los datos de las personas a partir de actualizar las formas en las que se recaban y se mantienen a salvo de los posibles riesgos que puede haber al utilizar dispositivos del *IoT*. Esto garantiza la confianza que deben tener los usuarios de estos servicios y/o dispositivos para usarlos de forma segura.

Para ello, es necesario comenzar a diferenciar entre lo que se considera un dato y lo que se puede determinar cómo información. El dato es aquella materia prima que se puede llegar a transformar en información y, por otro lado, la información es el conjunto de datos que tienen un significado específico dentro de un contexto determinado.

Es decir, para que los procesos de la seguridad de la información se lleven de forma concreta, es necesario que se analice el contexto y las características de las organizaciones que quieran proteger la información. Es decir, no es lo mismo proteger la información recopilada por las empresas fabricantes o aquellas que comercialicen los productos del *IoT,* o aquellas que utilicen los productos para recopilar los datos como lo pueden ser las instituciones gubernamentales.

De acuerdo con la Organización Internacional de Estándares (ISO por sus siglas en inglés), la seguridad de la información implica la "preservación de la confidencialidad, integridad y disponibilidad de la información".[55]

De este modo, existen diferentes elementos de la seguridad de la información que se deben considerar como fundamentales para salvaguardar los datos de algún peligro externo.

Por consiguiente, la disponibilidad de la información es de suma importancia puesto que el fácil acceso a ésta proyecta un buen funcionamiento de las bases de datos y de sus estructuras informáticas. Sin embargo, esto debe coexistir con la

[55] International Organization for Standardization, *Information technology, Security techniques-information security management systems-Overview and vocabulary,* 2014. Recuperado el 15 de diciembre de 2021, de: *https://standards,iso.org/ittf/PubliclyAvailableStandard.*

inaccesibilidad[56] de la información para quien no tiene permitido consultarla u obtenerla.

Para ejemplificar un extremo de la no disponibilidad de la información, se puede poner como ejemplo aquello que señala Richard Stillman en su artículo *¿Puede confiar en su ordenador?*[57], en el cual se habla de la viabilidad de la disposición de la información al ser controlada por el creador del *software* de un equipo de cómputo, y cómo se podría poner en riesgo la información a la que tenemos acceso; es decir, se puede alterar dependiendo de quién lo quiera y los fines que persiga.

Otro de los puntos involucra la confidencialidad, la cual está ligada al punto anterior pues solamente deber ser conocida por la o las personas autorizadas para ellos y éstas a su vez deben ser reservados con ella.

Para mantener la confidencialidad de la información, se deben tener los mecanismos necesarios para mantener el acceso a esos datos, éstos son: la autenticación, autorización y el registro.

- Autenticación

De acuerdo con la Comisión Interamericana de Telecomunicaciones de la Organización de los Estados Americanos, la autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación y autenticación, que en su conjunto verifican los derechos de acceso del usuario.[58]

---

[56] Universidad Internacional de Valencia, *La seguridad de la información en la era digital*, 2021. Recuperado el 20 de diciembre de 2021, de: *https://www.universidadviu.com/es/actualidad/nuestros-expertos/la-seguridad-de-la-informacion-en-la-era-digital.*

[57] Stallman, R., *¿Puede confiar en su ordenador?*, Free Software Foundation, 2017. Recuperado el 20 de enero de 2022, de: *https://www.gnu.org/philosophy/can-you-trust.es.html.*

[58] Comisión Interamericana de Telecomunicaciones de la OEA, *Autenticación de usuarios*, *Boletín electrónico* no. 24, junio, 2006. Recuperado el 20 de enero de 2022, de: *http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp.*

La autenticación sirve para verificar la identidad del usuario y garantizar la seguridad de la información, haciendo uso de más medidas de seguridad que las contraseñas dadas de forma personalizada.

Es por eso que lo ideal es combinar dos o más métodos de identificación; de esa forma se hace uso de la autenticación múltiple, siendo ésta un método más seguro. Podría ser con el uso de una tarjeta física y de un PIN (*Personal Identification Number*), o incluso incluir un método más para hacer más fuertes los sistemas de autenticación.

- Autorización

Consiste en el proceso por medio del cual la red de datos autoriza al usuario identificado acceder a determinados recursos de la misma. [59]

- Registro

Es el proceso mediante el cual la red registra todos y cada uno de los accesos a los recursos que realiza el usuario, autorizado o no.[60]

Como cualquier activo, es de suma importancia para diferentes entes. No obstante, en este caso, el activo de la información puede llegar a presentar diversas debilidades, lo que provoca que sea susceptible a ataques. De acuerdo con Alan Calder, estas debilidades son conocidas como vulnerabilidades, las cuales se pueden definir como las debilidades de un activo o grupo de activos que pueden ser explotados por una amenaza.[61]

Estas vulnerabilidades que presentan los activos provocan la aparición de diversos tipos de amenazas. Para ISO, la amenaza es “la causa potencial de un incidente no deseado, el cual puede tener como resultado el daño a un sistema u organización”[62], por lo que es necesario establecer un protocolo de seguridad de la

[59] *Idem.*
[60] *Idem.*
[61] Calder, A. y Watkins, S., *ISO27000 and Information Security: A Combined Glossary. United Kingdom: IT Governance Publishing*, 2010.
[62] International Organization for Standardization, *Information Technology-Security techniques-information security management systems-Overview and vocabulary*, 2014. Recuperado el 19 de diciembre de 2021, de: *https://standards,iso.org/ittf/PubliclyAvailableStandard*

información en el que no sólo se incluyan los medios de contención, sino de prevención ante posibles eventualidades.

A su vez, la materialización de una amenaza es definida como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una alta probabilidad de comprometer las opresiones del negocio y amenazan la seguridad de la información”.[63]

Este tipo de incidentes, como se explicó anteriormente, pueden llegar a causar daños en los activos (la información a proteger) y un impacto negativo en las empresas que cuidan o protegen estos datos.

Es importante señalar que, debido a las posibles amenazas o materialización de las mismas en contra de los datos que se protegen, es un hecho que ningún entorno que almacene dichos datos sea considerado 100% seguro. Por ello, para minimizar el riesgo y conocer de antemano la inversión que se debe hacer para proteger dicho activo es necesario identificar, evaluar y gestionar los riesgos de forma tal que se encuentren en un nivel aceptable.

Por ello, es necesario observar a la seguridad de la información como un proceso de gestión de riesgos aplicando las siguientes estrategias:

- Evitar el riesgo.
- Aceptar el riesgo.
- Transferencia del riesgo a uno o más entes.
- Compartir el riesgo con una o más entidades.
- Aplicación de controles.

Sin embargo, derivado de esto, se plantean diversas preguntas: ¿la implementación de los procesos para proteger la información es un gasto o una inversión?; ¿qué se protege?; ¿de quién se debe proteger? y ¿cuántos recursos se deben invertir?

[63] *Idem.*

Respecto a las organizaciones que se dedican a la recolección de datos derivado de los objetos del *IoT* o de empresas que facilitan el almacenamiento de estos datos, es necesario que tomen en cuenta las preguntas anteriormente planteadas en razón de que, como se mencionará en un capítulo posterior, existen diferentes normas técnicas de carácter no vinculatorio que pueden establecer los parámetros para el cuidado de la información; algunas de ellas están enfocadas a empresas de cierto perfil.

Para resolver esas dudas, es preciso que se empiece por definir el proyecto que debe de seguir cada empresa u organización. De esta forma, se podrá conocer el alcance de la pregunta antes planteada.

De las diferentes definiciones de lo que se considera como proyecto, puede sintetizarse como todo esfuerzo limitado a un tiempo determinado que pretende obtener resultados únicos. La delimitación de lo que implica un proyecto concibe la idea de que, para poder alcanzar esos resultados, es necesario que se inviertan ciertos costos; esto se va a definir dependiendo del proyecto que se realiza, debido a que de ellos depende si los beneficios son altos o no. Por consiguiente, para obtener beneficios los costos deben ser inferiores a lo que se pretende obtener.

Los costos no sólo implican un valor monetario, sino una sustracción de recursos tanto humanos y de tiempo como el valor económico. Es decir, se invierte en personal capacitado y en tiempo para la elaboración de dichos proyectos a fin de la implementación de los mismos; asimismo, se atiende la constante actualización del personal y de los sistemas de gestión de la información que se han utilizado.

Para que en cada proyecto la gestión de la información funcione de forma correcta, es importante que se lleve a cabo un proceso de evaluación de dicho instrumento, analizando las distintas variables que implican las posibles eventualidades y terminando con un dictamen sobre la conveniencia de implementarlo. Para dicha evaluación se consideran, entre otras cosas:

- Objetivos.
- Economización del costo, tiempo y maximización de la seguridad.

- Opciones para alcanzar los objetivos y solucionar los problemas.
- Riesgos asociados.

Es por eso que las empresas que se enfocan en la recolección de datos derivada de los objetos del Internet de las cosas o aquellas que ofrecen la infraestructura para almacenar dichos datos, como el uso de la nube, tienen que establecer las medidas de seguridad para que dicha información no se trasgreda. De ser así, esto implicaría trasgresiones a diversos derechos, así como la violación a diferentes obligaciones derivadas de la ley en materia de protección de datos que se tratará en secciones posteriores al presente trabajo.

- Normas internacionales en materia de seguridad de la información

Para regular la protección de datos a nivel particular, es necesaria la implementación de protocolos para cada tipo de organización de acuerdo a las necesidades de cada una; es decir, en la personalización de los protocolos o estrategias a seguir existen normas internacionales que pueden ser aplicadas por las organizaciones para proteger los datos.

Es de suma importancia señalar que este tipo de normatividad no contiene alguna coercitividad en el derecho mexicano. Sin embargo, en el ámbito privado ofrece una guía técnica sobre los protocolos a seguir para mantener un estándar específico y cuidar la información de las empresas que almacenen información, ya sea de ellos mismos o recopilada a terceros ajenos a la organización, así como contener las amenazas de seguridad de la información.

Esto en el caso de las empresas que almacenan datos obtenidos de terceros para el procesamiento de los mismos, como lo son los entes que participan en la recolección de datos por medio de los objetos del *IoT* para la personalización de los mismos o con fines de producción (recolección de datos para optimizar sus productos futuros a través de la recopilación de datos de los usuarios de este tipo de productos).

Existen dos organismos que por su relevancia e impacto a nivel internacional hacen que las propuestas técnicas en materia de seguridad de la información

tengan una enorme difusión y, por lo tanto, sean consideradas por una enorme cantidad de organizaciones, en su mayoría privadas.

Estas dos organizaciones son el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica (NIST, por sus siglas en inglés) y la Organización Internacional de Estándares (ISO, por sus siglas en inglés).

La primera de ellas fue fundada en 1901[64] con la finalidad de promover la innovación en ciencia y tecnología en los Estados Unidos de Norteamérica. Se caracteriza por la publicación de diversos documentos de estandarización en diferentes materias relacionadas con la ciencia y tecnología.

Tienen el objetivo de promover la innovación y la competitividad industrial en los Estados Unidos de Norteamérica para mejorar la seguridad económica y la calidad de vida de las personas, esto desde el punto de vista de la estandarización de la tecnología y sus procesos.

Sus principales áreas son:[65]

- Comunicaciones avanzadas, redes y sistemas de datos científicos (advanced communications, networks and scientific data systems).
- Fabricación avanzada y mediciones de materiales (advanced manufacturing and material measurements).
- Ciberseguridad y privacidad (cybersecurity and privacy).
- Medición fundamental, ciencia cuántica y difusión de la medición (fundamental measurement, quantum science and measurement dissemination).
- Medición de sistemas biológicos y de salud (health and biological systems measurement).
- Infraestructura física y resiliencia (physical infrastructure and resilience).

En lo que se refiere a ISO, este organismo se fundó en el año de 1946 debido a la reunión de varios delegados de 25 países en el *Institution of Civiles Engineer*

[64] NIST, *About us*. Recuperado el 1 de enero de 2022, de: *https://www.nist.gov/about-nist.*
[65] *Idem.*

de Londres; sin embargo, de forma oficial su origen data un año después, pero ya con 67 comités técnicos enfocados en materias específicas.[66]

Su enfoque es la creación de normas internacionales mediante la captación de diversos científicos y expertos en la materia que se desea desarrollar, con la finalidad de volver más general y adaptable a cualquier contexto la norma que desean estandarizar.

De esta forma, sus normas tienen el enfoque de un Sistema de Gestión de Seguridad de la Información (SGSI); es decir, intentan establecer las bases para la gestión ordenada de los riesgos a fin de lograr un nivel aceptable.

Dicho sistema es definido como "la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información".[67]

Con este último término se confirma la intención de llevar a cabo su finalidad: establecer un marco general que sirva de referencia para cualquier organización, en lugar de ser una metodología de aplicación inmediata.

La ISO 27000 y la ISO 27001 son ejemplos claros del proceso de implementación de un SGSI, estableciendo cuatro puntos para su establecimiento en cualquier organización, los cuales son:[68]

a) Definir el alcance del SGSI en términos de las características del negocio (organización, localización, activos y tecnología).

b) Definir una política para el SGSI aprobada por la dirección.

c) Definir un enfoque para la evaluación (*assesment*) del riesgo de la organización.

- Identificar una metodología de valoración del riesgo.

---

[66] ISO, *The ISO story*. Recuperado el 5 de diciembre de 2021, de: *https://www.iso.org/about-us.html.*
[67] International Organization for Standardization, *ISO/IEC, Information Technology-Security Techniques-Information security management systems-Overview and vocabulary*,15 de enero de 2014. Recuperado el 19 de diciembre de 2021, de: *https://standards.iso.org/ittf/PublidyVavailableStandards/c063411_ISO_IEC_27000_2014.zip.*
[68]Anáhuac Online, *Diplomado en ciberseguridad*. Recuperado el 1 de junio de 2022, de: *https://uvanahuac.instructure.com/courses/4449/pages/3-sg-si-optica-iso-27000?module_item_id=339275*

- Determinar criterios y niveles de aceptación del riesgo.

d) Identificar los riesgos.

- Identificar activos y propietarios de los mismos.
- Identificar las amenazas.
- Identificar las vulnerabilidades.
- Identificar los impactos.

e) Identificar y evaluar los riesgos.

- Valorar el impacto en caso de fallas de seguridad.
- Valorar la probabilidad de ocurrencia de fallas en la seguridad.
- Estimar los niveles de riesgo.
- Determinar cuando los riesgos son aceptables o requieren tratamiento de acuerdo a los criterios establecidos.

f) Identificar y evaluar opciones de tratamiento de riesgos.

g) Seleccionar objetivos de control y controles para el tratamiento de riesgos.

h) Obtener la aprobación de la dirección sobre el riesgo residual.

i) Obtener la aprobación de la dirección para implementar y operar el SGSI.

j) Preparar la declaración de aplicabilidad.

Esto da como resultado una política de seguridad institucional que a su vez genera una política de uso aceptable, siendo un informe por medio del cual a los empleados se les da a conocer lo que pueden o no hacer con los activos de la empresa; es necesaria la aceptación expresa para su implementación.

De esta manera, la aplicación de este tipo de estandarizaciones ayuda a facilitar el flujo y control de la información puesto que existe un documento en el que queda plasmada la intención de la empresa para el tratamiento de datos.

Dentro de este tipo de criterios a seguir es necesario identificar un tipo de infraestructura, la crítica, en la cual se encuentra todo activo, (incluida la

información) que describe los sistemas y activos cibernéticos y físicos que son indispensables para una organización. La destrucción o no disponibilidad de ella provocaría que el sistema de seguridad fallase o se debilitara.

Es indispensable tener en cuenta los activos críticos y los activos que no son esenciales. Como se mencionó, ningún sistema o protocolo de seguridad es 100% seguro, lo que se traduce en que no todos los activos de una organización (en especial aquellos que recolectan u almacenan datos a través de los objetos del *IoT*) son protegibles debido a que carecen de los recursos para lograrlo.

Como se mencionará en párrafos subsecuentes del presente trabajo, los protocolos de seguridad en cuestión de datos personales en los dispositivos del *IoT* o recolectados por estos, no están definidos y se han tenido que seguir protocolos generales sobre el almacenamiento de datos sin llegar a un consenso sobre lo que se debe tener para regularlos.

Por consiguiente, es notable la complejidad de establecer una regulación para este tipo de objetos tomando en cuenta el uso transfronterizo del Internet. La dificultad radica en que la puesta en marcha de algún tipo de regulación técnica con implicaciones jurídicas podría fomentar el desarrollo de versiones técnicas de los diversos procesos para el cuidado de la información, recolectada por este tipo de objetos, causando innovaciones o modificaciones a lo planteado por una autoridad.

2.4.3 Regulación de la Protección de Datos

La protección de datos personales es de suma importancia. Los objetos del Internet de las cosas, mediante el uso de aplicaciones, recolectan los datos de los usuarios, mismos que se rigen por la normatividad en materia de protección de datos.

En el ámbito internacional, la Organización de las Naciones Unidas (ONU) ha establecido directrices para regular los archivos de datos personales informatizados. Uno de ellos es el principio de legalidad y de lealtad, el cual establece que “la información relativa a las personas no debe ser recogida o

procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas".[69]

Un ejemplo de la importancia y el análisis que amerita el tratamiento de los datos personales en el ámbito internacional, son las Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos personales, emitidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 2013. Se aborda el flujo de datos e información y el intercambio científico y tecnológico.

Otro de los documentos en materia Internacional, del cual México es parte, es el expedido por la Red Iberoamericana de Protección de Datos, definiendo principios y algunos derechos en materia de protección de datos en la región Iberoamericana.

Otro de los mecanismos internacionales que han servido para establecer los principios de privacidad de la información es el Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico, del cual forma parte México. Se establecen las medidas para garantizar la seguridad y confidencialidad de los mensajes, o para proteger la privacidad de los datos personales de los usuarios finales.

Existen tratados y convenios internacionales en materia de protección de datos personales, como lo es la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948 (artículo 12), la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) de 1966 (artículo 11) y el Pacto Internacional de Derechos Civiles y Políticos del 19 de diciembre de 1966 (artículo 17).[70]

En el ámbito nacional, la Constitución Política de los Estados Unidos Mexicanos establece en el artículo 6° el acceso a la información y las formas en que

---

[69] Organización de las Naciones Unidas (ONU). *Directrices para la regulación de los archivos de datos personales informatizados*, Adoptadas mediante resolución 45/95 de la Asamblea General, 14 de diciembre de 1990. Recuperado el 2 de febrero de 2022, de: *D.3BIS_ Directrices de Protección de Datos de la ONU.doc (udg.mx).*

[70] Mendoza Enríquez, Olivia Andrea, *Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento*, *Rev. IUS,* Puebla, vol.XII, núm.41, ene./jun. 2018, pp.267-291.

se debe garantizar este derecho. En el apartado A, fracción II, se regula la información que se refiere a la vida privada y los datos personales.

En el artículo 16 párrafo segundo de la de la CPEUM, se regula el acceso, rectificación y cancelación de los datos de una persona, así como las excepciones al tratamiento de datos personales por cuestiones de seguridad nacional, cuestiones de orden público o proteger los derechos de terceros.

También se establece a grandes rasgos la regulación de las comunicaciones privadas en materia penal, siendo éstas inviolables, protegidas por la ley sancionando cualquier acto que vaya en contra de éstas, salvo que sean aportadas de forma voluntaria.

Otro de los instrumentos que regulan la protección de datos es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en la que se establecen los principios y el procedimiento para garantizar la protección de los datos privados de una persona cuando son recolectados por instituciones públicas. En dicha ley se encuentra un capítulo sobre la obtención y tratamiento de datos personales en posesión de instancias de seguridad, procuración y administración de justicia.

La ley que regula la protección de datos recabados por las entidades que no son públicas es la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

En estas disposiciones normativas, se establece que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), es el organismo encargado de garantizar la protección de derecho a la protección de datos personales.

Otro de los organismos involucrados en el cuidado de los datos personales es el IFT, promoviendo, informando y regulando la protección de datos cuando tienen que ver con las telecomunicaciones; de acuerdo con el artículo 6°, apartado B de la CPEUM.

La LFTyR también regula las cuestiones de privacidad, pero enfocado a los proveedores de servicios de Internet. En el artículo 145 de esta ley, se establece

que los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que expida el IFT.[71]

2.4.4 Recopilación de datos personales por parte de las empresas fabricantes de los objetos conectados a una red de Internet

Para la recopilación de los datos personales por parte de los objetos que se conectan a Internet, se necesita hacer uso de diversas aplicaciones que son el enlace entre el usuario y la empresa que va a almacenar los datos.

Es por eso que las aplicaciones usan los avisos de privacidad para hacerle notar al usuario los datos que quieren recabar; se le pregunta al usuario si acepta que se le recaben ciertos datos al momento de usar el dispositivo.

Los avisos de privacidad pueden mostrarse al principio o proporcionar al usuario el *link* para consultarlo. Al hacer uso de los medios digitales, estos avisos de privacidad son proporcionados en su mayoría de forma simplificada para que el usuario pueda saber los datos mínimos de quién es el que va a obtener sus datos.

Para mantener un correcto control de los datos que se proporcionan, es importante consultar los datos proporcionados y la forma en que se puede revertir el consentimiento o el procedimiento que tienen las empresas en caso de transgresiones a la privacidad.

Existen diferentes tipos de datos que se pueden recopilar, siendo los más relevantes los siguientes:

- Los datos para registrarse:

Son aquellos que se les solicitan a los usuarios para crear una cuenta y activar el dispositivo a fin de que pueda conectarse a Internet. Son necesarios para que el dispositivo pueda identificar al usuario y personalice las acciones que realiza de acuerdo a la persona que ingresa.

---

[71] Unidad de Política Regulatoria, *Plan de Acciones en Materia de Ciberseguridad del IFT*, 2018. Recuperado el 12 de enero de 2022, de:*http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesciberseguridad.pdf*

- Los datos de actividades:

Son aquellos que logran identificar el dispositivo por medio del cual se trata de acceder y conectarse a Internet; también identifica las actividades que se realizan mientras se usa este objeto. Esto ayuda a mejorar la experiencia de los usuarios porque utilizan los datos que recaban día con día.

- Datos no declarados:

Son aquellos que no son consentidos. Los dispositivos los recopilan al hacer uso de ordenes precargadas; es decir, con el uso de palabras clave o con la activación mediante movimientos físicos de forma involuntaria se recopilan estos datos.

Asimismo, las empresas han decidido aprovechar los datos geoespaciales que les proporcionan objetos como cámaras, sensores, monitores y celulares inteligentes. El objetivo consiste en mejorar dichos dispositivos en cuanto a sus funciones o incluso aplicar los datos en otros dispositivos para que puedan desarrollarse de forma completa, como sensores o controles para utilizarlos en la industria, la agricultura o el medio ambiente.

Respecto a ello, existen diversos fabricantes de procesadores de datos que facilitan esta interpretación de la información, como lo son *Media Tek*, *Qualcomm*, entre otros; sin embargo, *Arduino* es uno de los más usados por las personas para que este tipo de dispositivos estén al alcance de todos.

También se usan los datos para conocer la información en tiempo real, ya sea que se requieran para solucionar algún problema o para mostrarle al usuario de estos dispositivos aquellos datos que requieran saberse al momento.

Esta información puede ser el ritmo cardiaco, la presión arterial y demás datos médicos que son recolectados por relojes inteligentes, pulseras u otro dispositivo que recabe la información y la transfiera a otro como lo puede ser un *Smartphone* o a un servidor como la nube.

No obstante, la recolección de datos no sólo implica tener la tecnología necesaria para recopilarla como *Arduino*, las conexiones Wi-Fi, los *softwares*, la red

móvil, etcétera, sino que se debe tener una estructura automatizada por parte de la empresa para aprovechar los datos proporcionados por usuarios de estos dispositivos.

CAPÍTULO 3. FUNCIONAMIENTO Y TENDENCIAS DE LOS OBJETOS CONECTADOS A INTERNET

3.1 Conexión de los objetos a Internet

Para que un objeto pueda conectarse a Internet se necesita más que el *software* del mismo dispositivo; es importante contar con cierta infraestructura externa de la empresa que fabricó el producto.

Se deben tener las capacidades técnicas y digitales para acceder a Internet y contar con algún proveedor que permita conectarse a ella, si es que es un dispositivo que necesita de otro para conectarse; el segundo objeto debe tener las mismas o características similares que permitan el enlace.

Es por eso que, dependiendo del objeto del que se trate, así van a ser las necesidades que requiera el dispositivo principal. Es decir, si el dispositivo que recopila datos es una pulsera, ésta en la mayoría de los casos no permite ver los datos a simple vista; en esa situación se necesita de otro objeto que también debe estar conectado a Internet para visualizar dichos datos. Lo anterior no pasa con un *Smartphone* o una *Smart Tv*.

Por consiguiente, existen diversas formas de conexiones entre dispositivos o dispositivos y medios de almacenamiento, como lo son*: Device-to Device, Device-to-Cloud, Device-to-Gateway, Back-End Data-Sharing*, entre otras.

Sin embargo, para que esto sea posible, necesitan uno de los elementos más importantes: las aplicaciones (*Apps*). El uso de éstas permite que los datos sean recopilados y concentrados en un solo lugar digital; funciona de enlace entre el dispositivo principal y el artefacto a conectarse, o para vincularse a Internet y obtener los beneficios de este enlace digital.

3.1.1 Modelos de Conectividad

A. Conectividad Ubicua.

Hace referencia a aquella tecnología que facilita las diversas actividades que se realizan; éstas pueden ir desde un reloj inteligente, un *Smartphone* hasta los simuladores de realidad virtual que tienen como objetivo realizar diversas actividades aun cuando no se esté en un lugar de forma presencial.

Este término fue determinado por Mark Weiser para un trabajo que realizó sobre ciencias de la tecnología de la información y comunicación, pero fue hasta 1991 cuando el término tuvo gran importancia a nivel mundial.

Para su entendimiento, este término puede dividirse en cuatro partes:

- La primera hace referencia al uso mecánico y casi invisible de los dispositivos, de forma tal que la interacción entre la persona y el dispositivo sea tan sencilla y directa que la comprensión se logra volver mutua sin tantas interferencias tecnológicas.
- La segunda señala que los usuarios disponen de capacidades asociadas al contexto en el que se encuentran, careciendo de sentido. [72]
- La tercera establece la distribución de manera uniforme de los servicios, lo cual se ve afectado por el desarrollo tecnológico que se dispone, así como la infraestructura existente.
- La cuarta hace referencia a la interacción de diversos dispositivos en el mismo espacio físico para cumplir con las necesidades de los individuos que se encuentren en dicho espacio. [73]

B. Dispositivo a dispositivo (*Device-to Device*)

Se realiza mediante la comunicación entre dos o más dispositivos que se conectan directamente entre sí y no a través de un servidor de aplicaciones intermediario.[74]

[72] Diagrama de la Computación Ubicua. Recuperado el 2 de febrero de 2022, de: *https://coggle.it/diagram/W-jBZyXDNGXMMD68/t/computaci%C3%B3n-ubicua*
[73] *Idem.*
[74] Rose, Karen, *op. cit.*

En el hogar, los objetos que utilizan este tipo de tecnología pueden ser focos, interruptores, termostatos y cerraduras. Regularmente usan protocolos de corta distancia debido a que transfieren pequeñas cantidades de información a una velocidad baja, los cuales pueden ser: *Bluetooth*, *ZigBee* y *Z-Wave*.

El *Bluetooth* es aquella tecnología que envía señales de voz y datos hasta una distancia de 10 metros; es ideal para la transferencia de datos de alta velocidad.[75]

El *ZigBee* sirve para un conjunto de protocolos de comunicación de alto nivel que se usan para crear redes de área personal con un radio digital pequeño de baja potencia.[76]

La *Z-Wave* es una red en malla que usa ondas de radio de baja potencia para la comunicación de dispositivo a dispositivo.[77]

La desventaja entre estos métodos de conexión es que muchos de ellos no son compatibles entre sí, limitando de esta forma la capacidad de elección entre los diferentes dispositivos.

De acuerdo a lo publicado por la *Internet Engineering Task Force*, en el IEFT *Journal*, los fabricantes deben comenzar a poner especial atención en implementar formatos de datos específicos de diferentes dispositivos antes que métodos abiertos que permitan el uso de formatos de datos estándares.[78]

C. Dispositivo a puerta de enlace (Device to Gateway)

Esto quiere decir que existe un *software* de aplicación corriendo en un dispositivo de puerta de enlace local. Actúa de intermediario entre el dispositivo y el servicio en la nube y provee seguridad y otras funcionalidades tales como traducción de protocolos o datos.[79]

---

[75] Azure, *Guía de protocolos y tecnologías de IoT*. Recuperado el 3 de febrero de 2022, de: *https://azure.microsoft.com/es-mx/overview/internet-of-things-iot/iot-technology-protocols/*
[76] *Idem.*
[77] *Idem.*
[78] Duffy Marsan, Carolyn, *IAB Releases Guidelines for Internet-of-Things Developers*, en IETF Journal, EUA, 11.1, Internet Engineering Task Force, 2015, pp. 6-8.
[79] Rose, Karen, *op.cit.*

Por lo regular, este tipo de tecnología es usada por dispositivos que recopilan datos sobre la actividad física de una persona, como los pasos o el ritmo cardiaco; es por eso que necesitan de una aplicación para conectarse y así usarla de enlace.

Otra forma de usar esta conexión es mediante los dispositivos *hub*, que se encuentran en los diferentes dispositivos automatizados para el hogar. Sirven de puerta de enlace local entre los dispositivos individuales del Internet de las cosas y un servicio en la nube.

Este tipo de conexión muestra su ventaja sobre las otras, tal y como lo menciona la IEFT, una organización internacional de normalización:

> Este modelo de comunicación se usa en situaciones donde los objetos pequeños deben interoperar con dispositivos que no utilizan el protocolo de Internet. A veces se adopta este enfoque para integrar dispositivos que solo soportan IPv6, lo que significa que se necesita una puerta de enlace para los dispositivos y servicios existentes que solo soportan IPv4.[80]

Sin embargo, este tipo de tecnología es costosa y se encuentra en pleno desarrollo para su innovación, por lo que su uso de forma común en los dispositivos, para ciudades inteligentes, en la industria, en el cuidado del medio ambiente, va a ser sumamente complicado.

D. Dispositivo a la nube (*Device-to-Cloud*)

Este modelo de conexión permite que el dispositivo se conecte directamente al servicio de la nube, utilizando las conexiones de Wi-Fi o mediante el cableado de *Ethernet,* y así vincularse a la red IP.[81]

Esta forma de conexión tiene como ventaja la disponibilidad, el respaldo de información, el intercambio de datos y por último la sincronización. Al respecto, la Oficina de Seguridad de Internauta del Instituto de Ciberseguridad de España (INCIBE), señala lo siguiente:

[80] Duffy Marsan, Carolyn, *op. cit.*
[81] Rose, Karen, *op. cit.*

- Disponibilidad. Podemos acceder a los archivos alojados en la nube desde cualquier dispositivo conectado a Internet que cuente con la capacidad para utilizar dicho servicio. Así evitamos el uso de dispositivos de almacenamiento físicos, como una memoria USB para compartir la información.
- Copia de seguridad. Podemos utilizar este espacio para guardar archivos a modo de copia de seguridad.
- Compartir. Otra función que nos ofrece y muy utilizada por los usuarios, es la posibilidad de compartir la información con otras personas. Podemos hacerlo de forma limitada con aquellas que escojamos e incluso hacerlo de forma pública para que cualquier usuario pueda acceder a los archivos compartidos.
- Sincronización. Algunos servicios permiten sincronizar automáticamente los datos entre distintos dispositivos. De esta forma un archivo que creemos o modifiquemos en un dispositivo se actualizará en todos aquellos que estén conectados al mismo servicio en la nube. [82]

Sin embargo, existen diferentes adversidades al momento de querer usar este tipo de conexión puesto que hay dispositivos que son de diferentes fabricantes, lo que causa problemas de interoperabilidad e ineficiencias en la conexión.

E. *Back-End Data-Sharing*

Esta clase de arquitectura de comunicación permite que los usuarios exporten y analicen datos de objetos inteligentes de un servicio en la nube en combinación con datos de otras fuentes.[83]

Permite agregar y analizar los datos recogidos de flujos obtenidos de un solo dispositivo de la *IoT*, logrando así un intercambio de datos y facilitando el acceso y

[82] Instituto Nacional de Ciberseguridad, *Tu información en la nube*. Recuperado el 5 de febrero de 2022, de: *https://www.osi.es/es/tu-informacion-en-la-nube.*
[83] Rose, Karen, *op.cit.*

análisis de los datos producidos por toda la gama de aparatos instalados en un inmueble.[84]

3.1.2 IPv4

La dirección IPv4 se desarrolló a principios de 1980, permitiendo alrededor de 4.3 millones de direcciones utilizando un formato de 32 bits, lo que para la época era suficiente. No obstante, este modelo se convirtió en el más usado por los diferentes proveedores de servicios de Internet para hacer llegar a los usuarios finales los diversos servicios que ofrecen, además del aumento en el uso de dispositivos que permiten la conexión a Internet desde esa época.[85]

Desde entonces, las direcciones IPv4 se han ido acabando. El cambio se plantea hacia otras direcciones que permitan soportar el aumento tanto de dispositivos como de usuarios.

La *Internet Society* menciona que esta escasez de direcciones podría provocar los siguientes cuatro supuestos:

- Sus programas de Internet, juegos en línea y aplicaciones favoritos podrían ralentizarse o dejar de funcionar.
- Los dispositivos conectados a Internet tienen más dificultades para comunicarse entre sí, lo que dificulta la capacidad de ofrecer servicios como voz y video.
- La confiabilidad y transparencia de Internet podrían verse comprometidas debido a las direcciones IPv4 compartidas.
- Los nuevos dispositivos, electrodomésticos, sensores y otros objetos (a menudo denominados “Internet de las cosas”) no podrán conectarse o tendrán dificultades para comunicarse.[86]

---

[84] *Idem.*

[85] Patrizio, Andy, *Avast. IPv4 frente a IPv6: ¿en qué se diferencian?* Recuperado el 2 de noviembre de 2021, de: *https://www.avast.com/es-es/c-ipv4-vs-ipv6-addresses#gref*

[86] Internet Society, *IPv6*. Recuperado el 20 de febrero de 2021, de: *www.internetsociety.org/wp-content/uploads/2018/03/IPv6-Fact-Sheet-FinalWEB.pdf*

Esta transición de dirección IPv4 a IPv6 ha sido impulsada por los diversos fabricantes de productos del *IoT* a causa del número limitado de direcciones por el que se puede descomponer una dirección IPv4.

3.1.3 IPv6

El IPv6, de acuerdo con la *Internet Society*, es el estándar de Protocolo de Internet (IP por sus siglas en inglés) de próxima generación destinado a reemplazar eventualmente al IPv4.[87]

Este protocolo ha sido usado desde 1996, pero de forma pausada debido a que en esos momentos la ampliación de las direcciones no era necesaria. Logra ampliar de forma considerable los *Bits* pasando de 32, ofrecida por el IPv4, a 128; a la fecha se podría considerar como inagotable y logra satisfacer los 100 mil millones de dispositivos de la *IoT,* que se estiman entrarán en servicio en las próximas décadas.[88]

La *Internet Society*, en su reporte sobre La Internet de las Cosas realizado en 2015, estableció que este protocolo tiene varios desafíos: “Los principales desafíos para los desarrolladores de la *IoT* son que IPv6 no es interoperable con IPV4 en forma nativa y que la mayor parte del software de bajo costo fácilmente disponible para dispositivos de la *IoT* solo implementa IPv4”.[89]

Desde 2012, el uso de la IPv6 ha ido en aumento, causando que empresas como *Google* utilicen en el casi 50% de todo el tráfico de ciertos países el uso de este protocolo. De acuerdo a la *Internet Society*, se debe tener en cuenta lo siguiente:[90]

- Asegurarse que todos los equipos de red (incluidas las compras previstas) sean compatibles con IPv6; aunque no esté desplegando IPv6 hoy, su equipo debe estar preparado para IPv6 o puede que tenga que actualizar o recomprar dispositivos más adelante.

[87] *Idem.*
[88] Rose, Karen, *op. cit.*
[89] *Idem.*
[90] Rose, Karen, *op. cit.*

- Los operadores de redes deben solicitar la conectividad IPv6 a sus proveedores de servicios de Internet y asegurarse de que todos sus equipos de red son compatibles con IPv6.
- Los creadores de contenidos, los desarrolladores y las empresas pueden hacer que sus propios sitios web y contenidos estén disponibles a través de IPv6. Muchos proveedores de alojamiento ofrecen IPv6 y algunos incluso lo ofrecen a una tarifa reducida en comparación con respecto a IPv4.
- Los gobiernos pueden exigir el cumplimiento de IPv6 a todos los contratistas y relaciones comerciales, y liderar con ejemplo en el despliegue de IPv6 en todos los sitios web y servicios.

A nivel mundial, se ha incrementado el uso del protocolo IPv6 por parte de las empresas. La *Internet Society*, en el año de 2020, emitió las estadísticas respecto al despliegue del IPv6 en el mundo, esto debido a su 8° aniversario del lanzamiento mundial de la IPv6, destacando lo siguiente:[91]

- La red de *Reliance Jio* en la India, tiene más del 90% de despliegue de IPv6.
- La enorme red de *Comcast* en los Estados Unidos está en un 73% de IPv6.
- Los operadores inalámbricos combinados de EE. UU. tienen más del 85% de IPv6.
- *Deutsche Telekom* tiene más del 68% de IPv6.
- *Claro* en Brasil está en 62% IPv6.

[91] York, Dan, *Ayúdanos a conseguir más sitios web disponibles con IPv6 para celebrar el 8.º aniversario del lanzamiento mundial de la IPv6* ,Internet Society, 2020. Recuperado el 20 de febrero de 2022, de: *https://www.internetsociety.org/es/blog/2020/06/ayudanos-a-conseguir-mas-sitios-web-disponibles-con-ipv6-para-celebrar-el-8-o-aniversario-del-lanzamiento-mundial-de-la-ipv6/*

En el caso de México, el IFT publicó durante el 2020 un documento en el cual sugería la adopción del IPv6, donde proponía establecer redes masivas de *IoT*, además de contribuir a mejorar la seguridad en las conexiones. Este protocolo aporta mejoras respecto a los estándares de seguridad, movilidad y calidad de servicio del IPv4.

3.1.4 Tecnología M2M

La tecnología M2M es la abreviatura para referirse a la conexión “Machine to Machine”, que se traduciría como comunicación máquina a máquina; es decir, comunicación directa punto a punto utilizando módulos de hardware integrados y redes celulares o cableadas. [92]

En casi todos los dispositivos con conexión M2M, se necesita un sensor o medidor para capturar un evento, ya sea la temperatura, el nivel de inventario, etcétera. Se retransmite a través de una red hacia una aplicación que traduce el evento capturado en información.[93]

Para el año 2012 se esperó que se utilizarían alrededor de 60 millones de dispositivos usando la tecnología M2M; sin embargo, este tipo de tecnología disminuiría en uso con el tiempo debido al incremento en el aprovechamiento de conexiones a la nube.[94] Esto no significa que la transición sea rápida o que la conexión M2M esté desapareciendo; por el contrario, este tipo de conexión se ha ido actualizando al mundo usando la red Wi-Fi para conectarse a otro dispositivo.

Tal es el caso de naciones como Reino Unido, donde se aplica este tipo de conexiones en medidores de cuentas de servicios públicos (*Smart meters,* por su nombre en inglés), los cuales se encargan de medir el uso de energía y de agua de las personas, siendo de fácil instalación al ser colocadas en los domicilios de las

---

[92] Polsonetti, Chantal, *Know the Difference Between IoT and M2M*, 2014. Recuperado el 20 de diciembre de 2021, de: *www.automationworld.com/products/networks/blog/13312043/know-the-difference-between-iot-and-m2m*

[93] Marce, Cancho*, El internet de las cosas, En un mundo conectado de objetos inteligentes*, Fundación de la innovación Bankinter, 2011. Recuperado el 20 de marzo de 2022, de: https://www.fundacionbankinter.org/wp-content/uploads/2021/09/Publicacion-PDF-ES-FTF_IOT.pdf

[94] *Idem.*

personas; llevan información del consumo de los bienes en tiempo real y lo relacionan con el costo que lleva el uso de éstos.

La recopilación de estos datos mejora la interacción con el usuario debido a que la compañía conoce los mismos datos que las personas y facilita los procesos de facturación. No amerita que el personal de las empresas del Reino Unido acuda a los domicilios a recolectar los datos y los devuelva a los usuarios de estos servicios.

En el hogar también se encuentran dispositivos que utilizan este tipo de conexión, por ejemplo: las consolas de videojuegos, los dispositivos portátiles, dispositivos de seguridad, medidores de actividad física, incluso algunos asistentes de las actividades que se realizan de forma cotidiana.

Es por la injerencia de esta tecnología que su aplicación debe estar en constante renovación a fin de que no se vea remplazada por otro tipo de conexiones. Sin embargo, de acuerdo con Paul Lalancette, "el uso de manera efectiva de la tecnología M2M requiere experiencia en tecnología de comunicaciones, hardware, aplicaciones de software, integración e implantación de estos".[95]

3.1.5 Conexión a la red 5G

De acuerdo con lo dicho por el Comisionado del IFT, Ramiro Camacho Castillo, la Banda 5G "es la 'ola' tecnológica de conectividad de última generación que permitirá más velocidad, banda ancha, conectividad masiva de dispositivos o cosas, alto nivel de confianza técnica y baja latencia".[96]

De acuerdo al IFT, "los servicios móviles de quinta generación serán completamente diferentes a los servicios actuales de tercera y cuarta generación, ya que, permitirán llevar a cabo comunicaciones de gran fiabilidad y baja latencia (*URLLC, Ultra Reliable Low Latency Communications*), banda móvil mejorada

[95] *Idem.*
[96] Camacho Castillo, Ramiro, Comisionado IFT, *IoT y 5G*. Recuperado el 20 de octubre de 2022, de: *http://www.ift.org.mx/sites/default/files/conocenos/pleno/presentaciones/ramiro-camacho-castillo/ioty5g-sololectura.pdf.*

(*eMBB, Enhanced Mobile Broadband Access*), así como comunicaciones masivas tipo máquina (*mMTC, Massive Machine Type Communications)*".[97]

Esta tecnología se desarrolla bajo las bandas de frecuencia: por debajo de 1GHz; entre 1 y 6 GHz y por encima de los 6 GHz[98]. Por lo que, en coordinación con la ITU, el IFT, quien es el encargado de administrar el espacio radioeléctrico en el Estado mexicano, deberá habilitar a los proveedores de los diferentes servicios de telecomunicaciones el acceso a esta banda del espectro radioeléctrico.

De esta forma se garantizaría, tanto a los usuarios como a los diferentes proveedores de servicios, el uso de esta ventaja tecnológica. La Red 5G facilitará muchos de los procesos de conexión que existen entre los dispositivos M2M o aquellos que usan un intermediario para conectarse.

La coordinación que se menciona en el párrafo anterior se ha planificado desde hace mucho; sin embargo, se vio reflejada en el marco del programa IMT-2020 de la ITU, por medio de la cual los miembros de esta organización desarrollan normas internacionales que permitan el correcto funcionamiento de esta tecnología.[99]

Esta transición no es inmediata. Al contrario, se cree que para el año 2030 la tecnología 4G coexista con la 5G[100] debido a que la transición necesita la infraestructura adecuada para ello, así como la constante evolución de los servicios que se ofrecen en la tecnología antes mencionada.

No obstante, esto no deja de lado el increíble avance de esta tecnología. Las estimaciones muestran que para el año 2023 el número de conexiones 5G

---

[97]Lainez Izaguirre, Carlos. *et al*., *Visión y prospectiva de la conectividad 5G*. Recuperado el 20 de septiembre de 2021, de: *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/otros-documentos/visionyprospectivadelaconectividad5g.pdf.*

[98] *Idem.*

[99]ITU, *5G-Quinta generación de tecnologías móviles*, 2019. Recuperado el 26 de febrero de 2021, de: *https://www.itu.int/es/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.*

[100] Foro Económico Mundial en colaboración con PwC, *The Impact of 5G: Creating New Value across* Industries and Society, enero de 2020. Recuperado el 3 de marzo de 2022. De: https://www.weforum.org/whitepapers/the-impact-of-5g-creating-new-value-across-industries-and-society

alcanzará los mil millones, lo que representa una tasa anual de crecimiento compuesto del 217.2% durante el periodo que abarca de 2019 a 2023.[101]

Su uso va en constante aumento a causa de los múltiples beneficios como la conexión de 100 veces más dispositivos a la red, pudiendo habilitar y beneficiar a los objetos del Internet de las cosas y llegar hasta un millón de objetos conectados por kilómetro cuadrado.[102] Facilita la conexión de los objetos del hogar al Internet, el desempeño de éstos y el consumo de energía a causa de la rapidez con la que se podrían descargar documentos, películas o listas de reproducción de música, entre otros usos.[103]

Incluso, el uso de la tecnología 5G traería otros posibles beneficios como la inclusión de mejoras a los productos que se utilizan en los hogares, siendo posibles los controles por voz de aparatos que a la fecha lo incluyen los esparcidores de agua. Permiten la posibilidad de conectar todos los dispositivos del *IoT* de un hogar; y así, de esta manera se puede conocer el estatus de cada objeto sin la necesidad de acceder a ellos de forma individual.

Es por eso que la tecnología 5G es de suma importancia para los objetos del *IoT* pues se potencializarían los beneficios de este tipo de objetos.

3.2 Funcionalidad de las aplicaciones en los objetos conectados a Internet

Para poder reflejar la importancia de las aplicaciones al momento de usar algún objeto del Internet de las cosas, es preciso conceptualizar la palabra aplicación o app en el universo de la informática.

[101] Worldwide 5G Connections Forecast, 2019-2023, IDC, Recuperado el 30 de septiembre de 2021, de: https://www.businesswire.com/news/home/20191216005053/en/IDC-Forecasts-Worldwide-5G-Connections-Reach-1.1
[102] Lainez Izaguirre, Carlos. et al., *op. cit.*
[103] *Idem.*

De acuerdo con la RAE, una aplicación es “un programa preparado para una utilización específica como el pago de nóminas, el tratamiento de textos, etcétera”.[104]

En pocas palabras, una aplicación es un programa diseñado para realizar una función determinada y así facilitar las tareas complejas por las cuales fueron diseñadas; regularmente son usadas en dispositivos móviles, aunque su uso no excluye a que pueda usarse en dispositivos de escritorio o no portátiles como PC o consolas de videojuegos.

Para adquirir las aplicaciones existen tiendas virtuales, ya sea por medio de portales de Internet o haciendo uso de aplicaciones móviles. Las aplicaciones están elaboradas bajo ciertos protocolos informáticos propuestos por diversas empresas dedicadas a realizar sistemas operativos, facilitando así la descarga de éstas y su uso en dispositivos con el mismo sistema operativo.

Esto lleva a clasificar a las aplicaciones en los siguientes rubros:

- Aplicaciones para dispositivos de escritorio o dispositivos móviles.
- Por su sistema operativo. Como se mencionó antes, el sistema operativo para el cual fueron diseñadas restringe su uso a cualquier tipo de dispositivo.
- Por su temática. Las diversas categorías de las aplicaciones para un mismo sistema operativo van desde entretenimiento, comunicación, como lo son las de *apps* para consultar el correo electrónico o aquellas para enviar mensajes de texto, hasta cuestiones financieras o de salud.
- Por su forma de adquisición. Ya sea que se adquieran a través de una remuneración económica o sin costo alguno (como lo son la mayoría de las aplicaciones en las tiendas virtuales más conocidas).

De acuerdo con la *BBC*, en el año 2011 crear una aplicación implicaba el costo de 32.000 dólares en un tiempo aproximado de dos meses. Este costo

[104] RAE, *Significado de la palabra aplicación*. Recuperado el 29 de octubre de 2021, de: *https://dle.rae.es/aplicaci%C3%B3n*

significaría un aumento significativo si se hiciera para diversos sistemas operativos.[105]

Para el año 2021 se estima que el costo a pagar por la elaboración de una app sería desde $70,000 hasta $130,000 pesos, dependiendo de su complejidad pues el costo está basado en el tiempo invertido.[106]

Sin embargo, este costo no refleja la realización de una app por la misma persona que desee ser su propietaria, sino que a la fecha es posible realizar una aplicación sin costo, pero con el conocimiento necesario para realizarla, lo que se traduciría en un coste bajo.

El incremento en el uso de *apps* para satisfacer las necesidades de los usuarios al momento de adquirir o utilizar los servicios de diversos proveedores, así como el aumento en la creación de videojuegos en formato de aplicaciones móviles provoca que las aplicaciones móviles sean un elemento de diario de las personas y, por lo tanto, que se vuelva indispensable su creación para ofrecer servicios.

Es por eso que las cosas conectadas a Internet necesitan de aplicaciones para funcionar fuera del ecosistema por medio del cual funcionaría un objeto de conexión directa con otro (M2M), debido a que facilita la conexión con otro objeto mientras se está usando un *Smartphone* u otro dispositivo portátil.

También tiene como beneficio un mejor manejo de ciertos sitios web al usar las *apps* proveídas por las empresas titulares. La información se encuentra disponible desde un ordenador sin la necesidad de usar un buscador de Internet para ingresar.

Por ejemplo, en el mercado automotriz español se observa el uso de las aplicaciones móviles como mecanismo necesario para que un automóvil pueda conectarse a Internet.

---

[105] BBC, *Qué son las "apps" y para qué sirven*, 2011. Recuperado el 26 de febrero de 2021, de: *https://www.bbc.com/mundo/noticias/2011/04/110408_1336_tecnologia_apps_negocios_celulares_telefonos_inteligentes_dc*

[106] Retail Digital, *¿Cuánto cuesta desarrollar una app en México?*, 2021. Recuperado el 26 de febrero de 2022, de: *https://retaildigital.mx/cuanto-cuesta-desarrollar-una-app-en-mexico/*

Aunque es de lujo el uso de estos vehículos, este tipo de coches va en aumento debido a la cantidad de datos que pone a disposición de los usuarios, tales como estatus de varias partes del vehículo, cámaras del automóvil, ubicación en tiempo real, velocidad a la que se conduce, bloqueo del automóvil desde el teléfono, entre otras funciones.[107]

En el hogar también se refleja este uso al poder programar el tiempo de lavado en una lavadora o para programar el inicio de preparación de café en una cafetera mientras se realizan otras actividades.

Sin embargo, uno de los usos que se está convirtiendo en el más frecuente en los hogares es el uso de aplicaciones que utilizan los asistentes inteligentes para interactuar con los usuarios de estos productos. Los productos interactúan a través de inteligencia artificial; no obstante, necesitan de estas aplicaciones para actualizarse, agendar citas y llevar un control de los demás dispositivos conectados a ella como focos, luces[108], puertas, o dispositivos móviles.

La intención al crear estos dispositivos es la de convertir al hogar en un sitio inteligente[109] donde todos los dispositivos estarían conectados a un asistente con IA (inteligencia artificial). Por lo tanto, sería sencillo ordenarle a cualquier dispositivo del hogar que realice cierta actividad aun cuando no se esté allí.

3.3 Usos en el hogar del *IoT*

De acuerdo a un estudio del IFT durante el 2019, la categoría de “Hogar y Entretenimiento” tiene el quinto puesto dentro de una lista de 22 servicios ofrecidos mediante el uso de Internet.[110]

---

[107] Spring profesional, *Cómo afectan las aplicaciones móviles al Internet de las Cosas (IoT)*, España, 2021. Recuperado el 5 de noviembre de 2021, de: *https://blogcandidatos.springspain.com/transformacion-digital/como-afectan-las-aplicaciones-moviles-al-internet-de-las-cosas-iot/*

[108] Google, *Conoce la app de Google Home*. Recuperado el 5 de abril de 2022, de: *https://support.google.com/chromecast/answer/7071794?hl=es-419&co=GENIE.Platform%3DAndroid*

[109] Spring profesional, *op. cit.*

[110] Terrazas Briones, Pedro. *et al.*, *Análisis exploratorio de la comercialización de servicios de conectividad para IoT,* México, 2019. Recuperado el 30- de octubre- de 2021, de: *https://www.bing.com/search?q=Análisis+exploratorio+de+la+comercialización+de+servicios+de+c*

Los hogares inteligentes o *Smart Home* hacen referencia a las viviendas que están conformadas en su totalidad por electrodomésticos o equipos electrónicos controlados de forma remota través de un dispositivo móvil, esto gracias a la conexión a Internet dentro de su hogar.

Respecto a ello, existe una ciencia dedicada a la aplicación de la tecnología al hogar, siendo conocida como domótica. De acuerdo a la Fundación UNAM, el objeto de tener una *Smart Home* es contar con un "sistema demótico dentro de un hogar para que proporcione soluciones prácticas que se ejecuten a través de control automático, brindando comodidad y seguridad a los habitantes, así como un ahorro en el consumo de la energía eléctrica y la comunicación".[111]

Por ello, el objeto de este capítulo es enfocarse en aquellos objetos que se encuentran en un hogar sin que estén conectados todos entre ellos; es decir, objetos particulares conectados a Internet.

Como se mencionó en capítulos anteriores, la mayoría de los objetos que están en el hogar utilizan la tecnología "dispositivo a dispositivo", como son las bombillas de luz, los interruptores, los termostatos y las cerraduras y puertas (por ejemplo, un mensaje del estado de bloqueo de una puerta o un comando para encender una luz).[112]

Dentro de este tipo de objetos se encuentran los electrodomésticos inteligentes, los cuales aprovechan los sensores y la conexión para facilitar su uso a los usuarios. Por ejemplo, algunos refrigeradores controlan los productos que contienen y así pueden determinar su escasez a fin de elaborar automáticamente la lista para el supermercado; también pueden verificar la fecha de expiración de los alimentos que se almacenan en el refrigerador.

---

onectividad+para+IoT&qs=n&form=QBRE&msbsrank=6_6__0&sp=-1&pq=briones&sc=6-7&sk=&cvid=C8033F21832F4854A7C3AA90A4258163

[111] UNAM, *La UNAM te explica: Hogares Inteligentes*, 17 de junio, 2016. Recuperado el 20 de diciembre de 2021, de: *https://www.fundacionunam.org.mx/unam-al-dia/la-unam-te-explica-hogares-inteligentes/*

[112] Marce, Cancho*, El internet de las cosas, En un mundo conectado de objetos inteligentes*. Fundación de la innovación Bankinter, 2011. Recuperado el 11 de octubre de 2021, de: *https://www.fundacionbankinter.org/wp-content/uploads/2021/09/Publicacion-PDF-ES-FTF_IOT.pdf*.

Además de las lavadoras que pueden controlar el tiempo de lavado, mencionadas en capítulos anteriores, existen las televisiones inteligentes, objetos sumamente comunes en los hogares. Las *Smart Tv* son la representación del *IoT* pues proyectan de forma simple un objeto común que se conecta a Internet y que facilita el uso de ellas al no tener que vincular o conectar otro dispositivo para poder consultar contenido exclusivo para otros.

Ahora bien, esto ha evolucionado de forma tal que se puedan controlar de forma remota y programar su funcionamiento desde un dispositivo móvil como un *Smartphone* o una tableta electrónica, los cuales por sus características los hacen los ideales para controlar a estos dispositivos.

Marcelo Alcaraz, en su artículo sobre el Internet de las cosas, señala ejemplos de esta tecnología como: “las luces y persianas de la casa pueden activarse/desactivarse cuando el sol se oculte o si está muy nublado; el aire acondicionado en cada habitación puede ajustarse a la temperatura preferida del miembro de la familia que en ella se encuentre; la calefacción puede encenderse antes de nuestro horario de llegada del trabajo, etc.”.[113]

También señala que este tipo de objetos conectados a Internet tienen ventajas como “evitar cientos de accidentes que ocurren diariamente pudiendo tomar medidas al respecto de forma más inmediata o bien automatizando estas, por ejemplo, si el detector de humo se activa podría contactar directamente con el departamento o el carro de bomberos más cercano”.[114]

Es por eso que no sólo existen objetos del *IoT* que son de uso diario, como los descritos anteriormente, sino que también existen objetos que son de uso ocasional y no tan conocidos, pero que siguen formando parte del Internet de las cosas, como lo son aquellos enfocados en la seguridad.

Por ejemplo, existe un dispositivo del *IoT* que se usa en algunos hogares como medio de protección. Este es el botón de pánico, el cual consta de un botón que al pulsarlo envía una señal de peligro a la estación de policía; sin embargo, en

[113] Alcaraz, Marcelo, *Internet de las Cosas*, Universidad Católica, 2018. Recuperado el 12 de junio de 2021, de: *http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf*
[114] *Idem.*

la actualidad, el botón de seguridad se ha colocado en los dispositivos móviles, ampliando el rango y la movilidad de este sistema de seguridad.

Existen más variantes a los tipos de botones de seguridad puesto que, de conformidad con lo señalado por el IFT, también las alarmas de robo y cámaras de seguridad con sensores de movimiento forman parte del *IoT* que se enfoca en dicho rubro.[115]

3.4 Tendencias impulsadas por el *IoT*

De acuerdo a Elena Estavillo, ex comisionada del IFT, la interoperabilidad y portabilidad de datos entre dispositivos y sistemas será una cuestión fundamental para el desarrollo de las aplicaciones del Internet de las cosas.[116]

Así mismo, ella señala que "será clave la colaboración continua entre países para asegurar la funcionalidad de los servicios provistos a partir de dispositivos y/ datos que se trasladen entre distintas ubicaciones, cuidando que no existan barreras a la competencia ni a la adopción tecnológica y garantizando la protección a los datos personales".[117]

Por consiguiente, se pueden recibir beneficios tanto para los consumidores como para las empresas que ofrecen sus productos al usar este tipo de tecnología, ya que se planea obtener la información relacionada al consumo, las preferencias y los datos relevantes al momento de realizar alguna campaña publicitaria o para mejorar los productos que comercializan, ya sea en próximos productos o actualizando los que ya fueron adquiridos, logrando que los usuarios o consumidores se vean beneficiados.

Para los fines antes mencionados, la transmisión de datos puede contener ciertos retrasos de milésimas de segundos pues su fin es recabar datos para su posterior actualización. No obstante, hay que tener en cuenta que existen dispositivos que recaban datos de forma inmediata para ser enviados y recibidos en

[115] Terrazas Briones, Pedro Javier. *et al., op. cit.*
[116] Gaceta IFT 13, Año III, No.15, marzo 2017. Recuperado el 15 de febrero de 2021, de: https://www.ift.org.mx/sites/default/files/contenidogeneral/multimedia/gacetaift-13-accesible.pdf
[117] *Idem.*

tiempo real y no con diferencias de milésimas de segundo o milésima de segundo porque esto provocaría retraso en el envío y recepción de los datos; por lo tanto, puede no cumplirse la función para la cual fueron diseñados dichos objetos.

Sin embargo, para lograr que los dispositivos puedan enviar los datos necesarios y puedan ser recibidos es necesario que exista la infraestructura idónea a fin de que lleguen de la mejor calidad posible.

Aunque existen aplicaciones en los ramos de la salud, el hogar, la industria, las ciudades inteligentes y transporte, éstas no son de un uso global o desarrolladas en todo el potencial que tendrían estos objetos debido a diversos factores que ralentizan su desarrollo.

Sin embargo, esto no impide que estos productos provoquen el desarrollo de otras tecnologías que con posterioridad podrían facilitar el desarrollo de los objetos del *IoT.*

Por lo tanto, el desarrollo del Internet de las cosas ha provocado que se busque la mejora en áreas que la involucran directamente, así como aquellas que afectan otro tipo áreas. Algunas de estas son:

- Interoperabilidad.
- Economías emergentes y cuestiones relacionadas con el desarrollo.

3.4.1 Interoperabilidad

La interoperabilidad es la capacidad de los sistemas, o algunos de los componentes que tienen la facilidad, de comunicarse entre sí sin importar el fabricante o las características del producto. Un ejemplo de la interoperabilidad sería la conexión de sistemas de riego en campos agrícolas, aunque estos sean de diferentes fabricantes.

Así, la interoperabilidad es uno de los principios fundamentales por los cuales se rigen los dispositivos del *IoT* puesto que su principal función es facilitar las actividades que se realizan día a día y para ello se necesita la interconexión de los dispositivos.

La preferencia de los usuarios por los productos que se conecten fácilmente con otros hace que genere más confianza su adquisición. Sería más rentable adquirir un producto con esa capacidad de interconexión sin que tenga limitaciones técnicas y comerciales.

Para ello, se señalan los 7 niveles por los que todas las plataformas pasan para tener una conexión completa y sin interrupciones por cuestiones de falta de vinculación con otros dispositivos:[118]

- Nivel 0. No hay interoperabilidad.
- Nivel 1. Interoperabilidad técnica.
- Nivel 2. Interoperabilidad Sintáctica.
- Nivel 3. Interoperabilidad Semántica.
- Nivel 4. Interoperabilidad Pragmática.
- Nivel 5. Interoperabilidad Dinámica.
- Nivel 6. Interoperabilidad Conceptual.

Se señalan como las importantes la interoperabilidad técnica, sintáctica, semántica y organizacional, las cuales se perciben como:[119]

- **Interoperabilidad técnica:** se encuentra asociada con los protocolos de comunicación y la infraestructura necesaria para que funcione.
- **Interoperabilidad sintáctica:** es aquella que se encuentra asociada a formatos y codificaciones de datos.
- **Interoperabilidad semántica:** es aquella asociada a la comprensión común de la información intercambiada.

[118] River Publishers, *Advancing IoT Platforms Interoperability*, 2018. Recuperado el 20 de agosto de 2022, de: *https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf.*
[119] *Idem.*

- **Interoperabilidad organizacional:** es aquella asociada a la capacidad de las organizaciones para comunicar y transferir información de manera efectiva a través de sistemas de información de forma efectiva.

Lograr la interoperabilidad entre los diferentes dispositivos que se pueden conectar a Internet, especialmente los que se usan en el hogar, requiere de las interacciones entre los componentes clave en los sistemas del *IoT*.

El *Cross Platform Access* es patrón de acceso básico entre los dispositivos que integran el ecosistema del *IoT.* El objetivo principal es la de ocultar cuando una aplicación accede a información o activos de diferentes plataformas a través de la misma interfaz.

Esto es posible debido a que las aplicaciones o dispositivos descubren plataformas con información relevante, permitiendo la conexión entre plataformas que son potencialmente de diferentes proveedores y que puedan comunicarse a través de los mismos formatos.[120] De esta forma, se pueden conectar y acceder a información y funciones no sólo de diferentes plataformas, sino también de plataformas que almacenan información de otros dominios de aplicación.

Esto causa que se cree una independencia de la plataforma para lograr que una aplicación o dispositivo se utilice sobre diferentes estructuras, lo cual es útil cuando los dispositivos producen datos de *IoT* con tecnología diferente. Por ejemplo, cuando la observación de diferentes lugares se basa en radares.

Esto es a nivel técnico; sin embargo, se deben tener en cuenta otras cuestiones que sobrepasan el nivel técnico para lograr la interoperabilidad de los dispositivos del Internet de las cosas. Por la importancia y el alcance que tienen estos objetos, es necesario establecer acuerdos entre las empresas a fin de que la interoperabilidad se dé sin tantas complicaciones.

[120] *Idem.*

Es por eso que la promoción de este tipo de acuerdos entre los actores (que se describen en capítulos posteriores, sin los usuarios) favorece la conexión rápida y efectiva entre dispositivos, lo que se traduce en una mejoría en la competencia en el mercado de los objetos del *IoT*, y a su vez, trae aparejado un beneficio en favor de los usuarios.

Para ello, las empresas han implementado la iniciativa “IoTivity”, la cual tiene por objetivo orientar y fomentar la cooperación entre las 300 empresas y desarrolladores que tienen como miembros.[121]

Además, se establecieron los parámetros denominados “Arquitectura de Referencia de Internet Industrial”, mismos que se establecieron desde 2014 con la intención de facilitar esta interconexión entre dispositivos creados por los afiliados a estos parámetros[122].

En el ámbito europeo surgen proyectos de estandarización que tienen por objeto identificar semejanzas en entornos de los dispositivos del *IoT*, como ciudades inteligentes o sistemas de transporte con esta tecnología; algunas de ellas son la IEEE P2413[123] y la Iot-A.

Otro de los puntos importantes a considerar es la creación de dispositivos sin estándares de calidad altos o con los mínimos. Cada empresa tiene sus propios estándares, por lo que es difícil establecer una categoría que ayude a los usuarios a no adquirir productos que puedan provocarles riesgos de salud o dañar los dispositivos a los que se conecten.

[121] IoTivity, Marco de software de código abierto que permite la conexión de dispositivos entre sí, implementado en dispositivos del *IoT.* Recuperado el 22 de septiembre de 2022, de: *http://iotivity.org/*
[122] Industrial Internet Reference Architecture (IIRA), *La competencia de RAMI 4.0*. Recuperado el 22 de septiembre de 2022, de: *https://altertecnia.com/industrial-internet-reference-iira/*
[123] IEEE, S.A., Standard for an Architectural Framework for the Internet of Things. Recuperado el 23 de septiembre de 2021, de: *https://standards.ieee.org/ieee/2413/6226/*

En ese sentido, sería prudente establecer estándares comunes que ayuden a generar un mínimo y un máximo en los estándares de calidad trayendo innovación, seguridad y confianza del usuario.[124]

3.4.2 Economías emergentes y cuestiones relacionadas con el desarrollo

De acuerdo al informe denominado "*Harnessing the Internet of Things for Global Development,* presentando por el *Pacific Telecommunications Council",* los objetos del Internet de las cosas pueden funcionar como catalizadores para sobrepasar las metas de desarrollo digital.

En el documento se establecen 3 puntos que, de ser establecidos, acelerarían la evolución de la tecnología y del desarrollo de los países, los cuales son:[125]

a) Disponibilidad

Para el desarrollo de los dispositivos del *IoT* se necesita una infraestructura básica para que funcionen de manera eficiente (necesitan de la tecnología Wi-Fi, banda ancha, etcétera). Este tipo de dispositivos son baratos y fáciles de remplazar, por lo que cada vez más son utilizados en lugares con poco acceso, siendo construidos para resistir las condiciones de esos lugares.

b) Asequibilidad

El costo de los dispositivos del *IoT* es de fácil acceso en cuestiones económicas debido a que no se requiere más que la *IoT* básica para construir una base que facilite el uso de estos dispositivos en naciones en desarrollo.

c) Adaptabilidad

---

[124] Rose, Karen, *op. cit.*

[125] International Telecommunications Union, Suiza, *Harnessing the Internet of Things for Global Development*. Recuperado el 23 de junio de 2022, de: *https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf*

Una de las características fundamentales de los dispositivos del *IoT* es que son aparatos tecnológicos adaptables; no requieren de conocimientos técnicos para su instalación y uso. Ofrecen soluciones a corto, mediano y largo plazo, provocando una expansión en el uso de esa tecnología.

En conclusión, el uso de la *IoT* es algo que planea revolucionar el mundo a niveles de salud, ambientales, de producción agrícola e industrial, tecnológicos, etcétera. No sólo va a beneficiar a las empresas trasnacionales o países con desarrollo alto, sino que va a producir beneficios para los países en vías de desarrollo porque puede mejorar su industria acelerando los procesos de innovación y disminuir la distancia entre los países en vías de desarrollo y los que tienen un desarrollo alto.[126]

Para ello, es importante la colaboración de muchos entes para que exista un incremento tecnológico en los países en vías de desarrollo, así como la generación de innovación a fin de que los productos que puedan ofrecer las empresas trasnacionales no sean de forma inequitativa, causando daños al mercado y así provocando que se amplíe la brecha que existe entre los países del mundo.

[126] Rose, Karen, *op. cit.*

CAPÍTULO 4. AVANCES EN LA REGULACIÓN DEL INTERNET DE LAS COSAS A NIVEL INTERNACIONAL

4.1 Panorama General

Como se estableció anteriormente, el *IoT* es un tema con un grado de dificultad alto para que se pueda emitir regulación alguna debido a la complejidad de los temas. Sin embargo, existen algunos países que dentro de su normativa tienen considerada la regulación del *IoT*; aunque no de la forma en que se espera, pero con la intención de lograr avances importantes en el transcurso del tiempo.

Por los diversos estudios y aplicaciones del *IoT*, pareciera que la regulación de la Unión Europea sería la pionera en establecer las bases para regular el Internet de las cosas. Por el contrario, la Unión Europea aún no tiene disposiciones normativas enfocadas en este tema.

Aun así, desde 2010 cuentan con políticas públicas enfocadas al Internet de las cosas. Por ejemplo, la Agenda Digital para Europa de 2010 y la estrategia para el Mercado Único Digital de Europa de 2015, en las que se tiene la intención de adoptar y potenciar el uso de *IoT* en los diversos medios de comercio, así como el uso de estos en las diferentes fases de la cadena de producción.[127]

Esta visión se concreta en un documento denominado “Avanzando el Internet de las Cosas en Europa”[128], el cual se basa en tres pilares:

- Un próspero ecosistema de *IoT.*
- Enfoque de *IoT* centrado en el ser humano.
- Mercado único europeo para el *IoT.*

Al tener únicamente documentos con falta de coercitividad, la regulación del Internet de las cosas se encuentra en diversos documentos normativos de temas periféricos impuestos tanto por la Unión Europea como por los Estados que la

[127] Agenda Digital para Europa, 19 de mayo de 2010 (COM/2010/0245). Recuperado el 15 de julio de 2022, de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:si0016

[128] Advancing the Internet of Things in Europe, 19 de abril de 2016 (COM/2016). Recuperado el 20 de mayo de 2022, de: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

conforman, siendo de suma importancia tópicos como la protección de datos y la ciberseguridad, entre otros.[129]

4.2 Reino Unido

Antes de la entrada del Código de Prácticas de Seguridad del consumidor en relación con el Internet de las cosas, un documento que se explicará posteriormente, el uso de los dispositivos del *IoT* en el mundo comenzaba a ser una tecnología que iba en ascenso. Tan solo en el 2016 existían 13 millones de dispositivos conectados en el Reino Unido y las estimaciones realizadas en ese año para 2024 eran cerca de 156 millones de dispositivos.[130]

Por consiguiente, la regulación de este tipo de dispositivos era necesaria. Además, el incremento en su uso, el almacenamiento de datos y la libertad de los fabricantes para establecer sus propias medidas de seguridad provocaría diversos riesgos en la seguridad de los usuarios de estos dispositivos. En consecuencia, esta nación tendría años posteriores dos documentos que tienen por intención comenzar la regulación de los objetos del Internet de las cosas en el Reino Unido.

Sin embargo, el primero de ellos no tiene fuerza jurídica puesto que no es un instrumento normativo, sino más bien un código de práctica voluntaria al no traer aparejada la obligatoriedad.

El segundo es una propuesta de ley que, en caso de aprobación, traería aparejada la obligatoriedad en su cumplimiento. Su objetivo consiste en que los dispositivos que se vendan en territorio del Reino Unido estén protegidos ante posibles ataques digitales, mejorando de esta manera lo planteado en el Código antes mencionado.

[129] Barrio Andrés, Moisés, *Internet de las cosas,* España, REUS, 2018, 79-100
[130] OFCOM, *Connected Nations Report 2017: Data analysis*. Recuperado el 22 de junio de 2022, de: *https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108515/connected-nations-internet-things-2017.pdf.*

4.2.1 Código de Prácticas de Seguridad del consumidor en relación con el Internet de las cosas

El *Code of Practice for consumer IoT security* (Código de prácticas de seguridad del consumidor en relación con el Internet de las cosas, por su traducción en español) fue publicado el día 14 de octubre del año 2018[131], momento en que se haría del conocimiento de la población del Reino Unido.

Tiene como origen la intención del gobierno del Reino Unido, en colaboración con el Centro Nacional de Seguridad Cibernética (NCSC), de identificar propuestas para mejorar la seguridad de este tipo de dispositivos. Para ello, se estableció un grupo de estudio que en el año 2018 logró tener un informe de seguridad sobre el diseño de los dispositivos del *IoT.*

Este informe lleva por nombre "*Secure by Design"*, el cual, además de mostrar los datos que revelan diversos aspectos de la seguridad de los dispositivos del Internet de las cosas, mostraba un borrador del código antes mencionado, estableciendo los trece puntos por los cuales se rige.[132]

Por lo que, para el mismo año, el gobierno del Reino Unido celebró una consulta informal que ayudó a establecer de forma precisa los parámetros sobre los cuales se iba a regir el código antes mencionado. Finalmente, fue publicado el 14 de octubre de 2018.

Lo que busca este documento es establecer puntos a seguir de forma práctica que permitan la seguridad de los dispositivos del *IoT,* trayendo como consecuencia la protección a la privacidad y la seguridad de los usuarios, además de facilitar su uso.

Este código se rige por 13 directrices que resumen la totalidad de los puntos que regula, así como el objetivo que persigue este documento. Las pautas son:

---

[131] Uk Government, *Code of Practice for consumer IoT security*, 2018. Recuperado el 23 de febrero de 2022, de: *https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.*

[132] Uk Government, *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*, 2020. Recuperado el 24 de febrero de 2022, de: *https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation*.

a) Sin contraseñas universales

Este punto se refiere a que cada dispositivo debe traer como forma de acceso contraseñas únicas y no universales.

b) Política de divulgación de vulnerabilidades

Se refiere a un sistema de atención a los usuarios, por medio del cual se le informa al proveedor de problemas que puedan llegar a presentar.

c) Actualización del *software*

Este apartado se refiere a las actualizaciones que deben tener los dispositivos y la forma en que se deben realizar para mantener un nivel óptimo de seguridad.

d) Almacenamiento seguro de datos sensibles y de credenciales

En ella se establece que las credenciales de los usuarios (algunos datos pueden ser: nombre de usuario, contraseñas, etcétera) deben ser almacenadas de forma segura.

e) Cifrado de la información

Se refiere al cifrado en tránsito de la información sensible de los usuarios.

f) Minimizar las superficies de ataque que están expuestas

Este punto se refiere a que el *hardware* no debe estar expuesto a accesos externos de forma innecesaria.

g) Integridad del *software*

Se refiere a que el dispositivo debe tener la capacidad de alertar al consumidor sobre algún cambio no autorizado.

h) Protección de datos personales

Los fabricantes y los proveedores deben informar a los usuarios de estos dispositivos de la forma en que van a tratar sus datos personales: cómo se utilizan, quién y con qué fines.

i) Sistemas resistentes a interrupciones

Se refiere a la disponibilidad de los dispositivos para mantenerse funcionales ante la pérdida de conexión a la red.

j) Telemetría

Monitoreo de datos de uso y medición para evaluar la seguridad y prevenir futuros daños.

k) Eliminación de datos personales

Se refiere a que los dispositivos deben facilitar la configuración de la información personal para que puedan eliminarse.

l) Facilidades para la instalación y el mantenimiento de los dispositivos

Se refiere a que los dispositivos deben estar configurados para que se empleen los pasos mínimos y mejores prácticas de uso.

m) Validación de datos de entrada

Se refiere a la verificación de información para asegurarse de que cumplan con los requisitos y parámetros de calidad.

En síntesis, el Código busca complementar las posibles recomendaciones y estándares sobre seguridad digital que se vayan realizando través del tiempo, como las leyes sobre protección de datos o cuestiones técnicas que regulan los protocolos de seguridad de los dispositivos.

Dentro de los aspectos más relevantes y que se van a identificar en instrumentos mencionados con posterioridad en el presente trabajo, se encuentran los sujetos a los que se dirige este documento, siendo los siguientes:[133]

- Fabricante del dispositivo: Es el producto final; es decir, el objeto final que se va a conectar a Internet.
- Proveedor de los servicios: Son aquellas personas que proporcionan servicios de almacenamiento en la nube o de transferencia de datos.
- Desarrolladores de *apps* móviles: Son aquellos proveedores que permiten la interacción entre el objeto final y dispositivos móviles, como celulares.
- Vendedores minoristas: Son aquellas personas que comercian con los productos materiales; es decir, con los dispositivos que se conectan a Internet.

[133] *Idem.*

Otro punto esencial de este Código es el ámbito de aplicación; es decir, qué tipo de objetos son amparados por esta reglamentación no obligatoria. Se encuentran los objetos de consumo conectados a Internet (algunos ejemplos de estos son los juguetes infantiles, los sistemas de alarmas, las cámaras, los televisores, los asistentes domésticos, los electrodomésticos, entre otros) y servicios asociados (en este rubro se incluyen las *apps* móviles, los servicios de almacenamiento en la nube, entre otros).

De lo anterior se puede establecer que el objeto principal de este Código reside en los dispositivos del hogar; sin embargo, los ejemplos antes mencionados no son limitativos y también incluyen a objetos que pueden no ser para el hogar como los rastreadores móviles.

4.2.2 Proyecto de Ley de Seguridad de Productos e Infraestructura de Telecomunicaciones

Este proyecto de ley es relevante puesto que tiene como base la promoción de la infraestructura tecnológica necesaria para el desarrollo eficiente de las diferentes actividades en ella. Destaca la implementación de nuevas tecnologías que necesitan del despliegue de nueva infraestructura; se da apoyo al uso de la red 5G, la cual mejora la transmisión de datos por esta banda. Además, se plantea establecer medidas que protejan a los usuarios de dispositivos del *IoT*.

Como punto principal de esta investigación, se tomará en cuenta la parte que hace referencia a la protección de datos que deben ejercer los fabricantes, vendedores minoristas, creadores de aplicaciones móviles y distribuidores de servicios de telecomunicaciones al participar en todas las fases de la cadena de producción de un producto del *IoT*.

El apartado sobre objetos del Internet de las cosas, de la propuesta antes mencionada, tiene como base el Código mencionado en el capítulo anterior. Es decir, se basa en los mismos trece puntos que rigen al *Code of Practice for*

consumer IoT security. Sin embargo, de esta propuesta se destacan varios puntos que sirven para aclarar de forma simplificada su objetivo, los cuales son:[134]

a) Prohibición de contraseñas predeterminadas universales.
b) Proporción de los fabricantes a favor de los usuarios de un contacto público para informar de vulnerabilidades de seguridad.
c) Informe por parte de los fabricantes a los usuarios sobre el tiempo en que el producto adquirido va a recibir actualizaciones.
d) Regulación y supervisión de la ley por parte de un organismo regulador; sin embargo, aún no se designa en la ley.
e) Establecimiento de multas en caso de transgresiones a las disposiciones de la ley.

Los tres primeros puntos han recibido comentarios por parte de los usuarios (esto debido a que se pueden dejar comentarios a la ley, en razón de que se encuentra en consulta de acuerdo a la legislación del Reino Unido) sobre la viabilidad de establecer estas medidas. Del primero se dice que el establecer contraseñas predeterminadas podría vulnerar la reparación y/o asistencia para reparar posibles fallas en los dispositivos; del segundo que el hacer del conocimiento las vulnerabilidades antes de que el fabricante pudiera repararlas pudiera comprometer la seguridad; y del tercero, han surgido dudas sobre la viabilidad de que los fabricantes y/o vendedores de estos aparatos tecnológicos puedan disminuir el precio de los dispositivos de forma tal que su mercado incremente, poniendo en peligro el cuidado de los datos personales de las personas que los adquieren.

Sin embargo, este proyecto tiene ciertas diferencias respecto a los objetos que entran dentro de los parámetros establecidos en el *Code of Practice for consumer IoT security*. Se excluyen diversos dispositivos que podrían considerarse parte de los objetos del *IoT*, tal y como se ha mencionado en capítulos anteriores.

[134] Uk Government, *Product Security and Telecommunications Infrastructure (PSTI*), 2021. Recuperado el 26 de junio de 2022, de: https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

Del análisis de la parte 1, capítulo 1, en sus apartados 4, 5 y 6[135] de este Código, se excluyen vehículos, medidores inteligentes (mencionados anteriormente), computadoras de escritorio y algunas computadoras portátiles (por la posibilidad de conexión vía cable). Por lo tanto, no contempla diversos objetos que pueden tener las mismas deficiencias en ciberseguridad que tendrían si no estuviera en vigencia esta norma.

De acuerdo al estatus que ha revelado el congreso del Reino Unido (a la fecha de realización del presente trabajo), aún no se aprueba esta ley, Se encuentra en la Cámara de los Lores, en la etapa de análisis del comité, pasando el análisis íntegro en todas sus fases por parte de la Cámara de los Comunes.[136]

Como se pudo leer en párrafos anteriores, el Reino Unido tiene propuestas de regulación; sin embargo, carecen de coercitividad y, por ello, producen falta de análisis concretos sobre el cumplimiento, efectividad y casos de omisión al cumplimiento de una norma que regule aspectos de los objetos del Internet de las cosas.

Por consiguiente, realizar evaluaciones sobre las políticas públicas a seguir y las posibles reformas a estas disposiciones quedan sujetas a reportes sobre si se siguen los parámetros del Código o de las consultas públicas que aportan la visión de los diferentes sujetos obligados.

4.3 Estados Unidos

Dentro del universo de intentos de regulación de los objetos del *IoT*, se encuentran dos estados de uno de los países norteamericanos. Los Estados Unidos de América han implementado disposiciones con carácter coercitivo que permiten regular diversos aspectos sobre la ciberseguridad de este tipo de objetos.

De esta forma, se muestra que el Internet de las cosas es necesario para el desarrollo de diferentes actividades económicas en ese país, abarcando las

[135] *Idem.*
[136] UK Government, *Bill passage.* Recuperado el 26 de junio de 2022, de: https://bills.parliament.uk/bills/3069

distintas partes de la cadena de producción, el uso de los usuarios de este tipo de tecnología, etcétera.

La primera en aparecer es la disposición normativa SB-327 del estado de California, conocida como “Ley California” sobre dispositivos del *IoT*. Siguiendo sus pasos, aparece la ley HB 2395 del estado de Oregon; por último, surge la ley de mejora de la ciberseguridad, la cual tiene un ámbito federal, pero en lo que se refiere al *IoT* toma como referencia los estados antes mencionados.

4.3.1 Ley California

La regulación del Internet de las cosas implica la coordinación de los diferentes actores de esta tecnología. No se puede emitir una regulación por parte del gobierno de un país o de un organismo regulador sin considerar el impacto tanto positivo como negativo que implica este tipo de normatividad en las diferentes áreas que convergen con el *IoT*.

Debido a esto, la normatividad en materia del Internet de las cosas no ha sido un tema fácil de implementar, comenzando desde su discusión y las diferentes reformas en el sistema normativo que se tendrían que realizar.

No obstante, uno de los pasos más adelantados para su regulación se dio en el año 2018 con el proyecto de Ley del Senado del estado de California en los E.U.A.; versa sobre la obligatoriedad de establecer protocolos de seguridad en los dispositivos *IoT*. Sin embargo, su entrada en vigor se dio hasta el 1° de enero de 2020, por lo que el tiempo para llevar a cabo un análisis de los efectos de esta ley es corto pues solamente han pasado alrededor de 2 años desde su vigencia.

Los sujetos obligados desde la aprobación de la ley tuvieron un plazo relativamente corto para implementar los requerimientos que establece la misma, teniendo los documentos y las pruebas necesarias para garantizar esa seguridad razonable.

Esta ley obliga a los fabricantes, o las personas que contratan para fabricar en nombre de otra los dispositivos que se vendan o se ofrezcan en el estado de

California, a implementar características de seguridad razonable. Dichas características son:

- Que sean adecuadas a la naturaleza y función del producto.
- Apropiadas a la información que pueden recopilar, contener o transmitir.
- Que sean diseñadas para proteger el dispositivo y cualquier información contenida en el mismo del acceso no autorizado, destrucción, uso, modificación o divulgación.[137]

También establece lo que se debe considerar como seguridad razonable, siendo dos puntos los más relevantes:

- Tener una contraseña preprogramada única para cada dispositivo fabricado.
- El dispositivo debe contener una característica que requiera que un usuario genere un nuevo medio de autenticación antes de conceder acceso al dispositivo por primera vez. [138]

De la lectura de la ley, la conceptualización de seguridad razonable es ambigua y no es limitativa, por lo que queda a la interpretación de otras instituciones o de los mismos obligados. Las cuestiones de seguridad se llegan a incluir desde el arranque del dispositivo o las comunicaciones seguras, incluso hasta el sistema de detección de intrusiones.[139] Esto es un problema para hacer efectiva la ley y en determinado momento castigar posibles violaciones.

Para la interpretación de este punto en específico se ha utilizado el Informe de Violación de Datos de California del año 2016 realizado por la Fiscal General de

[137] Bourke Rowland law, *California IoT Law* (Ley sobre IoT de California). Recuperado el 13 de diciembre de 2021, de: https://www.bourkerowland.com/california-iot-law
[138] Robinson & Cole LLP, IoT Manufacturers – What You Need to Know About California's IoT Law (Manufactura del Internet de las Cosas, ¿Qué necesitas saber acerca de la ley sobre el Internet de las Cosas de California?). Recuperado el 17 de diciembre 2021, de: https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law
[139] *Idem.*

California Kamala Harris. Sin embargo, esto aún resulta insuficiente para atender y resolver el conflicto que genera la falta de delimitación de este término.

En esta ley también se especifica el ámbito personal de aplicación; es decir, los sujetos que ofrecen estos dispositivos. No obstante, aunque pareciera también incluir a las tiendas electrónicas o los mercados que venden estos dispositivos, lo cierto es que las excluye y no las hace responsables por comercializar dichos productos, dejando al fabricante y al socio de este la obligación de dar cumplimiento a la misma.

Por último, la delimitación más importante de esta norma es aquella que refiere al ámbito de aplicación de esta ley, limitándose únicamente a los dispositivos conectados a Internet, siendo aquellos aparatos tecnológicos u otros objetos físicos que sean capaces de conectarse, directamente o indirectamente, y les sea asignada una dirección *IP*.[140]

Dentro de esta norma existen otras exenciones de responsabilidad además a las señaladas en párrafos anteriores. Una de ellas tiene que ver con el caso en el que el usuario instale un *software* diferente al preinstalado; esto podría causar problemas de ciberseguridad. Sin embargo, esto no implica que esté prohibida la modificación o la instalación de material diferente al preinstalado; es decir, se le pueden añadir herramientas, pero no se puede cambiar aquellas que fueron preinstaladas por el fabricante, siendo esta una excluyente de responsabilidad.

Sobre las exenciones de responsabilidad respecto a los fabricantes de dispositivos del *IoT*, se encuentran aquellos que se enfocan en la atención médica u otras organizaciones sujetas a la Ley de Portabilidad y Responsabilidad del Seguro Médico de los Estados Unidos de América.

La base de esta Ley es la ciberseguridad, más que los aspectos técnicos para la fabricación de estos productos. Es por eso que los huecos legales son en ocasiones cubiertos por otras disposiciones tanto jurídicas como informativas, pero

[140] Robinson & Cole LLP, *op. cit.*

sienta las bases de lo que se debe tener en cuenta al tratar de regular la ciberseguridad de los dispositivos del *IoT*.

4.3.2 Ley Oregon

Otro de los estados que está llevando a cabo una regulación del *IoT* en su territorio es el estado de Oregon en los Estados Unidos de América.

La ley es la HB 2395 de Oregon, que entró en vigor en 2020. Debido a la proximidad con la ley de California, es evidente su influencia en su creación.

Aunque esta ley puede aplicarse a los dispositivos del *IoT*, no tiene el mismo enfoque puesto que se concentra en aquellos dispositivos del Internet de las cosas de consumidores y no en todos los tipos de dispositivos como lo hace la Ley de California.[141] Es decir, está dirigida a aquellos dispositivos que se utilizan principalmente para fines personales, familiares o domésticos, a los que se les agrega una dirección *IP* o un número para una conexión de corto alcance como lo es la conexión *Bluetooth*.

Otra diferencia con la Ley de California es la exclusión de responsabilidad en la instalación de *softwares* que no son los ofrecidos por el fabricante. En la Ley de Oregon se agrega el término de 2*softwares* que no son aprobados por el fabricante", por lo que pueden existir *softwares* que no son del fabricante, pero que sí son aprobados por este.

Para los fines del presente trabajo, la Ley de Oregon es el principal documento normativo a destacar por el objetivo al cual se enfoca; sin embargo, contiene aspectos que son idénticos casi en su totalidad a los que se encuentran en la Ley de California. Es por eso que la Ley California es considerada en esta investigación como el ejemplo de una regulación del *IoT* con intenciones a impulsar la correcta legislación de este campo pues existen actualizaciones constantes en la tecnología que impiden tener una regulación que esté a la vanguardia.

[141] Dugan, Colin, *California and Oregon's IoT Cybersecurity Law: The 7 Key Points Explained* (Ley de ciberseguridad de IoT de California y Oregon: los 7 puntos clave explicados), 2020. Recuperado el 22 de mayo de 2022, de: *https://bgnet.works/california-and-oregons-iot-cybersecurity-law-the-7-key-points-explained/*

4.3.3 Regulación Federal de los Estados Unidos de América

En el año 2019, el gobierno federal de los E.U.A. promovió, por medio del Comité de Supervisión y Reforma de la Cámara de Representantes, el proyecto de ley denominado *IoT Cybersecurity Improvement Act*[142] (Ley de Mejora de la Ciberseguridad de los dispositivos del Internet de las cosas, por su traducción en español). Planteaba que el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) emitiera de forma segura regulaciones para el desarrollo, configuración y administración de los dispositivos del Internet de las cosas .

Esta ley federal se diferencia de las disposiciones locales antes mencionadas; en su caso, quien quisiera vender dispositivos de este tipo al gobierno federal, tendría que diseñarlos y fabricarlos de acuerdo a las disposiciones planteadas por la NIST.

Esta propuesta tenía como base el informe interno de NIST 8259D, el cual aborda la identificación de dispositivos en productos de consumo de forma directa. Establece que estos aparatos deben identificarse de forma lógica, siendo las entidades autorizadas la únicas capaces para cambiar la configuración del dispositivo; el interfaz de los dispositivos debe estar bloqueado y, por último, los fabricantes deben emitir actualizaciones al *software* de forma segura.

Para 2021, se ha implementado una orden ejecutiva que propone añadir programas piloto para promover la educación sobre la seguridad de estos dispositivos y la implementación de un programa para etiquetar aquellos que sigan los parámetros de seguridad establecidos.

4.4 Latinoamérica

En Latinoamérica no existen regulaciones sobre los dispositivos del *IoT*. El objetivo de este tipo de aparatos tecnológicos carece de importancia; es decir, si son objetos para el hogar, la industria, para ciudades inteligentes, para la

[142] American Goverment, *IoT Cybersecurity Improvement Act* (Ley de Mejora de la Ciberseguridad de los dispositivos del internet de las cosas). Recuperado el 23 de junio de 2022, de: https://www.techtarget.com/searchsecurity/feature/IoT-Cybersecurity-Improvement-Act-calls-for-deployment-standards

agricultura, etcétera. Esto traza una diferencia con las regulaciones obligatorias y no obligatorias que tienen como punto de partida los objetos dirigidos al hogar.

No obstante, se han implementado diversas reformas o políticas públicas en aras de mejorar el acceso a esta tecnología y, por ende, mejorar las regulaciones sobre este tipo de objetos.

Por consiguiente, en líneas posteriores se mencionan actividades que han implementado algunos países latinoamericanos para comenzar a pensar en la regulación de los objetos del Internet de las cosas.

4.4.1 Brasil

Hay que destacar el papel de Brasil en la regulación de los dispositivos del *IoT*. Se ha logrado establecer el Plan Nacional de Internet de las Cosas, cuyo objetivo es aumentar la competitividad del sector de telecomunicaciones.

Dentro de las adopciones tomadas se encuentra la de poner a las empresas que se dedican a este sector en un régimen especial de tributación, así como facilitar los requerimientos para establecer la expansión de la banda ancha.[143]

4.4.2 Chile

Al igual que Brasil, el país chileno ha implementado varias iniciativas para que se comiencen a regular los diferentes aspectos del *IoT* en diferentes iniciativas y políticas públicas.

Se ha mejorado la infraestructura de las Tecnologías de la Información y Comunicación, la adopción de los diferentes productos del *IoT* por parte de las empresas y la capacidad de innovación.

Existen diversas leyes en el ámbito digital que pueden aplicarse a este tipo de objetos. Algunas de ellas son:

[143] Larocca, Nicolás, *Tras cuatro años, Brasil decretó la creación del Plan Nacional de IoT,* en Telesemana.com, 2019. Recuperado el 23 de- junio- de 2022, de: https://www.telesemana.com/blog/2019/06/27/tras-cuatro-anos-brasil-decreto-la-creacion-del-plan-nacional-de-iot/

- Ley No. 20.453. Sobre el principio de neutralidad de la red.[144]
- Ley No. 18.168[145] y la Ley 19.724.[146] Sobre las Telecomunicaciones en general.
- Ley 19.628[147] y Ley 20.575.[148] Sobre protección de datos personales.

[144] Ley 20453, *Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet*, 2010, Chile. Recuperado el 23 de junio de 2022, de: https://www.bcn.cl/leychile/navegar?idNorma=1016570&buscar=NEUTRALIDAD%2BDE%2BRED

[145] Ley No. 18.168, *General de Telecomunicaciones*, 2014, Chile. Recuperado el 23 de junio de 2022, de: https://www.informatica-juridica.com/anexos/ley-no-18-168-general-de-telecomunicaciones/

[146] Ley 19.724, *Del Fondo de Desarrollo de las Telecomunicaciones*, Ministerio de transportes y telecomunicaciones; subsecretaría de telecomunicaciones, Chile, 2001. Recuperado el 23 de junio de 2022, de: https://chile.justia.com/nacionales/leyes/ley-n-19-724/gdoc/

[147] Ley 19.628, *Sobre protección de la vida privada*, 1999, Chile. Recuperado el 23 de junio de 2022, de: https://www.hipervinculos.cl/wp-content/uploads/2015/11/Ley-19628.pdf

[148] Ley 20575, *Establece el principio de finalidad en el tratamiento de datos personales*, 2012, Chile. Recuperado el 23 de junio de 2022, de: https://www.bcn.cl/leychile/navegar?idNorma=1037366

CAPÍTULO 5. TEMÁTICAS A REGULAR DEL INTERNET DE LAS COSAS ENFOCADAS AL HOGAR

Para lograr una homogeneidad en la regulación de los dispositivos del *IoT*, hay que tener en cuenta a la tecnología, la economía y el derecho. Son las tres materias más importantes que convergen al querer regular el uso de esta herramienta.

Esto se debe a que convergen temas de conectividad, interoperabilidad, *softwares*, algoritmos, recopilación de datos e información, uso de aplicaciones móviles y derechos a ejercer derivados del uso de estos objetos, además de diferentes productores o distribuidores de los mismos, entre otros.

Debido a la transversalidad de los temas, la creación de una norma tendría diversos inconvenientes al momento de encajar en un tema en específico; destacan los fiscales, económicos, de jurisdicción internacional, de política exterior e interior, entre otros.

Como se desarrolló en el capítulo anterior, existen dos cuerpos normativos en los Estados Unidos de América que regulan cuestiones de protocolos de seguridad, siendo la Ley California y la Ley Oregon los estandartes de una regulación en esta materia.

Se aparta de esta mención el *Code of Practice for consumer IoT security* puesto que no es una regulación de los dispositivos del *IoT* que traiga aparejada la obligatoriedad, aunque es de suma importancia debido a que toma diversos aspectos que se deben considerar para emitir regulaciones sobre el Internet de las cosas.

Deja como resultado la iniciativa mencionada en capítulos anteriores, en la cual se propone la regulación de la seguridad y de la protección de los datos personales de los usuarios, así como la sugerencia de establecer un órgano que se encargue de supervisar el cumplimiento de la propuesta de regulación.

Sin embargo, como se indica en párrafos anteriores, no tiene el carácter obligatorio. Por lo tanto, limita el cumplimiento que puedan hacer los fabricantes de estos dispositivos.

En las leyes antes mencionadas se establecen protocolos de seguridad razonables los cuales carecen de límites y causan ambigüedad al momento de realizar sus interpretaciones. Esto se debe a que cada empresa comercializa la confiabilidad que le brinda a sus usuarios, invirtiendo en la investigación de diferentes formas para mejorar sus protocolos.

Es por eso que delimitar el tema de los objetos del Internet de las cosas y aislarlo de cuestiones externas permite establecer de forma teórica su regulación y facilita su aplicación de forma especializada a cada región del mundo. Esto sin importar las condiciones en las que se encuentre y desde una perspectiva económica hasta una política, entre otras que se enlacen con estos temas.

En el caso que atañe al presente trabajo de investigación, se tomará como base una regulación enfocada en el Internet de las cosas para el hogar. Este tipo de dispositivos se encuentran al alcance de las personas físicas y, por ende, se encuentran más dispositivos que servirían de fácil aplicación del contenido de esta propuesta.

Además, las interacciones entre las personas y los dispositivos de esta categoría (hogar) tienen una alta frecuencia, como el uso de televisores con acceso a Internet. El ENDUTIH 2020 demuestra que el 22.2 % de las personas se conectaron a través de estos dispositivos a una red de Internet, por lo que el uso de las *Smart Tv* se ha vuelto parte de la vida de los mexicanos.

Para señalar de forma concisa los aspectos relevantes al momento de querer regular el Internet de las cosas enfocadas al hogar es importante atender a las diferentes partes que se observan al querer realizar la propuesta de contenido de una norma en materia de los objetos del *IoT*:

- Actores en la ley.
- Autoridad Responsable.
- Cuestiones de privacidad.

5.1 Actores en la ley

Es por eso que para lograr una convergencia de estas materias es necesario identificar a los participantes que intervendrían en una posible regulación de los objetos del *IoT*.

Moisés Barrio, en su libro Internet de las Cosas, señala a los fabricantes, proveedores de plataformas, desarrolladores de *apps* e integradores como los sujetos involucrados.[149]

I.1 Fabricantes de dispositivos

Aquí engloba a los fabricantes del *hardware* para su funcionamiento y a los dispositivos físicos que se encargan de recopilar la información. En determinados casos, los fabricantes pueden crear el sistema operativo o modificar uno.[150]

I.2 Proveedores de Plataformas

En este caso, Moisés Barrios integra a los servicios de alojamiento y mantenimiento de las aplicaciones, como los servicios de la nube o servidores físicos locales. No obstante, señala que hay una problemática al no existir una estandarización de los métodos de transferencia de datos desde un dispositivo a otro o entre plataformas, puesto que cada fabricante define sus interfaces y formatos de datos.[151]

I.3 Desarrolladores de aplicaciones

Para que la recopilación de datos de los diferentes productos se dé de forma rápida y amplia, algunos proveedores usan aplicaciones móviles que son ofrecidas por empresas especializadas en la programación de estas herramientas.[152]

I.4 Integradores

[149] Barrio Andrés, Moisés, *op. cit.*
[150] *Idem.*
[151] *Idem.*
[152] *Idem.*

Este autor señala a las empresas que comercializan directamente la conjunción de los elementos antes mencionados para el beneficio de los usuarios finales.[153]

A mi parecer, esta delimitación de los sujetos involucrados o participantes carece de un elemento de suma importancia que son los usuarios. Si bien no participan en la fabricación de estos dispositivos, son el elemento más importante debido a que la regulación de los productos tiene un impacto directo en su persona.

Es por eso que al momento de querer realizar una norma jurídica sobre el Internet de las cosas se debe tener en cuenta al usuario, siendo parte fundamental de la cadena de uso de este tipo de tecnología.

No obstante, el usuario carece de un rol fundamental en la cadena antes mencionada puesto que la principal dirección de la norma es hacia los participantes de este tipo tecnología que logran que los productos estén a disponibilidad del usuario. Así, se establecen obligaciones para los participantes antes mencionados, mas no para los usuarios pues desprenderían, en su caso, algunos derechos en su beneficio.

Como se mencionará más adelante, es necesario establecer las exenciones de responsabilidad de las partes, debido a que esto facilitará el grado de responsabilidad y el responsable específico por el manejo deficiente de diversos aspectos que se deben incluir en la norma.

5.2 Autoridad Responsable

Para que exista una disposición normativa sobre el *IoT*, es preciso que sea aprobada por el órgano legislativo; es el facultado para discutir y aprobar una ley que tiene como consecuencias diferentes reformas a leyes específicas, y en particular, a la Constitución Política Federal. Además, al ser una norma enfocada únicamente en materia del Internet de las Cosas, tiene que ser supervisada por algún organismo autónomo que garantice su debido cumplimiento.

[153] *Idem.*

Esto sin olvidar que posterior a su posible aprobación, con los votos necesarios dependiendo del caso, de si es una reforma constitucional y/o la creación de una ley; el presidente tiene que promulgar y enviar al DOF el decreto para su publicación, salvo que tenga observaciones a dicho decreto.

El Instituto Federal de Telecomunicaciones, como Organismo Autónomo Constitucional, es el mejor posicionado para llevar a cabo este cumplimiento. Dentro de sus facultades resalta la regulación y supervisión de los servicios de telecomunicaciones, esto en conformidad con el artículo 28 de la Constitución Federal.

De las obligaciones derivadas de dicho instrumento normativo también se incluye la regulación y supervisión, entre otras actividades, de las redes y prestación de los servicios de telecomunicaciones. Por lo tanto, ese instituto es el autorizado por disposición Constitucional a llevar acabo los estudios y la posterior regulación de los dispositivos del *IoT*, comenzando por los utilizados en hogares, en razón de la masiva accesibilidad con la que se cuenta y el avance tecnológico del día a día.

De esta forma, es la institución especializada que regula los diferentes aspectos que rodean a los dispositivos del Internet de las cosas. A la fecha, el IFT se ha encargado de mostrar los avances de esta tecnología mediante estudios y proyectos futuros que dan a conocer el conocimiento necesario sobre la importancia del *IoT*.

Siguiendo la Hoja de Ruta 2021-2025 del IFT[154], se destaca la estrategia 3.1: Promover la seguridad, confianza e innovación para el desarrollo del ecosistema digital, en la cual una de sus acciones es desarrollar estudios sobre potenciales riesgos de ciberseguridad del desarrollo de redes del Internet de las cosas.

Esta planeación se ve reflejada en el estudio denominado 2Pronósticos de los Servicios de Telecomunicaciones"[155], en el cual se señala al Internet de las cosas como uno de los servicios móviles con alto crecimiento en los últimos años teniendo estimaciones de uso para 2024 de 25,440 mil millones de estos aparatos,

[154] IFT*, Estrategia IFT 2021- 2025, Hoja de Ruta*. Recuperado el 20 de noviembre de 2021, de: http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025.pdf
[155] *Idem.*

de los cuales el 48% son objetos electrónicos de consumo. Dentro de los mismos se encuentran los diferentes productos que se hay en el hogar como refrigeradores, relojes, pantallas inteligentes, etcétera.

En el Plan Anual de Trabajo 2022 del IFT, se tienen establecidos dos proyectos de suma importancia para comenzar a mirar a la regulación de estos dispositivos como el presente de las conexiones a Internet. Estos son: la elaboración de un código de mejores prácticas para la ciberseguridad del *IoT* y un catálogo de dispositivos *IoT*.

Así, se muestran las investigaciones sobre el tema, además de la realización de actividades en favor de la población; se pone a disposición del público en general una herramienta y un documento que permiten dar a conocer los diferentes aparatos tecnológicos que forman parte del Internet de las cosas. Se indican las ventajas, las amenazas, así como los riesgos y vulnerabilidades que provocan el uso de estos dispositivos con la intención de obtener un consumo inteligente sobre ellos.

De esta manera, se señalan diversas acciones estratégicas al momento de regular el tráfico de datos al hacer uso de los diferentes dispositivos del *IoT*, entre las que destacan la colaboración entre instituciones involucradas y la aportación de recomendaciones técnicas y de mejores prácticas asociadas al control y gestión de datos en las redes de telecomunicaciones.

En conclusión, el IFT tiene que ser la institución encargada de vigilar y promover el cumplimiento de las diferentes obligaciones en materia técnica que deben atender los actores de esta tecnología, con el fin de salvaguardar los diferentes derechos que tienen los usuarios de los objetos del *IoT*.

5.3 Cuestiones de privacidad

La recolección y manejo de datos forma parte del objeto del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), tal y como lo establece el artículo 6° de la CPEUM en relación con el artículo 16 del mismo ordenamiento.

La protección de datos personales se encuentra regulada por diversas disposiciones en esta materia, tanto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) como en la LFPDPPP, cuya supervisión está a cargo del INAI.

Por lo tanto, si se requiere ser más específico en el tema de los dispositivos del Internet de las cosas, se necesita realizar una innovación a estas disposiciones para que abarquen temas de protección de datos recopilados por dispositivos del *IoT*.

Esto se debe a que la ley fue diseñada para la recopilación de datos de forma general; es decir, tiene menciones sobre la captura de datos de forma digital. No obstante, al ser una disposición jurídica no especializada en la recopilación de datos por medios digitales, pasan de lado cuestiones como el uso de la nube o la forma en que se pueden transferir datos de un dispositivo a otro sin que se cambie de persona.

Por consiguiente, la creación de una disposición normativa que se enfoque en la recopilación, tratamiento, compartición y eliminación de datos por parte de las personas que utilizan dispositivos del Internet de las cosas a fin de ofrecer diferentes tipos de servicios o complementarlos, es necesaria para garantizar la protección de los usuarios de estas herramientas.

La recolección de datos se lleva a cabo por medio de los dispositivos del *IoT*, obteniendo datos sobre patrones de hábitos en el uso de estos objetos, no sólo de las personas titulares sino también de familiares o personas cercanas. Son patrones de sumo interés para las empresas pues permiten la segmentación de la información de cada persona al recolectar datos de una misma persona por diferentes medios sin que hayan dado su autorización y así usarse en cuestiones publicitarias de forma personalizada o para el simple almacenamiento.

Moisés Barrio señala que “las tareas de garantizar le seguridad de los datos y la protección de la privacidad se vuelven más difíciles cuando la información se

multiplica y se comparte cada vez más ampliamente en todo el mundo, como sucede en el *IoT*".[156]

Para disminuir esta transferencia de información, el artículo 6° de la LFPDPPP establece diversos principios sobre los que se deben basar las recolecciones de datos, siendo los siguientes: "(…) licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (…)".[157]

Por lo regular, la recolección de datos incluye datos personales como el nombre real del usuario o nombre de usuario, cuenta de correo electrónico, alguna contraseña personalizada para el registro y alguna otra cuenta que permita vincular más cuentas al dispositivo.

Sin embargo, esto puede variar dependiendo del medio por el cual se recolectan los datos; ya sea por medio de *apps* móviles, sitios web externos a la memoria del dispositivo o directamente desde el dispositivo *IoT*. Esto se debe a que por medio de *apps* móviles y sitios web se puede acceder a más datos puesto que la mayoría de los datos son almacenados en la nube y la capacidad de almacenamiento y de recepción es más amplia.

Como se mencionó antes, se corre el riesgo de compartir los datos personales de una persona sin el consentimiento de que se estén dando esos datos. Aquellos que son datos personales sensibles afectan la esfera íntima de la persona a quien se le recolectan, como lo son las preferencias en las búsquedas de contenido en Internet que pueden facilitar la identificación de una persona.

En conclusión, en cuanto a la seguridad que proporcionan los sujetos participantes en la fabricación, distribución y venta de los dispositivos del Internet de las cosas que se utilizan principalmente con fines hogareños y en general con los diferentes objetos del *IoT*, si no se van tomando en cuenta los diferentes aspectos que involucran a este tipo de tecnología se podría caer en retrasos al

[156] Barrio Andrés, Moisés, *op.cit.*
[157] Ley Federal de Protección de Datos Personales en Posesión de Particulares, D.O.F., 5 de julio de 2010. Recuperado el 20 de enero de 2022, de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

querer regular un área que está en constante cambio como lo es la tecnología aplicada a la vida cotidiana.

Por lo tanto, una reforma a la ley implicaría modificar ciertos aspectos que aplican a los demás sujetos obligados de esta ley; esto podría causar confusiones al momento de aplicarla. Es por eso que se reafirma la propuesta de creación de una disposición que englobe los aspectos técnicos y sustantivos de la protección de datos personales puesto que ésta se enfocaría en la recopilación de datos por medio de dispositivos del *IoT*. Se usaría como base la LFPDPPP, pero ahondando y siendo más específico en temas de protocolos de protección de datos o la transferencia entre dispositivos sin que en ellos varíe el recolector de datos.

De este modo, la propuesta de reforma para colocar al IFT como órgano autónomo supervisor implica diferentes modificaciones tanto a la LFTyR como a la CPEUM, en razón de las facultades y obligaciones que le fueron otorgadas a ese instituto, siendo necesarias estas reformas para evitar las controversias por invasión de facultades.

Tal y como lo señala el Pleno de la Suprema Corte de Justicia de la Nación (SCJN), en la tesis de Jurisprudencia P./J. 44/2015 por medio de la cual indica las facultades del IFT, que a la letra señala:

> **“INSTITUTO FEDERAL DE TELECOMUNICACIONES (IFT). CARACTERIZACIÓN CONSTITUCIONAL DE SUS FACULTADES REGULATORIAS**. Del listado de facultades previstas en el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos se advierte que el IFT no tiene asignada una función jurídica preponderante, sino que conjunta las tres clásicas: la de producción de normas generales, la de aplicación y la de adjudicación, siendo la primera la que corresponde propiamente a su función regulatoria, respecto de la cual en la norma constitucional hay referencia textual a dos tipos: 1) internas; y, 2) externas. Ahora bien, el precepto indicado, en su párrafo vigésimo, fracción III, establece que aquél emitirá su propio estatuto orgánico, esto es, producirá regulación interna; por su parte, la fracción IV del párrafo y artículo aludidos establece que **podrá emitir disposiciones administrativas de carácter general exclusivamente para cumplir su función regulatoria en el sector de su competencia, es decir, expedirá**

regulación externa. Ahora bien, **estas normas regulatorias tienen un límite material, por el cual sólo puede emitir normas generales en el ámbito de competencias en el que tiene poderes regulatorios, ya que la norma constitucional establece: "exclusivamente para el cumplimiento de su función regulatoria en el sector de su competencia"; por tanto, para determinar cuál es su sector de competencia es necesario precisar el criterio rector de su ámbito material de actuación, lo que prevén los párrafos décimo quinto y décimo sexto del artículo 28 mencionado en tres rubros: a) El desarrollo eficiente de la radiodifusión y las telecomunicaciones; b) La regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6o. y 7o. de la Constitución; y, c) En materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.** Por otra parte, sus facultades regulatorias tienen un límite jerárquico, pues el artículo 28 citado precisa que las disposiciones administrativas de carácter general que puede emitir dentro del sistema de fuentes jurídicas se encuentran por debajo de la Constitución y, en un peldaño inferior, también debajo de las leyes emitidas por el Congreso de la Unión. Así, el órgano referido tiene la facultad constitucional de emitir disposiciones administrativas de carácter general exclusivamente para cumplir su función regulatoria en el sector de su competencia, constituyendo sus disposiciones generales una fuente jurídica jerárquicamente inferior a las leyes emitidas por el Congreso con fundamento en el artículo 73, fracción XVII, de la Constitución Federal, a cuyos términos debe ajustarse dicho órgano constitucional autónomo, en términos del invocado artículo 28.”[158]

*Énfasis añadido

Derivado de esa tesis, que tuvo como origen la Controversia Constitucional 117/2014, se entiende que para lograr la propuesta planteada anteriormente es necesaria una reforma tanto a la LFTyR como a la Constitución para ampliar, de

[158] Tesis P./J. 44/2015, *Pleno de la Suprema Corte de Justicia de la Nación (SCJN)*, 2015. Versión electrónica recuperada el 22 de octubre de 2021, de: https://sjf2.scjn.gob.mx/detalle/tesis/2010670

forma limitativa a esta materia, las facultades sobre la supervisión en materia de protección de datos.

Para lograr satisfacer estas facultades de supervisión en materia de Protección de Datos, es necesario hacer una reforma en esta materia para delimitarla lo más posible hacia el Internet de las cosas. Esto sin quitarle facultades al INAI, sino estableciendo facultades coincidentes, pero aplicadas a diferentes materias. En cuanto a que la única injerencia del IFT en protección de datos sea en el área del *IoT*.

Esta necesidad de supervisión por parte del IFT se justifica en razón de la tesis emitida por el pleno de la SCJN con número P./J. 43/2015, la cual señala a la letra:

> **INSTITUTO FEDERAL DE TELECOMUNICACIONES (IFT). ES UN ÓRGANO CONSTITUCIONAL AUTÓNOMO CON UNA NÓMINA COMPETENCIAL PROPIA OPONIBLE AL RESTO DE LOS PODERES DEL ESTADO, QUE PUEDE UTILIZAR AL MÁXIMO DE SU CAPACIDAD PARA REALIZAR SUS FINES INSTITUCIONALES.** Con motivo de la reforma a la Constitución Política de los Estados Unidos Mexicanos publicada en el Diario Oficial de la Federación el 11 de junio de 2013, se introdujo una serie de contenidos normativos novedosos en su artículo 28, entre ellos, la creación y regulación del IFT como un nuevo órgano autónomo, con una nómina competencial propia y diferenciada respecto de los otros poderes y órganos previstos en la Norma Fundamental, de la cual deriva que no tiene asignada una función jurídica preponderante, sino que conjunta las tres clásicas: la de producción de normas generales, la de aplicación y la de adjudicación. Ahora bien, una de las implicaciones lógicas de lo anterior es que dicho órgano, al contar con competencias propias, puede oponerlas a los tres Poderes de la Unión en que se divide el poder público, según el artículo 49 de la Constitución Federal, en un ámbito material delimitado constitucionalmente definido, consistente en el desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en la propia Ley Suprema y en los términos que fijen las leyes. En otras palabras, con independencia de lo que hagan los otros Poderes, el órgano regulador tiene un ámbito de poder propio que

> puede utilizar al máximo de su capacidad para realizar sus fines institucionales, como consecuencia de ser titular de facultades constitucionales propias.[159]

Con la cual, con el objetivo de la realización de las actividades necesarias a fin de dar pleno cumplimiento a los fines para los que fue creado el instituto, puede usar el máximo de su capacidad; es decir, sin transgredir las facultades de los demás poderes y de otros organismos constitucionales autónomos y apegado al marco normativo el IFT puede realizar cualquier actividad necesaria para cumplir sus fines institucionales.

Como órgano autónomo encargado de la promoción y vigilancia de las telecomunicaciones, es preciso que tenga facultades para supervisar el cumplimiento de una norma que proporcionará certeza tanto técnica como jurídica de uno de los temas que al día de hoy se desarrolla a pasos agigantados, tal y como se describió en el presente trabajo.

Reiterando la intención de garantizar y evitar transgresiones a las facultades del INAI, se tendrían que colocar mecanismos de participación en la supervisión de esta norma. Lo podrían ser opiniones previas vinculantes para obtener la participación de este órgano autónomo o participaciones considerables al momento de emitir la regulación planteada anteriormente.

Y así se podrá dar certeza a los participantes en la fabricación, distribución y uso de los objetos del Internet de las cosas para garantizar el uso adecuado de forma regulada de este tipo de tecnología.

[159] Tesis P./J. 43/2015, *emitida por el pleno de la SCJN*, 2015. Versión electrónica recuperada el 22 de 22 de octubre de 2021, de: https://sjf2.scjn.gob.mx/detalle/tesis/2010671

CONCLUSIONES

A lo largo de la presente investigación, el tema del Internet de las cosas enfocadas al hogar se ha segmentado para una mejor comprensión global. Se buscó destacar los aspectos más importantes en los que se debe poner atención y con ello, regular el tema. Al vincular varios tópicos, desde lo económico y legal hasta lo técnico, fue necesario segmentar dicha cuestión desde sus raíces para comprender lo que implica.

A pesar de que los temas económicos, técnicos y jurídicos son los más relevantes, en el presente trabajo no se abordaron completamente los primeros dos debido a que no son el objeto principal. Sin embargo, esto no implicó que se dejaran a un lado; se mencionaron los aspectos de esos dos temas de forma superficial con la intención de tocar el tema jurídico y servir de complemento para el abordaje técnico y económico.

De esta investigación se obtiene una conclusión resumida en tres puntos:

I. El Internet es una herramienta que no se puede regular, pero el *IoT* de las cosas, sí.

Pareciera que los diferentes gobiernos del mundo se niegan al comienzo de la regulación del Internet. No obstante, si se comienza a desentrañar lo que implica regular el Internet podríamos darnos cuenta que los niveles en los que se puede dividir, señalados así para facilitar su explicación, muestran lo amplio que es y el manejo superficial que se tiene del tema.

La mayoría de los servicios digitales hacen uso del *Surface Web* y de la *Deep Web,* tales como redes sociales, cuentas de servicios de *streaming*, cuentas para controlar los diferentes objetos del *IoT*, entre otros usos.

Dejando de lado a la *Dark Web*, una de las franjas del Internet que se utiliza para ocultar actos delictivos o manejo de datos gubernamentales de alta seguridad, querer controlar el intercambio de datos en esta zona del Internet es sumamente complicado. Para acceder a la *Deep Web* se utilizan IP privadas y con diferentes candados de seguridad que limitan la entrada a personas que conocen la forma de hacerlo.

Lo anterior no quiere decir que el Internet de las cosas no se pueda comenzar a regular. El objeto de esto no es controlar el Internet, sino poner ciertos controles de seguridad a los objetos que se conectan a él.

Como se demostró en el presente trabajo, existe la posibilidad de establecer controles jurídicos a los objetos del Internet de las cosas al momento de recopilar y tratar los datos personales de los usuarios. Esto sin dejar de lado la posibilidad de establecer los controles técnicos en cuanto a los protocolos mínimos que deben tener estos objetos.

Para comenzar a regular este tema, es preciso conocer los actores que intervienen en la cadena de producción de estos objetos, y que a su vez los convierte en actores de la posible norma (Fabricantes de dispositivos, proveedores, desarrolladores, integradores y usuarios). Con esto se logra definir las responsabilidades que tiene cada uno y los derechos que derivan de esta norma.

II. La importancia del Internet de las cosas en nuestras vidas.

Los objetos del Internet de las cosas han logrado en los últimos tiempos un incremento en su uso, partiendo desde los dispositivos móviles como los celulares o laptops hasta objetos que en su momento no se consideraron como parte del *IoT* (las *Smart Tv*).

Incluso se ha llegado a objetos de un uso tan común que ahora se conectan a Internet para hacer nuestras actividades cotidianas más fáciles. Un ejemplo de ello son los refrigeradores que miden la cantidad de comida que se introduce en su interior, así como una posible fecha de caducidad; de igual forma, contienen lectores que permiten saber el contenido que hay en ellos y así facilitar “el hacer la despensa” sin tener que abrir el refrigerador. Esto gracias a las aplicaciones móviles que se comunican con nuestro *Smartphone*.

Cada día más objetos se están conectando a Internet; desde refrigeradores, como lo antes mencionado, hasta objetos en los que la cantidad de datos recopilada es menor, sin restarle su importancia. Lo son los focos, esparcidores de agua, contactos de electricidad, apagadores, relojes, pulseras, licuadoras o hasta tostadoras, cuyo objetivo es facilitar nuestras actividades del diario. A ellos se les

otorgan pequeños datos personales como rutinas y cuestiones de nuestra salud que requieren protocolos de seguridad con altos estándares; sin embargo, la procedencia de estos dispositivos no siempre garantiza que se utilizan protocolos de seguridad con altos estándares.

III. El manejo de datos recopilados por los objetos del *IoT*.

El manejo de datos por parte de este tipo de objetos no tiene estándares mínimos de seguridad (salvo los impuestos en la Ley California, la Ley Oregon de Estados Unidos de América y el Código de prácticas de seguridad del consumidor en relación con el internet de las cosas). Por lo tanto, la mayoría de las compañías dejan a su discreción los protocolos que deben manejar los objetos que comercializan.

Es por eso que la hipótesis de proponer una disposición normativa que se enfoque en la recopilación de datos de forma específica por parte de estos objetos facilita su regulación. Debe tomarse en cuenta que la LFPDPPP no tiene los alcances técnicos para regular los protocolos necesarios a fin de manejar los datos personales de los usuarios, así como no tiene especificadas las partes que conforman la cadena de estos objetos.

FUENTES DE CONSULTA

- **Impresas**

ÁLVAREZ GONZÁLEZ DE CASTILLA, CLARA LUZ, *Telecomunicaciones y Radiodifusión en México*, Ciudad de México, Posgrado de Derecho de la UNAM, 2018.

BARRIO ANDRÉS, MOISÉS, *Internet de las cosas*, España, REUS, 2018, pp. 79-100.

CALDER, A. y S. WATKINS*, ISO27000 and information security: a combined glossary*, United Kingdom, it governance publishing, 2010.

DUFFY MARSAN, CAROLYN. *IAB Releases Guidelines for Internet-of-Things Developers,* en IETF Journal 11.1, Internet Engineering Task Force, 2015.

LASTRA LASTRA, JOSÉ MANUEL, *Rifkin, Jeremy, La Tercera Revolución Industrial*, en *Boletín Mexicano de Derecho Comparado*, Ciudad de México, v. 50, núm. 150, dic. 2017, pp. 1457-1462.

MENDOZA ENRÍQUEZ, OLIVIA ANDREA, Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento, en *Rev. IUS,* Puebla, vol.XII, núm.41, ene./jun. 2018, pp.267-291.

MILLER, IGNACIO DAVID, *La segunda Revolución Industrial*, Buenos Aires, Kapelusz, 2016.

ROEL, VIRGILIO, *La Tercera Revolución Industrial y la Era del Conocimiento*, Perú, 3a. ed., Fondo Editorial UNMSM, 1998.

- **Electrónicas**

AMERICAN GOVERMENT, *IoT Cybersecurity Improvement Act* (Ley de Mejora de la Ciberseguridad de los dispositivos del internet de las cosas). Recuperado el 23 de junio de 2022, de: https://www.techtarget.com/searchsecurity/feature/IoT-Cybersecurity-Improvement-Act-calls-for-deployment-standards

ARDUINO, ¿Qué es Arduino? Recuperado el 19 de julio de 2021, de: https://arduino.cl/que-es-arduino/

ALCARAZ, MARCELO, *Internet de las Cosas*, Universidad Católica, 2018. Recuperado el 12 de junio de 2021, de: *http://jeuazarru.com/wp-content/uploads/2014/10/Internet-of-Things.pdf*

AVG, ¿Qué es el streaming y cómo funciona?, 2018, Recuperado el 19 de septiembre de 2021, de: https://www.avg.com/es/signal/what-is-streaming.

CAMACHO CASTILLO, RAMIRO, Comisionado IFT, *IoT y 5G*. Recuperado el 20 de octubre de 2022, de: http://www.ift.org.mx/sites/default/files/conocenos/pleno/presentaciones/ramiro-camacho-castillo/ioty5g-sololectura.pdf

COMISIÓN INTERAMERICANA DE TELECOMUNICACIONES DE LA OEA, *Autenticación de usuarios*, *Boletín electrónico* no. 24, junio, 2006. Recuperado el 20 de enero de 2022, de: *http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp.*

DUGAN, Colin, *California and Oregon's IoT Cybersecurity Law: The 7 Key Points Explained* (Ley de ciberseguridad de IoT de California y Oregon: los 7 puntos clave explicados), 2020. Recuperado el 22 de mayo de 2022, de: *https://bgnet.works/california-and-oregons-iot-cybersecurity-law-the-7-key-points-explained/*

ELDER, Jeff, *Kevin Ashton nombró El Internet de las Cosas*, 2019. Recuperado el 19 de octubre de 2021, de: https://blog.avast.com/es/kevin-ashton-named-the-internet-of-things.

ESTRADA CORONA, ADRIÁN, Protocolos TCP/IP de Internet, Revista Digital Universitaria, V, núm.8, 2004, pp. 1-7. Recuperado el 13 de noviembre de 2021, de: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf.

FEDERAL NETWORKING COUNCIL, *Concepto de Internet, 1995*. Recuperado el 02 de agosto de 2021, de: https://www.cs.columbia.edu/~hgs/internet/definition.html

IIC, ¿Qué es el Big Data? Recuperado el 12 de enero de 2022, de: https://www.iic.uam.es/big-data/

INTERNATIONAL TELECOMMUNICATIONS UNION, SUIZA, *Harnessing the Internet of Things for Global Development*. Recuperado el 23 de junio de 2022, de: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf

INSTITUTO FEDERAL DE TELECOMUNICACIONES*, Segundo informe de privacidad de la información de los usuarios en el uso de servicios digitales*, 2021. Recuperado el 1 de febrero de 2022, de: ww.ift.org.mx/usuarios-y-audiencias/segundo-informe-de-privacidad-de-la-informacion-de-los-usuarios-en-el-uso-de-servicios-digitales

INSTITUTO NACIONAL DE CIBERSEGURIDAD, *Tu información en la nube*. Recuperado el 5 de febrero de 2022, de: *https://www.osi.es/es/tu-informacion-en-la-nube.*

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA (INEGI), *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares ENDUTIH (2021),* Comunicado de Prensa núm. 350/22, 4 de julio, 2022, pp. 1-19. Recuperado el 24 de noviembre de 2021, de: *inegi.org.mx.*

INTERNET SOCIETY, *IPv6*, Recuperado el 20 de febrero de 2021, de: *www.internetsociety.org/wp-content/uploads/2018/03/IPv6-Fact-Sheet-FinalWEB.pdf*

ITU, *5G-Quinta generación de tecnologías móviles*, 2019. Recuperado el 26 de febrero de 2021, de: *https://www.itu.int/es/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.*

LAINEZ IZAGUIRRE, CARLOS. *et al*., *Visión y prospectiva de la conectividad 5G*. Recuperado el 20 de septiembre de 2021, de: *http://www.ift.org.mx/sites/default/files/comunicacion-y-medios/otros-documentos/visionyprospectivadelaconectividad5g.pdf*

LAROCCA, NICOLÁS, *Tras cuatro años, Brasil decretó la creación del Plan Nacional de IoT*, en *Telesemana.com*, 2019. Recuperado el 23 de- junio- de 2022, de: https://www.telesemana.com/blog/2019/06/27/tras-cuatro-anos-brasil-decreto-la-creacion-del-plan-nacional-de-iot/

MASTER MARKETING, *¿Cuándo nació Internet? Historia y evolución,* 2019. Recuperado el 13 de marzo de 2021, de: https://www.mastermarketing-valencia.com/marketing-digital/blog/internet-historia-evolucion/

MICROSOFT, Cloud Computing. Recuperado el 22 de octubre de 2021, de: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

NIST, *About us*. Recuperado el 1 de enero de 2022, de: https://www.nist.gov/about-nist.

OEA, *Sobre la CITEL*. Recuperado el 20 de agosto de 2022, de: https://www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/citel/About/Details/category/citel/about-citel

PATRIZIO, ANDY, *Avast. IPv4 frente a IPv6: ¿en qué se diferencian?* Recuperado el 2 de noviembre de 2021, de: https://www.avast.com/es-es/c-ipv4-vs-ipv6-addresses#gref

POLSONETTI, CHANTAL, *Know the Difference Between IoT and M2M*, 2014. Recuperado el 20 de diciembre de 2021, de: www.automationworld.com/products/networks/blog/13312043/know-the-difference-between-iot-and-m2mdifference-between-iot-and-m2m>, [10-octubre-2021].

PORCELLI, ADRIANA MARGARITA, *Un hito jurídico sobre Internet de las Cosas: la Ley de California n° 327 del año 2018 vigente a partir del 1 enero del 2020*, 2020. Recuperado el 20 de noviembre de 2021, de: https://www.scielo.br/j/rdgv/a/NBksbsTGzh38X5NDLsWNntq/?lang=es

RIVER PUBLISHERS, *Advancing IoT Platforms Interoperability*, 2018. Recuperado el 20 de agosto de 2022, de: https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf.

ROSE, KAREN*, La Internet de las Cosas—Una breve reseña. Problemas y desafíos de un mundo más conectado,* Suiza, Internet Society, 2015, p.68. Recuperado el 12 de diciembre de 2021, de: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf.

SPRING PROFESIONAL, *Cómo afectan las aplicaciones móviles al Internet de las Cosas (IoT)*, España, 2021. Recuperado el 5 de noviembre de 2021, de: https://blogcandidatos.springspain.com/transformacion-digital/como-afectan-las-aplicaciones-moviles-al-internet-de-las-cosas-iot/

STALLMAN, R., *¿Puede confiar en su ordenador?*, Free Software Foundation, 2017. Recuperado el 20 de enero de 2022, de: https://www.gnu.org/philosophy/can-you-trust.es.html.

TERRAZAS BRIONES, PEDRO. *et al.*, *Análisis exploratorio de la comercialización de servicios de conectividad para IoT,* México, 2019. Recuperado el 30- de octubre- de 2021,de:https://www.bing.com/search?q=Análisis+exploratorio+de+la+comercialización+de+servicios+de+conectividad+para+IoT&qs=n&form=QBRE&msbsrank=6_6__0&sp=-1&pq=briones&sc=6-7&sk=&cvid=C8033F21832F4854A7C3AA90A4258163

TRIGO ARANDA, VICENTE, *Historia y evolución de Internet*, en *Manual formativo de ACTA*, núm.33, 2004, pp. 22-32. Recuperado el 22 de septiembre de 2021, de: https://dialnet.unirioja.es/servlet/articulo?codigo=5098592

UIT, *Requisitos comunes de la Internet de las cosas*, 2014. Recuperado el 14 de noviembre de 2021, de: https://www.itu.int/ITUT/recommendations/rec.aspx?rec=12169&lang=es

UK GOVERNMENT, *Code of Practice for consumer IoT security*, 2018. Recuperado el 23 de febrero de 2022, de: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security.

UK GOVERNMENT, *Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*, 2020. Recuperado el 24 de febrero de 2022, de: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.

UK GOVERNMENT, *Product Security and Telecommunications Infrastructure (PSTI*), 2021. Recuperado el 26 de junio de 2022, de: https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

UK GOVERNMENT, *Bill passage*. Recuperado el 26 de junio de 2022, de: https://bills.parliament.uk/bills/3069

UNIDAD DE POLÍTICA REGULATORIA, *Plan de Acciones en Materia de Ciberseguridad del IFT*, 2018. Recuperado el 12 de enero de 2022, de:http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesciberseguridad.pdf

UNIVERSIDAD INTERNACIONAL DE VALENCIA, *La seguridad de la información en la era digital*, 2021 Recuperado el 20 de diciembre de 2021, de: https://www.universidadviu.com/es/actualidad/nuestros-expertos/la-seguridad-de-la-informacion-en-la-era-digital.

VILA DE PRADO, ROBERTO, Consecuencias económicas y sociales de la cuarta revolución industrial y estrategias pensadas para la adopción de la actividad económica, en Revista Aportes de la Comunicación y la Cultura, núm. 26, junio 2019, pp. 89-108. Recuperado el 19 de agosto de 2021, de: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S230686712019000100010

YORK, DAN, *Ayúdanos a conseguir más sitios web disponibles con IPv6 para celebrar el 8.º aniversario del lanzamiento mundial de la IPv6* ,Internet Society, 2020. Recuperado el 20 de febrero de 2022, de: https://www.internetsociety.org/es/blog/2020/06/ayudanos-a-conseguir-mas-sitios-web-disponibles-con-ipv6-para-celebrar-el-8-o-aniversario-del-lanzamiento-mundial-de-la-ipv6/

- **Normas jurídicas:**

Ley 20453, Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet, 2010, Chile. Recuperado el 23 de junio de 2022, de: https://www.bcn.cl/leychile/navegar?idNorma=1016570&buscar=NEUTRALIDAD%2BDE%2BRED

Ley No. 18.168, General de Telecomunicaciones, 2014, Chile. Recuperado el 23 de junio de 2022, de: https://www.informatica-juridica.com/anexos/ley-no-18-168-general-de-telecomunicaciones/

Ley 19.724, Del Fondo de Desarrollo de las Telecomunicaciones, Ministerio de transportes y telecomunicaciones; subsecretaría de telecomunicaciones, Chile. Recuperado el 23 de junio de 2022, de: https://chile.justia.com/nacionales/leyes/ley-n-19-724/gdoc/

Ley 19.628, Sobre protección de la vida privada, 1999, Chile. Recuperado el 23 de junio de 2022, de: https://www.hipervinculos.cl/wp-content/uploads/2015/11/Ley-19628.pdf

Ley 20575, Establece el principio de finalidad en el tratamiento de datos personales, 2012, Chile. Recuperado el 23 de junio de 2022, de: https://www.bcn.cl/leychile/navegar?idNorma=1037366

Ley Federal de Telecomunicaciones y Radiodifusión, 2014, México. Recuperado el 17 de agosto de 2021, de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf