El Internet de las cosas: la importancia de salvaguardar el derecho a la privacidad y el derecho humano al Internet

The Internet of Things: the importance of safeguarding the right to privacy and the human right to the Internet

Diana Vanessa Gutiérrez Espinoza
Academia Interamericana de Derechos Humanos
Universidad Autónoma de Coahuila
Orcid: 0000-0002-5300-5505

Víctor M. Vera García
Academia Interamericana de Derechos Humanos
Universidad Autónoma de Coahuila
Orcid: 0000-0002-9360-3067

Fecha de recepción: 24 de febrero de 2022
Fecha de aceptación: 12 de mayo de 2022

Resumen: El presente trabajo describe los problemas que surgen a raíz del fenómeno llamado el Internet de las cosas, que es la conexión masiva de objetos de la vida cotidiana al Internet. Estos problemas se dan principalmente en el ámbito de la privacidad de las personas. Por tal motivo se presentan diversos argumentos y planteamientos para armonizar el derecho a la privacidad y el derecho humano al Internet.

Abstract: This paper describes the problems arising from the phenomenon called the Internet of Things, which is the massive connection of everyday objects to the Internet. These problems are mainly related to the privacy of individuals. For this reason, several arguments, and approaches to harmonize the right to privacy and the human right to the Internet are presented.

Palabras clave: *derecho a la privacidad, derecho humano al Internet, el Internet de las cosas.*

Keywords: *right to privacy, human right to the Internet, the Internet of Things*

I. Introducción

Cada día más gente utiliza Internet en el mundo, sobre todo en países con economías emergentes, como Malasia, Brasil o China (Bonilla Fabela *et al.* 2016: 2314). En países desarrollados, la presencia del Internet en la vida cotidiana está ya prácticamente insertada como algo cotidiano, y de hecho, ya muchas interacciones humanas no se pueden llevar a cabo sin la ayuda de esta conexión. Esta conexión se está dando cada vez más a través de dispositivos de uso cotidiano que se comunican entre sí y recogen información de ellos mismos así como de las personas que los utilizan. A esta red de interconexión cada vez más grande, paralela en el mundo real de *world wide web*, se le denomina como el *Internet de las cosas* (IoT por sus siglas en inglés).

Esta tendencia a comunicar cada aspecto de la vida cotidiana y a recoger información está más presente en el mundo. Se estimaba que para el año 2020, 30 mil millones de dispositivos estarían conectados al Internet de las cosas (Dw Documental 2022). Todos estos dispositivos conectados tienen la intención de beneficiar a los seres humanos. Se busca reducir cargas de trabajo que pueden ser automatizadas por las inteligencias virtuales o artificiales. Sin embargo, así como existen aplicaciones benéficas para el IoT,

también existen problemas latentes o presentes, en especial aquellos relacionados con el derecho a la privacidad de las personas.

La información de las personas se ha definido como el nuevo petróleo o una nueva clase de activo (Kuneva 2009: 1). Sin una regulación rigurosa por ejemplo, la información recopilada se puede vender para campañas de marketing y publicidad, lo cual ya se ha hecho con efectos nocivos. No obstante, esa información ahora se utiliza también por los hospitales para prestar atención médica, o por las empresas aseguradoras para decidir a qué personas asegurar y a qué precios vender sus servicios (Orlowski 2020).

En el año 2000 sólo una tercera parte de la información mundial estaba almacenada de forma digital, el resto se encontraba en medios analógicos como el papel, por su parte al menos para 2015 más del 98% de la información de las personas es digital (Gil González 2016: 18). A comienzos de 2022 no es exagerado pensar que el 100% de la información de las personas se encuentra dentro de alguna de las múltiples bases de datos digitales. Debido a lo anterior resulta trascendental fomentar la discusión respeto a la problemática que trae consigo el IoT y en esto es en lo que se enfoca el presente trabajo.

Conviene señalar también que existe un concepto que está muy ligado al IoT, y es el denominado *Big data,* que: "Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que estén sujetas a un análisis extenso basado en el uso de algoritmos" (Gil González 216: 17). Podría decirse que el IoT es la herramienta necesaria para que el Big data funcione de forma óptima, pues sin aparatos de la vida cotidiana conectados a Internet y utilizados activa y voluntariamente por las personas, resultaría complicado poder recabar esa cantidad masiva de información.

Ahora bien, este artículo se centra primordialmente en entender cómo funciona la comunicación entre cosas a través de Internet y describir consideraciones ya planteadas sobre cómo se puede

regular para salvaguardar la privacidad de las personas. Sin embargo, como el IoT y el *Big data* están tan intrínsecamente relacionados es poco probable pensar que las reflexiones aquí vertidas sólo sirvan para el primer concepto. Teniendo eso en cuenta mucha de la información que existe sobre regulación habla exclusivamente del manejo de los datos ya recopilados, no de la forma en que se recaban los mismos o de las herramientas que se utilizan para ello. Aquí se presenta dicha información y se hacen comentarios al respecto de cómo agregar al IoT en tal regulación.

No obstante, el IoT precisa que se tomen en cuenta cuestiones como micrófonos, cámaras, sensores u otros medios de medición de la información en los objetos conectados a Internet. Dichas cuestiones son las que se comentarán en el presente.

Por otro lado, se abre una acotación en el texto para hablar de un derecho que debe ponderarse al considerar cualquier cuestión de privacidad o de interconexión de las cosas a través del Internet. Este es el derecho humano al Internet, el cual podría definirse como la otra cara en cuestiones relacionadas a la conexión global. Así como hay un problema de privacidad, también existe la falta de información y la necesidad de contar con herramientas útiles para garantizar que los conocimientos y los avances tecnológicos sean disfrutados cada vez más por un mayor número de personas.

Así pues, el orden en que se presentan los tópicos del tema a tratar es como se describe en las siguientes líneas. Primero, se dará una explicación breve de lo que se entiende por el IoT, presentando antecedentes, definiciones y las problemáticas que el fenómeno conlleva. En segundo lugar, se hablará de los derechos humanos que tienen relación con el fenómeno del IoT, como son el derecho al Internet y en especial el derecho a la privacidad. En tercer lugar se expondrán las breves consideraciones que se han tenido respecto a las formas en que se puede resolver jurídicamente el problema de la privacidad de las personas. Finalmente se señalarán las conclusiones derivadas de la investigación.

II. ¿Qué es el Internet de las cosas?

1. Origen, definición y alcances

El término de IoT surgió en los años noventa, cuando fue acuñado por Kevin Ashton en el contexto de gestión de la cadena de suministro, la cual es el proceso de distribución de productos terminados al consumidor y que inicia desde la etapa de obtención de materiales y su transformación. Este concepto surge prácticamente con la llamada revolución de Internet, cuando se dio por vez primera la posibilidad de la interconexión entre personas a través de aparatos pensados para tal propósito (Mora González 2015: 22).

Ahora bien, el inconveniente que se buscaba resolver en la gestión de la cadena de suministro era la necesidad de recabar información de cada objeto gestionado. La idea era colocar información a cada objeto para poder escanearlo y monitorearlo, revisar su estado dentro de la cadena, pedir que se comportara de cierta forma, así como revisar cualquier otra variable de información (Mora González 2015: 23).

Definir el IoT no es sencillo, pues la tecnología va avanzando y lo que hace unos años parecía el estándar puede que hoy no lo sea ya. Además, la idea que tienen algunos expertos o académicos no es igual que la de otros, pues unas definiciones son amplias mientras que otras están más limitadas. De hecho, existen algunos autores que definen al IoT no como un conjunto de dispositivos o aparatos conectados sino como un ambiente computacional o inteligente, donde coexisten entidades conscientes de su contexto y capaces de comunicarse con otras entidades del ecosistema (Khodadadi 2016: 2). Sin embargo, existen elementos que pueden considerarse esenciales relativos a la idea del IoT y tener así una base común.

Teniendo en cuenta lo anterior distintos autores y autoras dan una serie de definiciones de las cuales se reproducen algunas. Una primera definición establece que el IoT es: "la interconexión en red de objetos -desde los más sofisticados hasta los más mun-

danos- mediante identificadores como sensores, etiquetas RFID (identificación por radiofrecuencia) y direcciones IP (Protocolo de Internet)" (Conner 2010). Otra definición del IoT dice que es: "la interconexión de objetos, cosas, elementos cotidianos a la Internet, a través de diferentes tecnologías como son los dispositivos habilitados con la tecnología inalámbrica abierta como bluetooth, la identificación por radiofrecuencia (RFID), Wi-Fi y los servicios que brindan teléfonos inteligentes, así como sensores y actuadores (dispositivos que permiten la manipulación y control) que estén integrados a los objetos" (Mora González 2015: 22).

Por su parte una tercera definición dada por Wachter menciona que: "El IoT puede referirse a una red de objetos sensores que monitorean y registran aspectos de su entorno y los comportamientos de los usuarios dentro del mismo. Junto a las ya conocidas etiquetas RFID, las redes de sensores inalámbricos y los dispositivos con Bluetooth que han surgido como sensores del IoT" (2018: 436).

De las distintas definiciones señaladas se pueden desprender dos elementos en común. Estos elementos son: 1) una conexión en red a través del Internet; y 2) la interconexión se da entre objetos de uso cotidiano. De hecho, estos elementos permiten diferenciar la tendencia del IoT con aquellas situaciones que empezaron al menos desde la década de los años ochenta en que inició la era computacional y la primitiva conexión a Internet (Gil González 2016: 19).

La diferencia más importante radica en que anteriormente las conexiones a la world wide web eran a través de dispositivos especializados para ese propósito, como computadoras de sobremesa, computadoras portátiles, u otros dispositivos diseñados especializados que ayudaban en tareas a científicos o profesionales en sus respectivos ámbitos, como las computadoras industriales (Dw Documental 2022). Y si bien como se ha dicho anteriormente, este concepto no es nuevo, se podría argumentar que el IoT inició con la creación de los dispositivos inteligentes, empezando por los smartphones. El primero de estos dispositivos, el iPhone fue pre-

sentado por primera vez el 9 de enero de 2007 en la conferencia Macworld (Evans 2011: 2 y 3).

Con el paso de los años cada vez son más y más los aparatos que tienen la etiqueta de *inteligentes*. Los teléfonos son la respuesta más obvia, pero actualmente existen coches, relojes, televisiones, refrigeradores, lámparas, focos, enchufes, licuadoras y hornos de microondas con ese adjetivo; además de los asistentes como Siri, Alexa, Google o Cortana. Es más, el término de inteligente ya se aplica a lugares que cuentan con una red importante de estos artefactos conectados entre sí, y el ejemplo más claro son las denominadas casas inteligentes (Zheng 2018).

Pese a la amplia gama de dispositivos inteligentes que ya existen en el mercado puede afirmarse que el IoT se encuentra en su infancia, pero no es descabellado pensar que, en un futuro no muy lejano, esta interconexión de artefactos de uso cotidiano llegará a todos los aspectos de la vida humana. Desde hace años se habla que la integración de sensores en armarios o maletines podrían crear un inventario de las prendas que se encuentran en los primeros o de los objetos que hay en los segundos (Conner 2010). Prácticamente cualquier tipo de herramienta, utensilio, mueble o vehículo puede ser conectado a través de Internet e interactuar con nuestras otras posesiones.

En las iteraciones más recientes de la Consumer Electronics Show (Ces), la feria de electrónica más grande de Estados Unidos, se pueden encontrar inodoros para gatos, inodoros humanos, lavabos, botes de basura, rociadores e incluso pañales que se conectan a Internet (Dw Documental 2022). La expresión que se usa en la actualidad ya ni siquiera es el *Internet de las cosas*, sino el *Internet de todas las cosas* (Harari 2019: 1079).

En cuestión de la conexión a Internet, la imaginación parece ser el límite. Sin embargo, ¿para qué se busca en primer lugar que aparatos electrodomésticos, muebles, prendas de vestir o incluso seres vivos se conecten al Internet? La respuesta es simple

y compleja a la vez. El conectar todo aquello que forma parte de la vida cotidiana de seres humanos hace la vida más sencilla, de eso no hay duda. Desde las cosas más simples como preguntarle a Alexa "¿cómo está el clima?", hasta el refrigerador inteligente que avisa cuando falta algún insumo como leche o huevo, es demostrado que la conexión a Internet de distintos aparatos quita al ser humano una serie de cargas que hasta el momento aún tiene.

De hecho, el objetivo del IoT es en primer lugar la interconexión de todas las cosas, y en segundo lugar, el asegurarse que todas esas cosas sean inteligentes. En un caso hipotético, de un puente que comunica dos ciudades como el Bay Bridge que conecta San Francisco y Oakland, si este contara con acelerómetros enlazados a Internet, estos mismos podrían registrar el patrón de vibración de fallas inminentes. Así se evitaría que obras como ésta quedaran cerradas por días debido a las reparaciones (Conner 2010).

Respecto a la predisposición de la gente a que se recaben sus datos personales a través de dispositivos inteligentes, la práctica y la experiencia de los primeros años hacen pensar que será más fácil tener la voluntad de las personas en la recabación de sus datos. Según el filósofo e historiador Yuval Noah Harari, la gente estaría más que dispuesta a entregar un poco de su libertad y privacidad para poder hacer más sencilla su vida, puesto que en la nueva religión llamada dataísmo, el estar desconectado del flujo de datos supone arriesgarse a perder incluso el sentido de la vida (Harari 2019: 1087 y ss.). Es por lo anterior que pese a los múltiples movimientos de desconectarse de las redes sociales o de Internet en general que van surgiendo, la realidad para la gran mayoría de personas será entregar voluntariamente un poco de su libertad e información personal a cambio de ese sentido de existencia.

El resolver los problemas técnicos, científicos y de recursos tanto materiales como humanos que impiden una conexión total de las cosas está en manos de las personas expertas. Sin embargo, tras esta breve exposición de lo que significa el IoT no queda duda que es una tendencia que únicamente está creciendo y ganando popula-

ridad. Sus aplicaciones son interesantes, innovadoras y extremadamente útiles. Una red gigantesca de cosas conectadas a Internet y que recaba todos los días datos de sus usuarios, es sumamente benéfica si es usada de forma adecuada y ética. No obstante, no pasa desapercibido que así como existen beneficios de lo anterior, existen también riesgos muy latentes y presentes.

Actualmente ya existen diversos ejemplos de la mala utilización de la información personal, principalmente para la manipulación de la opinión pública o la polarización en campañas electorales como las presidenciales de Estados Unidos en donde Donald Trump resultó electo (Orlowski 2020). Sobre los inminentes riesgos que supone para la privacidad de las personas el IoT, se habla en las siguientes líneas.

2. La problemática que trae consigo

Una vez entendido de dónde viene el IoT, los elementos que conforman su definición y los beneficios para la vida de las personas, toca ahora abordar el tema contrario: la preocupación por un mal manejo de la información de las personas.

Conectar cosas a Internet tiene como ya se desarrolló, la intención de ayudar a mejorar la vida de las personas, ¿cómo se logra esto? Para poder atender a las necesidades de quienes utilizan las cosas inteligentes, estás herramientas o aparatos recopilan toda la información posible de sus usuarios. Desde hábitos cotidianos como la hora en que duerme la gente, a qué hora se despierta en las mañanas, los días que va a trabajar; hasta cuestiones más personales como pasatiempos, ideologías políticas o incluso el historial médico (Orlowski 2020).

De acuerdo con Gil González existen tres riesgos potenciales derivados de la recolección de información personal: 1) el riesgo de llegar a conclusiones erróneas que no son revisadas; 2) el riesgo de tomar decisiones automatizadas sin un razonamiento humano previo; y 3) el riesgo para la privacidad de las personas (2016: 32).

Los dos primeros riesgos son interesantes en sí mismos, sin embargo, el tema principal de este trabajo es la privacidad de las personas, sobre la cual se habla de forma más detallada en siguientes párrafos.

De manera somera se pueden dar ejemplos de tópicos relacionados con el IoT que, de ser empleados sin considerar a los usuarios, pueden suponer un riesgo importante para la privacidad de los mismos. La gran mayoría de estos dispositivos se pueden controlar con comandos de voz, lo cual supone que en los mismos existen micrófonos. Otros tantos de estos dispositivos poseen cámaras o pueden controlar cámaras de forma remota. Y otros más poseen sensores que recogen todo tipo de información, como los relojes inteligentes que pueden medir la presión arterial, el nivel de oxigenación de la sangre y cuántas horas duerme una persona (Baig 2020).

En este sentido las empresas desean saber todo sobre las personas y para algunos este emprendimiento está cruzando límites. ¿Deberían los dispositivos conectados a Internet analizar el cuerpo de las personas? En principio todo se realiza por una razón benéfica, sin embargo, también se han realizado monitoreos violentando la vida privada de las personas y para conceder o denegar tratamientos, seguros y servicios. Una compañía de seguros, por ejemplo, estuvo monitoreando el uso de una máscara oxigenadora para tratar la apnea del sueño en uno de sus pacientes. Dicho paciente no tenía conocimiento de que lo estaban monitoreando y aunado a eso la compañía utilizó dicha información para negarle un nuevo aparato pues argumentaron que este no había sido usado (Dw Documental 2022).

Además de lo anterior, existe también un problema grave que no pasa desapercibido y es el que los datos personales de usuarios de distintas plataformas son recolectados y posteriormente vendidos y transferidos a terceros, generalmente empresas de publicidad que les dan un uso que los usuarios no aceptaron. Esta situación alcanzó notoriedad e indignación cuando salió a la luz que la empresa Cambridge Analytica recolectó datos de millones de usuarios de Facebook sin el conocimiento de ninguno de ellos para dar ase-

soría en las campañas presidenciales de Ted Cruz y Donald Trump en 2016 (Redacción Bbc Mundo 2018; Orlowski 2020).

La posibilidad de que algo como lo de Cambridge Analytica se repita crece exponencialmente si no se da una respuesta de regulación ante el rápido desarrollo de las tecnologías que dan forma al IoT y de las cosas conectadas a Internet. Lo anterior debido a que, si ya resultó sencillo recolectar información personal a través de redes sociales, más fácil resultará colectar datos de las personas a través de sus teléfonos, carros, bocinas, casas, etcétera.

Existen académicos que piensan en las catastróficas situaciones que las anteriores actividades pueden traer consigo. Por ejemplo, de acuerdo con Morte Ferrer, Weltzer habla ya de las posibilidades de una *dictadura smart* debido a los riesgos derivados del grado de desarrollo que algunas tecnologías están alcanzando (Morte Ferrer 2017: 230).

III. Derechos humanos involucrados en el IoT

A partir de definir el concepto del IoT y determinar cuáles son sus alcances, es posible fijar dos de los principales derechos que se involucran en el tema: 1) el derecho humano al Internet y 2) el derecho humano a la privacidad. Al tratar de mejorar, hacer más eficientes y rápidos todos los procesos de la vida diaria por medio de las tecnologías, surgen necesidades específicas que deben ser analizadas desde la óptica jurídica.

En este sentido, el IoT es una herramienta para el intercambio de información con la finalidad de facilitar las actividades diarias de las personas. Lo anterior, se resume en la prestación de servicios avanzados a través de interconexión de cosas físicas y/o virtuales. La definición del IoT y su evolución ha traído una amplia gama de ventajas. Sin embargo, la expansión del Internet de las cosas también trajo una serie de desventajas que repercuten en la priva-

cidad y protección de las personas. A continuación, se desarrollan algunas de las principales ideas del derecho al Internet, que contempla las ventajas de la interconexión y el derecho a la privacidad, una necesidad cada vez mayor en un mundo tan interconectado.

1. El derecho humano al Internet

Antes de definir en qué consiste el derecho humano al internet, es necesario mencionar que el Internet forma parte de las Tecnologías de Información y Comunicación (Tic). La evolución y constante transformación de la sociedad, bajo la necesidad de mejorar y agilizar la vida diaria en todos sus ámbitos ha permitido que las Tic estén presentes en todo el mundo.

En este sentido, un aspecto muy importante de las Tic implica que deben ser aprovechadas para lograr el desarrollo integral de las sociedades. Esto se refiere al impulso del potencial humano desde los diversos aspectos, impactando en el ámbito económico y social, en condiciones de igualdad (Sánchez Duarte 2008: 156-157).

Sin duda, el Internet ha sido una herramienta que ha cambiado a la humanidad impactando en diversos aspectos y ha logrado romper barreras para mantener comunicaciones en todo el mundo abriendo paso a la verdadera era de la globalización (Salazar Jaramillo 2014: 283).

Es importante establecer que el origen del Internet se ubica en el año 1969, pero fue hasta los años noventa que el Internet comenzó a extenderse como un servicio atractivo para las personas en general (Trigo Aranda 2004: 3-5). En estos primeros antecedentes del surgimiento del Internet, se puede comparar la evolución de cómo se ha consolidado como una herramienta fundamental transversal en múltiples aspectos de la vida humana, siendo reconocido en la actualidad como un derecho humano.

Ante una sociedad contemporánea con grandes necesidades, el Internet se ha constituido como un derecho humano para todas

las personas. Por tanto, el Internet es un derecho al avance científico y tecnológico al igual que el disfrute de los beneficios que produzca. En el artículo 27 de la Declaración Universal de Derechos Humanos, se reconoce el derecho que toda persona tiene "a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten".

Cabe destacar que el derecho al Internet se vincula con una serie de derechos, esto se relaciona con las características propias de los derechos humanos, como son: la interdependencia e indivisibilidad. Resulta indispensable mencionar la conexión que existe entre el derecho humano al Internet y otros derechos humanos, como son: la educación, el trabajo, el acceso a la información, la libertad de expresión, entre otros.

A partir del derecho a la libertad de expresión es posible empezar a visualizar el reconocimiento del Internet como un derecho humano. En el informe de Frank La Rue, como Relator Especial sobre la promoción y protección del derecho a la libertad de opinión de 2011, se centra en el derecho que tienen todas las personas para buscar, recibir y difundir información e ideas de todo tipo por medio del Internet. Entre los puntos más importantes de este documento se destacan:

1) Resaltar la importancia de la naturaleza singular y transformadora del Internet que permite el ejercicio de muchos derechos humanos, entre estos la libertad de expresión.

2) El Internet como una herramienta para impulsar el progreso de las sociedades.

3) El acceso a la infraestructura física y técnica necesaria para acceder en un principio a Internet. Relacionado con la obligación que asumen los Estados para adoptar las medidas necesarias para garantizar el acceso universal al Internet y disminuir la brecha digital (Resolución A/HRC/17/27, 16 mayo 2011).

Fue en 2016, que el Consejo de Derechos Humanos a través de su resolución A/HRC/32/l.20 reconoció la necesidad de promoción, protección y disfrute de los derechos humanos en Internet, de la cual se destacan los siguientes aspectos:

1) La obligación de proteger los derechos de todas las pesonas en Internet.

2) El reconocimiento de la naturaleza mundial y abierta, como fuerza impulsora de aceleración de progresos.

3) La vinculación e importancia que tiene el Internet y la educación.

4) El acceso al Internet y el impulso para cerrar la brecha digital.

5) La importancia de generar confianza en Internet, específicamente en derechos como la libertad de expresión, la privacidad entre otros derechos humanos.

A través de algunos antecedentes mencionados, se ha evidenciado que el Internet es una herramienta indispensable a la que todas las personas deben tener acceso, al ser un vehículo fundamental para poder garantizar muchos otros derechos humanos. En marzo de 2020 la Organización Mundial de la Salud declaró la pandemia de enfermedad por el virus SARS-COV2, como emergencia de salud pública e interés internacional. Debido a la situación de emergencia, el mundo se detuvo y las actividades que se realizaban comúnmente transitaron a ser virtuales.

Esta situación que ha perdurado hasta la actualidad (2022), ha permitido concientizar la necesidad fundamental de que todas las personas tengan acceso al Internet. Lo anterior debido a que el Internet es una herramienta fundamental para poder continuar la gran mayoría de las actividades de la vida diaria, especialmente la educación y el trabajo. Las circunstancias actuales han permitido reafirmar la importancia de que los Estados adopten medidas que permitan garantizar el derecho humano al Internet.

2. El derecho humano a la privacidad

La privacidad como un derecho humano deriva de la expectativa de seguridad y protección en el ámbito personal. En el artículo 12 de la Declaración Universal de Derechos Humanos se establece que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

El derecho a la privacidad, es diferente al derecho a la vida privada entendiendo que este último es más amplio de lo que implica el primero. A lo largo de la historia diferenciar entre estos estos derechos y establecer su contenido no ha sido sencillo (Piñar Mañas y Recio Gayo 2019: 40).

Del fundamento del derecho a la privacidad se destaca que su redacción se centra en las intervenciones objetivas-materiales que pudieran llegar a sufrir las personas en su ámbito personal. Sin embargo, en la actualidad las interferencias en el ámbito personal han trascendido a la esfera digital debido a la evolución de las Tic y lo fundamental que se ha vuelto el Internet en el panorama mundial actual. Por tanto, las injerencias de la privacidad de las personas es posible observarlas en el uso de las Tic, específicamente del Internet.

Es importante visualizar que si bien el Internet ha traído consigo una infinidad de ventajas para la humanidad en diversos ámbitos y a su vez una serie de consecuencias entre las cuales se ubica la exposición de la privacidad de las personas, como consecuencia del fácil intercambio de información que ofrecen las tecnologías. El derecho a la privacidad tiene un contenido amplio y a lo largo de la historia definir su contenido ha sido una tarea compleja. Para el desarrollo de este texto, nos ubicaremos en el concepto de la privacidad digital.

Como anteriormente se mencionó el derecho a la privacidad, pareciera centrarse en el mundo físico. Sin embargo, la expansión de las Tic y especialmente del Internet ha generado una especial preocupación sobre la protección y seguridad en el ámbito digital e incluso combinar el aspecto físico y el digital, relacionado con el IoT. El concepto de la privacidad digital, aún es abstracto y se encuentra pendiente de ser desarrollado su contenido de manera precisa (Onu Noticias 2018).

En la Resolución A/C.3/71/L.39 de la Asamblea General de Naciones Unidas sobre el derecho a la privacidad en la era digital se establece que:

1) Todas las personas deben estar protegidas en Internet, incluyendo el derecho a la privacidad.

2) Los Estados tienen la obligación de promover el establecimiento, mantenimiento y fortalecimiento de un entorno abierto, seguro, estable, accesible y pacífico en el ciberespacio.

3) Los Estados deben respetar y proteger el derecho a la privacidad en el contexto de las comunicaciones digitales.

4) Examinar y analizar sobre la base del derecho internacional de los derechos humanos: la promoción y protección del derecho a la privacidad en la era digital, las garantías procesales, la supervisión y recursos nacionales efectivos.

Por otro lado, en el artículo 11 de la Convención Americana sobre Derechos Humanos se establece que:

> "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Del informe de la Relatoría Especial para la Libertad de Expresión (Rele) sobre los estándares para una Internet libre, abierta e incluyente deriva una explicación de cada uno de los aspectos mencionados en el artículo 11 de la Convención en el contexto del Internet.

1) El derecho a la privacidad, conforme a los estándares interamericanos se refiere a que toda persona debe quedar exenta o inmune a invasiones o agresiones abusivas o arbitrarias por parte de terceros o de autoridades.

2) El domicilio de acuerdo a lo desarrollado por la Corte Interamericana de Derechos Humanos se constituye como el ámbito propio o *natural* de desarrollo personal y familiar del individuo.

3) El concepto de correspondencia ha sido ampliado por medio de la jurisprudencia al incluir las comunicaciones telefónicas y a través de nuevas tecnologías como es el Internet (Rele 2016: 74-78).

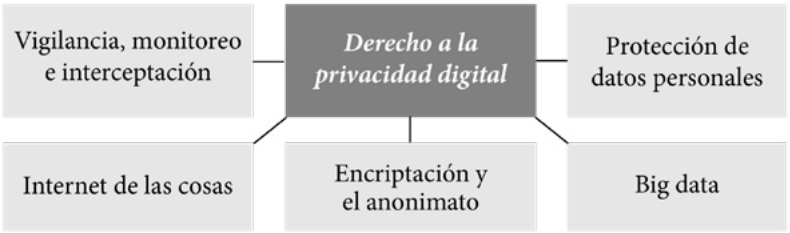
En este sentido, la Comisión Interamericana de Derechos Humanos (Cidh) ha establecido que el derecho humano a la privacidad protege cuatro bienes jurídicos:

> "a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzcan en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen" (Cidh 2013 párr. 130).

De las disposiciones mencionadas con anterioridad, se establece que, al reconocer al Internet como un derecho humano, por ser una necesidad fundamental en la actualidad para todas las personas surgen las obligaciones generales que tienen los Estados, principalmente respetar y proteger este derecho. Al establecer el contenido de las obligaciones, resulta evidente que no solo es asegurar el acceso al Internet, sino que los Estados tienen el deber de proteger la privacidad en la era digital, adoptando las medidas necesarias y adecuadas para ello.

Al surgir el Internet, no solo se obtuvieron ventajas sino también una serie de desafíos que giran en torno a la protección del derecho a la privacidad de las personas. Ya que no solo es asegurar el acceso al Internet, es brindar un acceso seguro en el que no se vean afectados otros derechos humanos. El Internet se ha constituido como una herramienta indispensable para el desarrollo de todas las personas. Al trasladar el derecho a la privacidad en el uso del Internet, se presentan una serie de dificultades (Rele 2016: 85).

1. Principales problemáticas de la protección del derecho a la privacidad digital



Elaboración propia a partir del informe de la Relatoría Especial para la Libertad de Expresión sobre los estándares para una Internet libre, abierta e incluyente 2016.

Desde los estándres de protección del Derecho Internacional de los Derechos Humanos, se observa que existen obligaciones de los Estados de proteger y respetar el derecho humano al Internet y a su vez proteger la privacidad al usar esta herramienta puntuali-

zando cada estándar de este derecho que se genera en el contexto de la era digital. Sin embargo, aún quedan cuestiones por resolver e interpretar debido a los grandes desafíos por la evolución de las tecnologías y su constante expansión.

En este sentido, es difícil establecer un concepto de la privacidad digital. A continuación, se presentan algunas definiciones que han sido desarrolladas. La primera de ellas se refiere a la privacidad en Internet, se define como "la autonomía individual, la capacidad de elegir, de tomar decisiones informadas en otras palabras, a mantener el control sobre diferentes aspectos de nuestra propia vida" (Terwangne 2012: 54).

Actualmente no existe una definición universal de la privacidad en el Internet, otra de las definiciones es que "consiste en determinar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros" (Internet Society 2017: 1). Establecer el contenido del derecho a la privacidad en el Internet, no es sencillo por los diferentes factores que se involucran entre ellos, la constante evolución de las tecnologías, así como el concepto de datos personales en el uso del Internet y su regulación normativa (Piñar Mañas y Recio Gayo 2019: 39 y 40).

Una de las grandes preocupaciones en la protección del derecho a la privacidad en el ámbito digital es la adopción del IoT. A través del tiempo el uso de Internet se caracterizaba por ser comunicaciones humanas que utilizan la web como una plataforma. Ahora la evolución de las tecnologías ha permitido crear objetos capaces de comunicarse entre sí sin la intervención humana. Lo anterior implica que las personas estarán rodeadas de objetos que recopilan información y la comunican a empresas proveedoras de servicio, siendo una red informática que conecta los objetos con la vida de las personas (Rele 2016: 93).

Sin duda, la introducción total del mundo en la tecnología demanda observar y analizar el fenómeno detenidamente, ya que el uso de las Tic involucra una serie de derechos que deben ser pro-

tegidos. Por ejemplo, los Estados no solo tienen la obligación de garantizar el acceso al Internet, sino que deben adoptar todas las medidas adecuadas para proteger y brindar seguridad respecto a otros derechos, entre ellos el derecho a la privacidad.

Específicamente del IoT, en la interacción de una red de datos de una persona y la conexión entre objetos. Es posible observar que la problemática va más allá del intercambio de datos personales. Ahora la conexión con los objetos, permite la invasión del espacio personal por medio de los dispositivos que se encuentran en la red. Es decir, se tiene una realidad virtual de vigilancia "invisible" en la realidad objetiva (Piñar Mañas 2010: 38).

Si bien, el Internet es una de las más importantes innovaciones, pero debido a su evolución y constante actualización resulta ser impredecible desde el ámbito jurídico. Al recordar el origen del Internet, era imposible imaginar que hoy en día existiría una conexión con las cosas de la vida diaria y que se volvería indispensable y fundamental para todas las personas. De esta idea deriva la necesidad de reconocer el Internet como un derecho humano, también la evolución de la realidad social y la necesidad de adecuar la realidad jurídica.

Específicamente, sobre el IoT es necesario hablar de la compatibilidad del reconocimiento y la garantía del derecho humano a la privacidad. Es indispensable ver el concepto del IoT, no solo en el ámbito individual sino también en el colectivo. En el ámbito colectivo, hoy en día encontramos el concepto de ciudades inteligentes, referente al uso de las tecnologías para la mejora de la infraestructura pública. Desde el ámbito jurídico debe existir una regulación que permita proteger el derecho a la privacidad en IoT en el ámbito individual y colectivo.

IV. Propuestas para solucionar el dilema entre la necesidad de privacidad e información

En esta sección se expone una serie de propuestas planteadas anteriormente por académicos o instituciones que podrían tenerse en consideración para resolver el dilema. Se describen las menos verosímiles como son el prohibir completamente o dejar una libertad absoluta que resulta en autorregulación. Lo anterior sólo como un comentario de reflexión académica. De igual manera se habla sobre la respuesta más real y posible que se lleva implementando al menos desde la preocupación por la privacidad derivado del fenómeno *Big data*. Esta hipótesis es la de la regulación por parte de los ordenamientos jurídicos.

1. Las hipótesis de la prohibición y la libertad

La hipótesis de la prohibición es simplemente no permitir la recaudación de datos a través de las cosas inteligentes o prohibir las cosas inteligentes. Como ya se ha visto, el IoT es una tendencia que es muy poco probable que desaparezca. De hecho, las nuevas tecnologías que se van desarrollando tienen como objetivo propiciar que el IoT sea la realidad cotidiana presente en la vida de todas las personas, o al menos de la gran mayoría de estas en el planeta. Por ende pensar que se pueda dar una prohibición como tal en el ordenamiento jurídico de los Estados resulta una idea prácticamente imposible de realizar.

Una hipótesis que no debe ser muy bien vista al momento de regular estas transacciones es el de completa libertad. Una especie de mercado libre de los datos personales. Tal vez en una sociedad más responsable y menos propensa a utilizar sin consideración los datos personales como mercancía podría existir una autorregulación y eso sería suficiente.

De hecho, la autorregulación es la única forma en que se puede dar el supuesto de libertad, la cual se realizaría a través de adop-

ción de códigos éticos, protocolos y otras medidas similares. Esto, en conjunto con las disposiciones de derecho positivo formaría un esquema de heterorregulación (Arellano Toledo 2015: 38). Así pues, la única forma en que sería factible dejar al IoT controlarse de forma propia sería si eso estuviera enmarcado dentro de una normativa de los Estados.

2. La hipótesis de la regulación

La tercera hipótesis de solución del dilema es la de la regulación, y como se adelantaba, es la más obvia, conveniente y realista de las tres hipótesis. Lo anterior debido a que negar por completo o no hacer nada respecto de situaciones fácticas que afectan los derechos de las personas solo trae consigo más problemas e inseguridad jurídica.

Dentro de esta hipótesis es necesario tener en consideración ciertos principios cuyo respeto y observancia son claves. Tales principios son los de:

1) legitimidad y consentimiento, esto significa que para que la obtención y manejo de los datos sea legítima el consentimiento debe ser inequívoco;

2) limitación de la finalidad, que se refiere a que los datos sólo deben ser usados para el fin que fueron recabados;

3) calidad, los datos deben ser adecuados, pertinentes, no excesivos, exactos y actualizados;

4) minimización de los datos, lo que se traduce en que solo deben recabarse datos que sean necesarios para el fin que se utilizarán; e

5) información y transparencia, que se refiere a la posibilidad de la persona de conocer cuáles datos suyos son manejados por los responsables y/o encargados del tratamiento (González Pedraz 2014: 3).

En las siguientes líneas se hablará de ejemplos de regulación sin una relación aparente más que la de ejemplificar la tendencia más aceptada para resolver el problema que presenta el flujo masivo de datos y el IoT.

A nivel continental se tiene, por ejemplo, el Reglamento general de protección de datos de la Unión Europea (en adelante el Reglamento) que entró en vigor el 24 de mayo de 2016 y comenzó su aplicación el 25 de mayo de 2018, para dar tiempo a que organizaciones, empresas e instituciones se adaptaran para el cumplimiento del mismo. En este Reglamento ya se encuentran regulaciones respecto al manejo de los datos digitales de las personas y novedades como el derecho al olvido (artículo 17) y la portabilidad de datos (artículo 20). Esta regulación aplica tanto a particulares como a autoridades de los Estados miembros de la Unión Europea.

En tal Reglamento también se habla de un concepto necesario para garantizar los derechos a la privacidad de las personas, el cual ya se había mencionado y este es el *consentimiento informado*, que se regula en el artículo 7. El consentimiento informado no es otra cosa más que aceptar o negar una situación o condición a conciencia, teniendo a la mano toda la información posible, tanto positiva como negativa y las implicaciones de lo que se está aceptando o negando.

En la regulación del IoT es de suma importancia prestar atención al consentimiento libre e informado, puesto que es con este consentimiento con que comienza la recepción de datos de quienes usan las cosas inteligentes. Pensamos que la mejor forma de atender dicha cuestión debe ser con una separación entre la voluntad de usar el dispositivo inteligente y la voluntad de recabar ciertos datos. Esta última debe ser siempre explícita y no se debe dar por sentado que el emplear dispositivos inteligentes es equivalente a un consentimiento de recabar todos los datos posibles por el citado objeto.

En México hasta 2016 existía la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010, la cual sólo establecía las obligaciones para el sector privado. Sin embargo, se podía entender que las mismas disposiciones establecidas en la Ley aplicaban para las obligaciones del Estado mexicano en cuanto al tema (Arellano Toledo 2015: 43). Posteriormente en enero de 2017 se promulgó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual ya regulaba la actuación de las autoridades federales que manejan datos de las personas en el país.

Ambas leyes y las obligaciones señaladas en las mismas recogen lo estipulado por los artículos 6, 7 y 16 de la Constitución mexicana. Estos artículos establecen el derecho de libertad de expresión, que abarca también el de recibir información, el derecho de expresar tales ideas a través de cualquier medio, incluyendo los digitales, así como el derecho a la privacidad, en donde se encuadra la obligación de protección de los datos personales.

V. Conclusiones

Derivado de la investigación presentada se observa que la situación vivida a raíz de la conexión masiva de objetos, así como del fenómeno *Big data* es bastante compleja. En esta realidad se entrelazan los intereses de empresas, gobiernos y particulares. Estos intereses son enteramente benéficos para la vida de los usuarios pues ayudan a cumplir con el derecho humano al Internet. Sin embargo, también benefician económicamente a las empresas privadas y son excelentes herramientas de control para los gobiernos. Es necesario hacer visible esta novedosa problemática, pues el IoT es una realidad que ha llegado para quedarse, al menos en los próximos años y muy probablemente pueda surgir una transformación aún no previsible de la situación en años más lejanos.

Actualmente las tecnologías se han vuelto fundamentales en la vida de las personas, específicamente el uso del Internet. El IoT involucra una interacción entre lo físico y lo digital por medio de una red, facilitando los procesos de intercambio de información e impactando en la eficacia de las actividades cotidianas. Sin duda, la evolución de las tecnologías ha traído consigo muchas ventajas.

Por un lado, los Estados tienen la obligación de garantizar el acceso al Internet a todas las personas, al ser un derecho en sí mismo y a la vez vehículo para alcanzar otros derechos humanos. Pero en un contexto de constante evolución, surge la necesidad de conocer y analizar qué prerrogativas se involucran. Uno de los que se ve involucrado es el derecho a la privacidad, esto se relaciona con una serie de desventajas relacionadas con los avances tecnológicos, donde la privacidad se ve en riesgo.

En este sentido, los Estados no solo tienen la obligación de brindar el acceso al Internet, sino que deben garantizar la protección y la seguridad en el ámbito de la privacidad de todas las personas. El Internet debe ser un espacio seguro, que permita proteger la privacidad. Sin embargo, el IoT presenta una serie de dificultades para garantizar de manera efectiva el derecho a la privacidad, que tienen que ser analizadas desde la óptica jurídica.

El IoT y el flujo masivo de información que se genera gracias a este no hará más que aumentar en los años venideros. Cada vez más objetos se suman a la larga lista de cosas inteligentes y las personas están más que dispuestas a seguir utilizando estos mismos pese a los riesgos de privacidad que puedan suponer. Es deber de los Estados el atender la realidad presente de las personas bajo su custodia y para ello se requiere de una regulación que tome en cuenta el IoT y sus implicaciones en la vida privada de las personas.

La forma en que estas nuevas y rápidamente cambiantes tendencias se vigilarán depende de entender las realidades contemporáneas. Realidades donde se comunican e interconectan con más

facilidad millones de personas en el mundo y sus aparatos inteligentes. Sólo haciendo eso es que se podrá garantizar efectivamente el derecho a la privacidad de las personas en una era que no parece desaparecer pronto del panorama, la era del *Internet de las cosas*.

Bibliografía

Arellano Toledo, Wilma (2015): "Gobierno abierto y privacidad: la problemática del Big data y el cómputo en la nube", en *Virtualis*, vol. 5, núm. 10, 34-59.

Baig, Edward C. (2020): "Nuevos relojes inteligentes monitorean la salud en vez de la actividad física", en *AARP*, 28 septiembre. Disponible en: «*https://www.aarp.org/espanol/hogar-familia/tecnologia/info-2020/nuevos-relojes-inteligentes.html*» [Consultado el 4 de febrero de 2022].

Bonilla Fabela, Isaias, *et al.* (2016): "IoT, el Internet de las cosas y la innovación de sus aplicaciones", en *VinculaTégica*, año 2, núm. 1, 2313-2340.

Conner, Margery (2010): *Sensors empower the Internet of Things*, en página web de EDN, 27 mayo. Disponible en: «*https://www.edn.com/sensors-empower-the-internet-of-things/*» [Consultado el 8 de febrero de 2022].

Comisión Interamericana de Derechos Humanos. *Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV* (Libertad de Expresión e Internet).

Dw Documental (2022): *El internet de las cosas - nuestra relación con Internet | DW Documental*, en página web YouTube, 16 enero. Disponible en: «*https://youtu.be/iUbR046La68*» [Consultado el 27 de enero de 2022].

Evans, Dave (2011): *Internet de las cosas, Cómo la próxima evolución de Internet lo cambia todo*, Cisco. Disponible en: «*https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf*» [Consultado el 4 de febrero de 2022].

Gil González, Elena (2016): *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Agencia Estatal Boletín Oficial del Estado, Madrid.

González Pedraz, Judith (2014): "Big Data y bibliotecas: convertir datos en conocimiento", en *IV Jornada Profesional de la Red de Bibliotecas del Instituto Cervantes*, vol. 7, 1-5.

Harari, Yuval Noah (2019): *Obra completa: Pack con: Sapiens | Homo Deus | 21 lecciones para el siglo XXI*, Debate, Edición Kindle.

Internet Society (2017): *Introducción a la privacidad en Internet.* Disponible en: «*https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-Privacy-20151030-es.pdf*» [Consultado el 20 de febrero de 2022].

Khodadadi, Farzad *et al.* (2017): *Internet of things: An overview,* en página web de Arxiv, 19 marzo. Disponible en: «*https://arxiv.org/abs/1703.06409*» [Consultado el 10 de febrero de 2022].

Kuneva, Meglena (2009): *Targeting and Profiling*, Roundtable on Online Data Collection, Unión Europea, Bruselas.

Mora González, Sonia (2015): "Entendiendo el Internet de las cosas Internet of Things (IoT)", en *Investiga Tec.*, núm. 24, 22-23.

Morte Ferrer, Ricardo (2017): "Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca", en *Dilemata*, núm. 24, 219-233.

Onu noticias (2018): *Artículo 12: derecho a la intimidad*. Disponible en: «*https://news.un.org/es/story/2018/11/1446671#:~:text=-Nos%20permite%20protegernos%20de%20las,nuestras%20comunicaciones%20y%20a%20nuestra%20informaci%-C3%B3n*» [Consultado el 16 de febrero de 2022].

Orlowski, Jeff (2020): *The social dilemma*, prod. por Adelman Hallee et. al, Estados Unidos.

Piñar Mañas, José Luis y Recio Gayo, Miguel (2019): "La privacidad en internet" en *La Constitución en la sociedad y economía digitales,* Recio Gayo, Miguel (coord.), Suprema Corte de Justicia de la Nación, México, 37-87.

Piñar Mañas, José Luis (2010): "¿Existe la privacidad?" en *Protección de datos personales. Compendio de lecturas y legislación*, colección Inai, 16-55.

Redacción Bbc Mundo (2018): "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día", en Bbc News, 20 marzo. Disponible en: «*https://www.bbc.com/mundo/noticias-43472797*» [Consultado el 18 de febrero de 2022]

Relatoría Especial para la Libertad de Expresión (2016): *Estándares para una Internet abierta e incluyente*, Organización de los Estados Americanos, Estados Unidos.

Salazar Jaramillo, Rafael (2014): "Derechos humanos e internet, derecho al olvido, internet y bien público", en *Revista UPTC*, núm. 24, 279-288.

Sánchez Duarte, Esmeralda (2008): "Las tecnologías de la información y comunicación (Tic) desde una perspectiva social", en *Revista electrónica Educare*, vol.XII. 155-162.

de Terwangne, Cécile (2012): "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido" en *Revista de Internet, Derecho y Política*, núm. 13. 53-66.

Trigo Aranda, Vicente (2014): "Historia y evolución del internet", en *Revista de la Asociación de Autores Científico-Técnicos y Académicos*, núm. 33. 22-32.

Wachter, Sandra (2018): "Normative challenges of identification on the Internet of Things: Privacy, profiling, discrimination, and the Gdpr", en *Computer Law & Security Review: The International Journal of Technology Law and Practice*, vol. 34, núm. 3, 436-449.

Zheng, Serena *et al.* (2018): "User Perceptions of Smart Home IoT Privacy", en *Proceedings of the Acm Hum. -Comput. Interact.*, vol. 2, núm. Cscw, 200:1-200:20.