Interconectando Saberes
ISSN: 2448-8704
Año 6, No. 12
julio-diciembre de 2021
doi: https://doi.org/10.25009/is.v0i12.2721

Estudio de la legislación del Internet de las cosas en México

Alma Delia Otero Escobar [a]
Elsa Suárez Jasso [b]

Resumen – El internet de las cosas actualmente se ha proliferado de manera extraordinaria en el mundo. En México se han hecho esfuerzos por cubrir los aspectos legales que implica el uso de tan importante tecnología, tratando de solventar los vacíos existentes, ya que el avance de la tecnología ha rebasado el tiempo de legislación de las mismas. El objetivo de esta investigación es identificar el alcance de la legislación en el internet de las cosas partiendo de las generalidades, entorno, servicios y modelos de implementación en las organizaciones actuales. Se trata de una investigación documental y descriptiva, su principal contribución prevalece en la recopilación, interpretación de los aspectos legales del internet de las cosas aplicados a un caso real.

Palabras clave – Internet de las Cosas, Legislación, Usos.

Abstract – The internet of things today has proliferated in an extraordinary way in the world. In Mexico, efforts have been made to cover the legal aspects that imply the use of such important technology, trying to solve the existing gaps, since the advancement of technology has exceeded the time of their legislation. The objective of this research is to identify the scope of legislation on the Internet of Things based on the generalities, environment, services, and implementation models in current organizations. It is a documentary and descriptive investigation; its main contribution prevails in the compilation and interpretation of the legal aspects of the internet of things applied to a real case.

Keywords – Internet of Things, Legislation, Uses.

CÓMO CITAR
HOW TO CITE:

Otero-Escobar, A. D., Suárez-Jasso, E. (2021). Estudio de la legislación del Internet de las cosas en México. *Interconectando Saberes*, (12), 1-14 https://doi.org/10.25009/is.v0i12.2721

Recibido: 18 de junio de 2021
Aceptado: 5 de julio de 2021
Publicado: 20 de julio de 2021

[a] Universidad Veracruzana – Facultad de Contaduría y Administración, México. E-mail: aoteroe@gmail.com
0000-0001-9266-6587
[b] Universidad Veracruzana – Facultad de Contaduría y Administración, México. E-mail: elsuarez@uv.mx
0000-0002-7341-1068

INTRODUCCIÓN

El Internet de las Cosas o bien *Internet of Things*, define una red que no sólo conecta a las personas, sino también a los objetos que las rodean gracias al desarrollo de las tecnologías de la comunicación y el incremento de la velocidad de las conexiones de *Internet* y actualmente se identifica como papel clave en el desarrollo social, económico, educativo y cultural en el mundo.

Este artículo se presenta como un análisis al concepto y a los usos legales que plantea el internet de las cosas en adelante IoT en su acrónimo en inglés, se identifica la situación legal pasando por diferentes etapas que van desde el concepto, los proveedores, servicios que ofrecen, modelos de servicio, ventajas y desventajas, hasta llegar precisamente a la revisión de leyes, respecto a las medidas de seguridad y jurídicas que deben adoptarse con relación a este servicio tecnológico, aplicables al recibir /dar el servicio mencionado. Finalmente, se hace referencia a un caso práctico aplicable en México.

Los siguientes objetivos específicos son: Identificar al proveedor, así como al usuario; Comprender el desarrollo y funcionamiento del IoT.; Dar a conocer el marco legal en el que se desarrolla y desenvuelve el IoT; Identificar los riesgos de la seguridad y privacidad de los datos y finalmente: Comprender el compromiso legal ante el nuevo escenario que el IoT pone ante el usuario y el proveedor.

JUSTIFICACIÓN

Vermesan (2011) define al IoT como "una interacción entro lo físico y lo digital", se identifica como un conjunto de dispositivos y sensores electrónicos interconectados entre sí, en el que cada uno se encarga de medir recopilar y enviar los datos a un servidor centralizado o a la nube. Una vez que estos datos hayan sido recopilados son tratados y se extrae la información que se considera importante, los dispositivos de IoT pueden recibir del servidor o de la nube, una serie de instrucciones para realizar una determinada tarea.

El IoT ha tomado gran relevancia no sólo en el desarrollo tecnológico sino en aspectos que impactan directamente en la sociedad actual y en la economía de las organizaciones donde millones de dispositivos están siendo conectados entre sí a través de distintas redes de comunicación.

Según Gartner (2020) alrededor de 21,000 millones de cosas conectadas están en este momento recogiendo datos y realizando todo tipo de tareas. La mayoría son dispositivos de consumo, desde altavoces inteligentes hasta relojes y cerraduras de puertas. El resto sirve a los negocios: dispositivos médicos, sensores de motor, robots industriales, controladores, etc.

De acuerdo con *Network World, Computerworld, CSO, CIO* e *InfoWorld*, no existe un ejemplo más dramático del valor del IoT que el dispositivo médico, como es el caso del termómetro conectado de Kinsa, del que la empresa está agregando datos para señalar posibles brotes de COVID-19. (Fruhlinger, 2020), (Knorr 2020), (CSO 2020), (Binning, 2020) y (Heller, 2020).

Lucas Mearian, redactor de *Computerworld*, observa que el IoT ya ha llegado a la corriente principal de la salud. No sólo el 79% de los proveedores de salud con ingresos superiores a 100 millones de dólares hayan puesto en producción dispositivos de IoT, sino porque Gartner predice un aumento del 13% en el gasto en IoT

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

médico en el próximo año fiscal, además de que el 75% de los proveedores de salud creen que los proyectos de IoT darán resultados financieros en tres años. (Mearian, 2020).

Debido a esto vivimos en una era donde la gran mayoría de los dispositivos están conectados a través de internet, y por ende, los objetos entre sí (AELICES, 2015).

Una aplicación de gran impacto del IoT es el dispositivo médico, como es el caso del termómetro de la empresa Kinsa que creó una red de termómetros conectados para recoger una enorme cantidad de datos sanitarios anónimos que podrían ofrecer una visión de las pandemias actuales como lo es el COVID-19 y futuras, (Gold, 2020).

En *IoT en la granja: Drones y sensores para obtener mejores rendimientos*, el redactor principal de Network World, Jon Gold, entrevista a tres profesionales agrícolas que utilizan dispositivos de IoT para optimizar sus operaciones. En dos de esos casos, los sensores de humedad del suelo proporcionan los datos necesarios para encontrar un equilibrio entre el riego adecuado y la conservación del agua, con un ahorro de costos potencialmente grande. (Gold, 2020)

Para obtener valor de los datos de IoT —cuyo volumen Cisco predice que superará los 800 zettabytes a finales de 2021— se necesitan las herramientas analíticas adecuadas y una estrategia analítica coherente, que el colaborador de CIO Bob Violino esboza en *Analítica de IoT: Cosechando valor de los datos de IoT*. Los elementos básicos incluyen la creación de una organización analítica discreta; establecer una arquitectura escalable de datos de IoT; desplegar sistemas basados en IA que actúen autónomamente sobre los datos de IoT; y usar servicios públicos de nube para la escala y la reducción del tiempo de comercialización (Violino, 2020).

La proliferación del IoT es notoria e innegable, sin embargo, se desconoce es el alcance de la legislación de su uso y aplicación en México por lo que resulta de interés presentar las implicaciones legales de una tecnología tan extendida a nivel mundial.

METODOLOGÍA

Su hace uso de la investigación documental y descriptiva, de acuerdo con (Valderrábano, Hernández y Trujillo, 2020) la investigación documental es aquella que se basa en el estudio "de todo aquello que ha dejado huella en el ser humano", es así como en esta investigación se han localizado en diversas fuentes de información aspectos de relevancia para cumplir con los objetivos planteados. Dicha investigación documental implica el análisis de documentos a criterio del investigador. Por otro lado, es descriptiva ya que busca explicar los aspectos más importantes en el contexto legislativo en México. Además, mide y evalúa diversos aspectos y dimensiones del fenómeno de interés de manera independiente, después integra dichas observaciones con el fin de definir cómo es y cómo se manifiesta (Hernández, Fernández y Baptista, 2006).

GENERALIDADES DEL IOT

Características

Se identifican seis características claves del IoT:

1. El *software y hardware*. Indispensable para su funcionamiento.
2. La conectividad. Fundamentalmente a través de *Internet*, sus protocolos y estándares.

3. La sensibilidad. Identifica la identificación de personas y objetos respecto a cómo es su funcionamiento, manejo y relación.
4. La interacción. Ya sea máquina a máquina M2M o de objetos a personas.
5. La energía. Fundamental para el funcionamiento del IoT.
6. La seguridad. Garantizar una arquitectura segura, tanto en términos tradicionales (riesgo eléctrico, protección a personas) como lo es el riesgo digital (ciberseguridad y la privacidad).

Servicios

El número de aplicaciones y servicios del IoT es prácticamente ilimitado y se puede adaptar a muchos campos de la actividad humana, facilitando y mejorando la calidad de vida en múltiples formas. Algunas aplicaciones y servicios son de acuerdo con (Salazar & Silvestre, 2014):

- Entornos familiares: edificios inteligentes conectados su función principal es mejorar la eficiencia y seguridad, son basados en aplicaciones domóticas que incluyen sensores y actuadores inteligentes para controlar electrodomésticos, servicios de salud, educación en el hogar, entre otros.
- Ciudades inteligentes y transporte: seguridad, verificación del tráfico del transporte, uso en áreas gubernamentales, electorales y de servicios de emergencia por citar algunos.
- Educación: desarrollado para el aprendizaje virtual escuelas y organizaciones.
- Electrónica de consumo: como dispositivos móviles, Smart TV, computadoras, etc.
- Salud: monitoreo de enfermedades crónicas de los pacientes de un hospital.
- Automatización: para realizar cálculos de control de tráfico y la localización, por ejemplo.
- Agricultura y medio ambiente: midiendo y analizando los principales agentes contaminantes.
- Servicios de energía: proporciona los datos precisos sobre el consumo de energía.
- Conectividad inteligente: su perspectiva es mantener el mundo comunicado y conectado, donde principalmente esta la gestión de los datos y las redes sociales.
- Servicios de comunicación M2M: analiza gran cantidad de datos, también existe la realidad virtual, los servicios de computación en la nube de almacenamiento gratuito de pago y seguridad de la red.
- Fabricación: a través de sensores se busca garantizar los comportamientos de las máquinas y de los recursos humanos.

Modelos de implementación

Se distinguen los siguientes modos de implementación (Rose, Eldridge & Chapin, 2015):

Comunicación de dispositivo a dispositivo. El dispositivo representa dos o más dispositivos que se conectan y se comunican directamente entre sí.

Comunicación de dispositivo a la nube. El dispositivo de la IoT se conecta directamente a un servicio en la nube.

- Modelo de Puerta a enlace. El dispositivo de la IoT se conecta a través de un servicio a la puerta de enlace de capa de aplicación como una forma de llegar a un servicio en la nube.
- Modelo Back-End. Los usuarios pueden exportar y analizar datos de objetos

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

inteligentes de un servicio en la nube en combinación con datos de otras fuentes.

ASPECTOS LEGALES

Actualmente, los regímenes legales no dan cuenta de la rapidez con la que se mueven las nuevas tecnologías y sus consecuencias. Frente a este desfase, el fenómeno regulatorio en México aplica la normatividad existente y la adecúa a los avances tecnológicos que se van presentando, en este caso al Internet de las Cosas.

La presencia del IoT es muy amplia y su importancia crece de manera acelerada, es así como resulta de gran relevancia analizar las implicaciones legales en el contexto de su uso e implementación ya que cada vez son más las personas que hacen uso de éste, de manera personal o empresarial. Algunos elementos de estudio para este análisis son:

- La *privacidad* se considera una amenaza para el IoT, es la pérdida del derecho a la intimidad, un derecho humano garantizado en diversas leyes fundamentales y ordenamientos internacionales. Actualmente, el derecho a la protección de la intimidad personal cobra y tiene mucha relevancia, debido a los manifiestos avances tecnológicos, que han provocado cada vez más la vulnerabilidad de la vida privada de las personas. El derecho a no ser perturbado en su privacidad implica algunos aspectos, pero para el caso del IoT tiene incidencia directa en el control y manejo de los dispositivos conectados a través de internet y por tanto de la información y datos personales recopilada en bases de datos.
- La *seguridad* por su parte implica que los proveedores garanticen que cuentan con las medidas de seguridad necesarias, para que la información otorgada siga teniendo las características de ser confiable, segura y que no pueda un tercero disponer y hacer uso de ella.

Así mismo, resulta de gran importancia que los usuarios sigan teniendo la posibilidad de elección respecto a bienes, servicios o tecnologías a través de la portabilidad; además que se garantice el acceso permanente a los servicios adquiridos que gocen de disponibilidad rápida en tiempos de respuesta.

Por lo que debe asegurarse que el usuario tenga conocimiento de las Cláusulas de derechos de Proveedores y limitación de responsabilidad donde se mencionen los términos de acceso a los servicios de IoT y los derechos adquiridos.

Como se ha mencionado el IoT ha tenido un crecimiento exponencial. Es así como los servicios proporcionados no tienen claridad, por ejemplo, en aspectos fiscales, tanto por parte de los proveedores como de los usuarios debe considerarse la jurisdicción del Estado en donde se encuentre domiciliado el usuario.

Existen leyes en México que obligan a mantener la confidencialidad y seguridad de la información, entre las cuales se mencionan las siguientes: Ley General de Profesiones; Ley Federal del Trabajo; Ley de la Propiedad Industrial; Ley Federal de Protección al Consumidor; Ley Federal de Archivo; Ley Federal de Firma Electrónica; Código de Comercio y Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Algunas particularidades importantes dentro del contexto de estudio se detallan a continuación:

La *Ley General de Profesiones*, cuyo objeto es regular el ejercicio profesional entre las autoridades federales y locales, prescribiendo la manera de probar los registros, actos y procedimientos que dentro de dicha función se realicen, así como el exhorto de preservar el secreto profesional en el ejercicio de la profesión.

Mientras el artículo 134, fracción XIII de la *Ley Federal del Trabajo* menciona que es obligación del trabajador la guarda de secretos técnicos, comerciales y de fabricación de productos, además de los asuntos administrativos reservados, cuya divulgación pueda causar perjuicios a la empresa. Así mismo, la fracción IX del artículo 47 del ordenamiento en comento prohíbe al trabajador revelar los secretos de fábrica o asuntos de carácter reservado en perjuicio de la empresa, siendo motivo de la revelación de la información, la rescisión del trabajo sin responsabilidad para el patrón.

Siguiendo en el análisis legal, en la *Ley de la Propiedad Industrial* aborda el tema de la información confidencial, en su artículo 82 menciona que debe considerarse como un secreto industrial toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

Con relación a los medios o sistemas suficientes en la preservación de la confidencialidad de la información, el artículo 83 de la misma ley hace referencia que ésta deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares. Aunado a ello, se contempla que toda persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado (Artículo 85 de la *Ley de la Propiedad Industrial*). Si eres una persona física o moral y contrata a un trabajador que esté laborando o haya laborado, o a un profesionista, asesor o consultor que preste o haya prestado sus servicios para otra persona, con el fin de obtener secretos industriales de ésta, el numeral 86 de la *Ley de la Propiedad Industrial* establece que será responsable del pago de daños y perjuicios que le ocasione a dicha persona física o moral.

Esta misma *Ley de la Propiedad Industrial* considera delito por querella la revelación de un secreto industrial, siendo la sanción una pena privativa de la libertad de 2 a 6 años de prisión y multa por el importe de cien a diez mil días de salario mínimo general vigente en el Distrito Federal (Artículo 224 de la *Ley de la Propiedad Industrial*).

En cuanto a *la Ley Federal de Protección al Consumidor*, se prevé un capítulo respecto a los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. Siendo el artículo 76 BIS, el que enumere las disposiciones legales relativas a ello, destacando algunas que se deberán cumplir:

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

a) Que el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, no pudiendo difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del consumidor o autoridad competente.
b) Que el proveedor deberá utilizar alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste de las características de dichos elementos.
c) El consumidor tiene derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor.

La *Ley Federal de Archivos* establece las disposiciones que permiten la conservación de los archivos en posesión de los Poderes de la Unión, así como el resguardo, difusión y acceso de archivos privados de importancia histórica, técnica, social, cultural o científica.

Por lo que respecta al *Código de Comercio*, su Título Segundo dedicado al Comercio Electrónico, lo divide en cuatro capítulos, el primero de ellos referente a los mensajes de datos, tema en el que se incluye el IoT. De ello podemos mencionar que el artículo 89 de este Código señala que: las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa. En este articulo 89 se mencionan algunas definiciones referentes al comercio electrónico, dando indicios de que el IoT empieza a regularse, estos son: destinatario, digitalización, emisor, firma electrónica, el mensaje de datos, prestador de servicios de certificación y los sistemas de información, los cuales permean para actuar legalmente bajo la premisa del IoT.

Se transcriben de este artículo 89 las definiciones mencionadas, para efectos de conocer que el IoT se hace uso y transferencia de información de los dispositivos coenctados de manera permanente y continua:

- Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos.
- Digitalización: Migración de documentos impresos a mensaje de datos, de acuerdo con lo dispuesto en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría de Economía.
- Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
- Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

- Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con firmas electrónicas, expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría de Economía.
- Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Por tanto, el IoT se sirve de los conceptos presentados con el fin de actuar legalmente bajo la premisa de servicios IoT.

La *Ley Federal de Firma Electrónica* establece la regulación de la firma electrónica avanzada, el certificado electrónico y los servicios relacionados de su alrededor (Téllez, 2013), además pretende homologar la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas en otros ordenamientos legales.

Dentro de los conceptos a destacar en esta ley, que van de la mano con el IoT y de los servicios que ofrece, son:

a) Medios Electrónicos: son los dispositivos tecnológicos para el procesamiento, impresión, despliegue, conservación y, en su caso, modificación de información.
b) Mensaje de Datos: es la información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos.
c) Página Web: es el sitio en Internet que contiene información, aplicaciones y, en su caso, vínculos a otras páginas.

Sin embargo, a pesar de que esta ley representa un avance hablando de los sistemas de información electrónicos, es un ordenamiento que se dirige a regular la actuación de las entidades y dependencias públicas, sus servidores y los particulares que usen la firma electrónica avanzada en términos de esta Ley. Aunque ello no quiere decir, que las mismas entidades públicas no hagan uso de los servicios de IoT. De hecho, partimos de la realidad que se nos muestra hoy en día, ya que muchos de los servicios que se ofrecen por parte de las dependencias públicas son a través de la web, materializando una parte de lo que llamamos e-gobierno o gobierno electrónico.

El e-gobierno y el IoT son actualmente un binomio indisoluble, el primero tendió una red electrónica para diversos servicios o actividades públicas, entendiéndose como el aprovechamiento que la función pública hizo de las TIC con el fin de brindar a la población mejores y más rápidos servicios por parte de sus dependencias, mediante la organización y automatización de sus procesos, especialmente en los trámites que ofrecen, optimizando los recursos de cada entidad pública desde los financieros hasta los humanos, mientras que el IoT le presenta al e-gobierno la posibilidad de manejar y almacenar grandes cantidades de información agilizando su trabajo. Todo lo anterior, teniendo como marco de referencia una, tal vez, incipiente legislación.

Para concluir el análisis legal, tenemos la *Ley Federal de Protección de Datos Personales en Posesión de*

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

Particulares (LFPDPPP) que entró en vigor el 5 de julio de 2010, siendo su artículo primero el que se establezca su alcance jurídico-público, al tener por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Además de que tiene como finalidad establecer y mantener medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales de cualquier individuo en contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, colocando a las personas en el centro de la tutela del Estado.

Al día siguiente de la expedición de esta ley, las empresas de todos los giros de actividades se vieron obligadas a publicar avisos de privacidad y proteger la información personal que pudiese encontrar en sus bases de datos, como lo son las instituciones financieras, bancarias y de crédito, aseguradoras, medios de comunicación, empresas telefónicas, comerciales, industriales, de servicios, hospitales, aerolíneas, escuelas, médicos, laboratorios, bufetes de abogados, despachos contables, empresas publicitarias, tiendas departamentales, restaurantes, agencias de automóviles, etc. Y es que esta ley está dirigida a los particulares sean personas físicas o morales de carácter privado, que lleven a cabo el tratamiento de datos personales, de acuerdo con su artículo 2.

Se ha mencionado que la Ley de protección de datos mexicana contiene normas claras y respetuosas respecto a la privacidad de la información proporcionada por las personas, ello como resultado de principios internacionales aceptados y regulados en otros Estados soberanos y diversos organismos internacionales. Teniendo esto como referencia, se destacan algunos conceptos claves enumerados en la LFPDPPP, basados en los principios internacionales ya aceptados, que pueden ser aplicables en el IoT, como lo son:

1. Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales. Del aviso de privacidad, cabe resaltar que las empresas que hacen uso del IoT, deben manifestarlo de forma evidente en sus páginas electrónicas, donde el usuario puede dar lectura y aceptar las condiciones previstas en la ley.
2. Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.
3. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.
4. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. Nuevamente, para las empresas cuyo objeto es prestado a través del IoT, la manifestación de la

voluntad será marcando una casilla aceptando las condiciones descritas por la empresa.

5. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.
6. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.
7. Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación.

Se establece en la legislación que, si los datos personales son vulnerados por las empresas que los almacenan, es decir, si se pierden, si hay un acceso no autorizado o si los hackean, se deberá informar a la brevedad a los titulares de los datos o información personal, a fin de que ellos puedan tomar las medidas correspondientes y necesarias en defensa de sus derechos. (Gomez, 2012)

El *Instituto Federal de Acceso a la Información* (IFAI), ha manifestado que de lo más relevante que se debe saber con respecto a la LFPDPPP:

- Un dato personal es cualquier información relacionada con el individuo.
- Son datos personales: el nombre, domicilio, teléfono, fotografía o huellas dactilares, así como cualquier otro dato que sirva para la identificación de la persona.
- La persona es dueña de sus propios datos personales y sólo ella decide cómo, cuándo, a quién y para qué entrega su información personal, salvo las excepciones que establezcan las leyes.
- Es de relevancia que la persona cuide sus datos personales por razones de seguridad, además de ser su derecho.
- Los datos o información personal deben ser protegidos contra el mal uso como: robo de identidad, transmisiones ilícitas o accesos no autorizados.
- La Ley regula las condiciones en que las empresas deben usar los datos personales.
- Existen datos sensibles requiriendo de mayor protección, se consideran como tales: el origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencias sexuales.

A estos conceptos se suman los principios legales que deberán cumplir las empresas, personas físicas o morales en el tratamiento o guarda de información o datos personales en forma física o electrónica, los cuales son: consentimiento, licitud, finalidad, información, calidad, lealtad, responsabilidad y proporcionalidad.

Partiendo del hecho y derecho que, en el tratamiento y manejo de datos personales, se supone que existe un acuerdo de privacidad, entendiendo éste como la confianza que se deposita entre dos o más personas, con respecto de que los datos personales o información proporcionada, será tratada conforme a lo

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

acordado por las partes, estando sujeta al consentimiento de su titular (Artículo 7 LFPDPPP). Dicho consentimiento podrá manifestarse expresa o tácitamente, para el primer caso podrá ser verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Mientras que tácitamente será cuando el tratamiento de sus datos o información, cuando no manifieste su oposición y se hubiese puesto a disposición del aviso de privacidad.

Esto nos lleva a referenciar el contenido de los avisos de privacidad que deberán cumplir los responsables del manejo de la información, incluyendo aquellas que se dedican a los servicios de computación en la nube, a saber:

1. La identidad y domicilio del responsable que los recaba.
2. Las finalidades del tratamiento de datos.
3. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.
4. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición.
5. En su caso, las transferencias de datos que se efectúen.
6. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad. (Artículo 16 LFPDPPP)

Siguiendo con el aviso de privacidad y como lo señala la LFPDPPP, éste debe ponerse a disposición de los usuarios a través de formatos impresos, visuales, digitales, sonoros o cualquier otra tecnología. Para el caso de que sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información relativa a la identidad y domicilio del responsable que los recaba, así como las finalidades del tratamiento de datos; así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Actualmente se han establecido convenios de IoT, los cuales contemplan que las dependencias públicas o privadas permitan la tercerización de servicios, mientras que los proveedores ofrezcan seguridad, privacidad y protección de los datos personales. Si el proveedor cumple con las políticas de privacidad y cumple con las normas que suscriben la legislación, se podría afirmar que el proveedor es realmente confiable y establecido legalmente.

Sin duda, el IoT ha sido una herramienta ya necesaria para el almacenamiento y manejo de la información, dando un tratamiento especial y confidencial de los datos que clientes o usuarios hagan de diversos servicios que las empresas ofrezcan en la web, la responsabilidad de éstas parte del aviso de confidencialidad y posteriormente con el manejo de la información que se encuentra en los servidores web.

CASO DE ESTUDIO: APLICACIONES LEGALES EN EL CLOUD COMPUTING

En México, un ejemplo de aplicación IoT muy cercana a la población lo realiza Mobike, la start-up de origen chino, que ofrece ahora en la Ciudad de México un servicio para compartir bicicletas. Esta compañía se asoció con Gemalto para proporcionar una conectividad IoT inalámbrica y segura. Los usuarios sólo requieren descargar la aplicación Mobike –disponible en iOS y

Android– para crear una cuenta y encontrar la bicicleta inteligente disponible más cercana.

Con un solo clic, los usuarios pueden escanear el código QR en el manubrio de la bicicleta, que libera un candado de rueda habilitado por Gemalto antes de marcharse. El vehículo dispone de sensores para reportar las condiciones de la bicicleta y un localizador GPS integrado (Becerra, 2018).

Todos los dispositivos de IoT manejan datos de su usuario, por ejemplo, en el caso de las pulseras para medir la actividad de una persona, presenta algunos riesgos asociados al no tener la protección de datos ni la seguridad necesaria ya que están diseñados con poco o ningún pensamiento de seguridad. Esto se debe a que tiene relativamente poca memoria y capacidad de computación para respaldar la seguridad, pero también porque a menudo están diseñados con poco tiempo de lanzamiento al mercado, precio y características como consideraciones principales con exclusión de la seguridad.

CONCLUSIONES

El internet de las cosas tiene su principal fundamento en la gestión remota de la información. Las empresas, entes públicos y organizaciones transfieren grandes cantidades de información a servidores pertenecientes en su mayoría a terceros. Esto trae consigo varias implicaciones o consecuencias jurídicas, más aún en el caso cuando los datos se alojan o almacenan en servidores de otros países, convergiendo dos o más jurisdicciones, surgiendo la necesidad de determinar aspectos legales y contractuales aplicables al caso.

En varios países se han promulgado leyes donde su principal objetivo es proteger la información, siendo Suecia en el año de 1973 el primer país en el mundo en contar con una ley de protección de datos, siguiendo el ejemplo Estados Unidos en 1974 y otros de Europa occidental.

Por otro lado, en México se ha promulgado su propia ley de protección de datos, siendo ésta una de las más nuevas del mundo; sin embargo, en el análisis de esta ley y otras correlativas de la materia, se puede identificar que no contemplan de manera explícita el tratamiento de datos personales en servicios de IoT, mientras que en países de la Unión Europea, Argentina, Canadá y otros, consideran puertos seguros a los países que tienen la posibilidad de transferir datos almacenados de forma segura y cobijados por la ley contractual y de protección de datos de su país.

Ahora bien, partiendo del entorno de la sociedad de la información, México tiene un avance significativo en la economía digital y el gobierno electrónico como ya se expuso en el desarrollo de esta investigación; sin embargo, siguen faltando algunas tareas. La encomienda actual del gobierno es crucial en la era de la información, ya que la combinación de los avances tecnológicos con las nuevas formas de operación y el manejo de la información almacenada a través de IoT, hará que sea más eficiente y efectivo. Nuestro país cuenta con esfuerzos importantes en esta materia (trinomio: TIC-procesos de operación-manejo y almacenamiento de información en nube); sin embargo, sigue sin existir una política pública integral y legal en la materia, que concentre los esfuerzos y reúna a los agentes involucrados en pro del desarrollo, competitividad y la innovación tecnológica a nivel mundial.

Como diagnóstico, se puede afirmar que México necesita crear estrategias para impulsar a las pequeñas y

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721

medianas empresas que se encuentran obsoletas con respecto a la tecnología, además de desarrollar medios de comunicación de los cuales informe los beneficios, ventajas y desventajas del IoT,

El Estado para los servicios web que ofrece, debe tener el objetivo de optimizar el gasto público teniendo un mejor tratamiento de la información que tiene y genera al interior y exterior de sus dependencias, con la finalidad de incrementar la calidad y rapidez en sus servicios con la población, siendo el IoT la pieza clave para iniciar y poner en marcha como parte de los servicios públicos del país.

En cuanto al área privada, los usuarios de los servicios o productos que se ofrecen en la web, buscan no solo la versatilidad de la búsqueda de información, sino también la seguridad y privacidad de los datos o información que comparten en una solicitud, o en una compra, etc. La tranquilidad del usuario parte del hecho de que su información ha sido entregada para no ser violada, que el almacenamiento y manejo de la información es profesional, que se han adoptado los medios suficientes para la guarda de su información, siendo el IoT un medio para lograr esos objetivos.

Sin duda y después del análisis a la legislación en la materia, existen retos jurídicos importantes para el éxito en la adopción y el desarrollo del IoT desde la perspectiva pública como la privada, siendo los dos temas prioritarios por tratar: la privacidad y la seguridad de la información en la web. Explicar con claridad los resultados obtenidos y las posibilidades de mejora.

BIBLIOGRAFÍA

Aelices (2015). I*nternet of Things: Evolución o Revolución. Obtenido de Internet of Things: Evolución o Revolución*. https://www.eoi.es/blogs/redinnovacionEOI/2015/09/20/internet-of-things-evolucion-o-revolucion/

Becerra, J. (2018). *Reporte Especial: Internet de las Cosas en México, ¿es redituable su aplicación?* https://cio.com.mx/reporte-especial-internet-las-cosas-en-mexico-redituable-aplicacion/

Binning, D. (2020). *The CIO Show: IoT really is a thing now*. https://www.cio.com/article/3586256/the-cio-show-iot-really-is-a-thing-now.html

Código de Comercio. 28 de marzo de 2018 (México).

Código de Comercio. 8 de junio de 2009 (México).

CSO (2020). *The IoT security survival guide*. https://www.csoonline.com/article/3196246/the-iot-security-survival-guide.html

Eldridge, R., Chapin, K. & Lyman, S. (2015). La internet de las cosas una breve reseña. *Internet Society (ISOC)*.

Fernández, R. (2020). Distribución de los accesos a redes móviles a nivel mundial en 2025, por generación. *Statista*. https://es.statista.com/estadisticas/933729/internet-movil-a-redes-2g-3g-4g-y-5g-en-el-mundo/xs

Fruhlinger, J. (2020). What is IoT? The internet of things explained. *Network World*. https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

Gartner (2020). Internet of Things (IoT). *Gartner Glossary*. https://www.gartner.com/en/information-technology/glossary/internet-of-things

Gold, J. (2020). Termómetros conectados, la vía para rastrear la COVID-19. *Network World*. https://www.networkworld.es/movilidad/termometros-conectados-la-via-para-rastrear-la-covid19

González, M. (2014). El wearable que delató al asesino. *Xataka*. https://www.xataka.com/wearables/el-wearable-que-delato-al-asesino

Heller, M. (2020). How to choose a cloud IoT platform. *InfoWorld*. https://www.infoworld.com/article/3539010/how-to-choose-a-cloud-iot-platform.html

Hernández, R., Fernández, C., y Baptista, P. (2006). *Metodología de la investigación*. México: McGraw-Hill.

Knorr, E. (2020). The Internet of Things in 2020: More vital than ever. *Network World*. https://www.networkworld.com/article/3542891/the-internet-of-things-in-2020-more-vital-than-ever.html

Ley de Firma Electrónica Avanzada. 11 de enero de 2012 (México).

Ley Federal de Protección a la Propiedad Industrial. 1 de julio de 2020 (México).

Ley Federal de Protección al Consumidor. 12 de abril de 2019 (México).
Ley Federal de Protección de Datos Personales en Posesión de Particulares. 5 de julio de 2010 (México).
Ley Federal del Trabajo. 23 de abril de 2021 (México).
Ley General de Archivos. 15 de junio de 2018 (México).
Mearian, L. (2020). How IoT is becoming the pulse of healthcare. *Computer World*. https://www.computerworld.com/article/3529427/how-iot-is-becoming-the-pulse-of-healthcare.html
Rose, K., Eldridge, S. y Chapin, L. (2015). El internet de las cosas. Una breve reseña. Int*ernet Society (ISOC)*. https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf
Salazar, J., Silvestre, S. (sf). Internet de las cosas. *TechPedia*. https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf
Unión, C. d. (8 de junio de 2009). Código de comercio. Recuperado el 1 de septiembre de 2016, de Código de comercio: http://www.oas.org/juridico/spanish/mesicic3_mex_anexo8.pdf
Valderrábano, M. Hernández, R. y Trujillo, M. 2002. La investigación documental. *Colección Digital UDLAP*. http://catarina.udlap.mx/u_dl_a/tales/documentos/lhr/olvera_p_m/capitulo2.pdf
Vermesan, O. (2011) Internet of things strategic research roadmap, Internet of Things: Global Technological and Societal Trends
Vijayan, J. (2014). The Internet of Things likely to drive an upheaval for security. *Computer World.* https://www.computerworld.com/article/2488878/the-internet-of-things-likely-to-drive-an-upheaval-for-security.html
Violino, B. (sf). Analítica de IoT: Obteniendo valor de los datos de la IoT. *CIO Peru*. https://cioperu.pe/articulo/30188/analitica-de-iot-obteniendo-valor-de-los-datos-de-la-iot/
Yubal, F. (2014). Fitbit vuelve a los juzgados, pero esta vez como testigo. *Genbeta*. https://www.genbeta.com/actualidad/fitbit-vuelve-a-los-juzgados-pero-esta-vez-como-testigo

Interconectando Saberes, Año 6, Número 12, julio-diciembre de 2021, pp.1-14
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i12.2721