# SEGURIDAD DE PRODUCTOS DE CONSUMO EN EL INTERNET DE LAS COSAS

## DOCUMENTOS SOBRE ECONOMÍA DIGITAL DE LA OCDE

Marzo 2018 **Núm. 267**


Traducido con el apoyo de

Asociación de Internet.mx

Microsoft

OCDE
MEJORES POLÍTICAS PARA UNA VIDA MEJOR

# *Prólogo*

Este informe evalúa los beneficios y los desafíos de seguridad para productos de consumo planteados por el Internet de las Cosas. Fue desarrollado por el Grupo de Trabajo sobre la Seguridad de los Productos de Consumo (WPCPS, por sus siglas en inglés) como seguimiento de su trabajo acerca de la seguridad de los productos en línea y como complemento del trabajo del Comité de Políticas de Consumo (CCP, por sus siglas en inglés) acerca de las Políticas de Consumo en el Hogar Inteligente.

El informe fue elaborado por Rod Freeman, abogado internacional de seguridad de productos y socio en Cooley (Reino Unido) en colaboración con Brigitte Acoca del Secretariado de la OCDE.

El informe se benefició de una contribución financiera por parte del gobierno de Corea. El CCP lo desclasificó mediante un proceso escrito que concluyó el 2 de marzo de 2018.

Esta publicación es una contribución al proyecto "Going Digital" de la OCDE, cuyo objetivo es proporcionar a los responsables de políticas, herramientas que necesitan con el fin de que sus economías y sociedades prosperen en un mundo cada vez más digital y basado en datos.

Para más información visite www.oecd.org/going-digital.
#GoingDigital



Publicado originalmente por la OCDE en inglés bajo el título: OECD (2018), "Consumer product safety in the Internet of Things", OECD Digital Economy Papers, No. 267, OECD Publishing, París, https://doi.org/10.1787/7c45fa66-en.



Este documento, así como todos los datos y mapas aquí incluidos, se entenderán sin prejuicio respecto al estatus o soberanía de cualquier territorio, a la delimitación de las fronteras y límites internacionales ni al nombre de cualquier territorio, ciudad o área.

# *Presentación a la edición en español*

Conforme avanza el creciente uso de los consumidores de dispositivos y aplicaciones que operan en entornos del Internet de las Cosas ("Internet of Things" o IoT), queda claro que uno de los temas regulatorios críticos en la materia tiene que ver con la seguridad de los productos que aprovechan IoT. Ya sea que estos productos se estén extendiendo, tanto en el marco de seguridad de productos de consumo en el ámbito nacional como internacional, las regulaciones se están adecuando para atender estas cuestiones y riesgos emergentes. Este es uno de los principales aspectos que han sido explorados por el grupo de trabajo de la OCDE sobre seguridad de productos de consumo, de hecho, en la mayoría de los países de la OCDE, la seguridad de los productos tiende a regular bienes físicos "terminados" más que a los dispositivos IoT, los cuales son de naturaleza dinámica y pueden evolucionar a lo largo de su ciclo de vida, por ejemplo, una actualización de software. Estos productos, que podrían ser seguros al salir al mercado, podrían no serlo posteriormente.

En este contexto cambiante, la gestión de la seguridad de los productos IoT, es fundamental, el hackeo de este tipo de bienes podría, por ejemplo, tener serias implicaciones en la salud y la seguridad física de los consumidores. Otra cuestión importante que requiere claridad es la responsabilidad del fabricante del producto, la cual, en la compleja actualidad de las cadenas de suministro de productos IoT, podría ser difícil de comprender por aquellos consumidores perjudicados.

No cabe duda de que la seguridad de productos y aplicaciones de consumo en el entorno de IoT requiere un enfoque específico, como se destaca en el estudio "Seguridad de productos de consumo en el Internet de las Cosas", presentado originalmente en inglés bajo el título "*Consumer Product Safety in the Internet of Things"*, como parte de la iniciativa *Going Digital* de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

El tema es crucial, pues cada vez con mayor frecuencia, tanto los usuarios de IoT como los reguladores y formuladores de políticas públicas, enfrentarán nuevos casos de uso de IoT —incluidas situaciones en las que los usuarios posiblemente no sean conscientes de que están interactuando con un dispositivo de IoT— que plantearán continuas preguntas sobre cómo debemos gestionar las necesidades de seguridad junto con las oportunidades para la innovación.

Por todo ello, la Asociación de Internet MX y Microsoft México se enorgullecen en presentar la edición en español del presente documento, con la certeza de que será una herramienta útil para contribuir al diseño de marcos normativos y de política pública en materia de seguridad en IoT.

Guadalajara, Jalisco, a 3 de diciembre de 2019.

Asociación de Internet MX
Enrique Culebro Karam
Presidente

Microsoft México, S. de R.L. de C.V.
Enrique Perezyera
Director General

# *Índice*



## Figuras



* IoT es el acrónimo en inglés del Internet de la cosas.

# *Resumen ejecutivo*

No existe una definición acordada de manera global de lo que abarca el Internet de las cosas (IoT, por sus siglas en inglés). La OCDE se refiere a esto como *"un ecosistema en el que las aplicaciones y los servicios se basan en datos recopilados de dispositivos que detectan e interactúan con el mundo físico"*, (OCDE, 2016[1]). El IoT incluye (OCDE, 2015[2]):

> *... dispositivos y objetos cuyo estado se puede modificar a través de Internet, con o sin la participación activa de individuos. Esto incluye laptops, enrutadores, servidores, tabletas y teléfonos inteligentes* (smartphones)*, que a menudo se consideran parte del "Internet tradicional". Sin embargo, estos dispositivos son parte integral de la operación, lectura y análisis del estado de los dispositivos del IoT y frecuentemente constituyen el "corazón y cerebro" del sistema. Como tal, no sería correcto excluirlos.*

Las tecnologías asociadas incluyen la inteligencia artificial, el cómputo en la nube y cadena de bloques. Existen cuatro categorías generales de bienes y servicios de consumo ("productos") que dependen de las tecnologías del IoT. Estos incluyen dispositivos portátiles, dispositivos y aplicaciones domésticas inteligentes, juguetes y equipos de cuidado infantil así como automóviles conectados. Estos productos a menudo combinan el uso de sensores con la recopilación y el análisis de datos para permitir sistemas autónomos e inteligentes que no solamente pueden interactuar entre sí, sino también con las personas.

La falta o variación de las definiciones del IoT ha dificultado la medición del mercado. Sin embargo, los datos disponibles parecen sugerir que los mercados de consumo para los productos del IoT deberían seguir creciendo, impulsados por una serie de beneficios percibidos tanto para los consumidores como para las empresas. Para los consumidores, el IoT ofrece una mayor selección de productos, seguridad, conocimientos sobre los hábitos de consumo y ahorro de costos, comodidad y personalización. Para las empresas, los beneficios incluyen mayores posibilidades para dar seguimiento y rastrear productos en las cadenas de suministro globales así como en ayudar a los fabricantes y otros actores del IoT para la identificación y mitigación de los riesgos.

Si bien estas tecnologías podrían mejorar potencialmente la calidad de los productos y prevenir o reducir los riesgos para la seguridad de los productos de consumo, también introducen nuevos riesgos de seguridad, en los que los esquemas de responsabilidad y regulatorios de seguridad de productos existentes pueden estar mal preparados para solventarlos. Por lo tanto, es importante que la seguridad de los productos de consumo sea prioritaria en el orden de las personas encargadas de dictar políticas con el fin de garantizar que se pueda aprovechar todo el beneficio que dichas tecnologías ofrecen.

Existe un argumento de que el IoT presenta nuevos desafíos para la seguridad del producto y que los esquemas regulatorios deberán adaptarse. No obstante, existe un contraargumento que si bien los productos son nuevos, los problemas no son necesariamente nuevos y las regulaciones existentes son suficientes. Al considerar estos dos enfoques, será necesario establecer un equilibrio entre asegurar un alto nivel de seguridad de los productos de consumo y asegurar que la innovación no sea innecesariamente sofocada, lo que dará como resultado la privación a los consumidores de nuevas tecnologías que podrían mejorar la seguridad de los productos.

Este informe no busca obtener conclusiones finales o hacer recomendaciones de políticas específicas. Está previsto para resaltar algunos de las cuestiones clave que enfrentan las

personas encargadas de dictar políticas de seguridad de productos en esta importante área, las cuales son las siguientes:

- En qué medida los marcos regulatorios de seguridad del producto abordan adecuadamente los riesgos y desafíos de seguridad del producto asociados con el IoT?
- Si en los regímenes de seguridad del producto se necesitan cambios, ¿en qué grado también se requieren cambios en los regímenes de responsabilidad civil derivada de productos defectuosos?
- Teniendo en cuenta la complejidad de las cadenas de suministro del IoT:
  a. ¿Quién debería ser responsable de la certificación y el cumplimiento de la seguridad (tanto inicialmente como de forma continua)?
  b. ¿Cómo deberían los consumidores identificar a la(s) parte(s) responsable(s)?
  c. ¿Cuál debería ser el alcance de esas responsabilidades?

# *Seguridad de productos de consumo en el Internet de las cosas*

## 1. Introducción

A pesar de la disminución en el crecimiento de la productividad en los últimos años, han surgido nuevos mercados digitales de consumo a nivel mundial, impulsados por el desarrollo y la difusión de una gama de productos y procesos de producción basados en tecnología innovadora y en evolución. Estos incluyen el IoT, el cual está habilitado por la convergencia de conectividad de red, interconexión de máquina a máquina ("M2M")[1], software integrado en la máquina, recopilación y análisis de datos ("macrodatos"), así como tecnología, como la inteligencia artificial, cadena de bloques y cómputo en la nube.

Si bien no existe una definición internacionalmente acordada del IoT, el concepto se entiende como un ecosistema en el que los dispositivos y otros objetos están directamente conectados a internet o están mediados a través de redes de área local o extendida. Dichos dispositivos y objetos incluyen sensores y actuadores que, en combinación con el análisis de macrodatos y el cómputo en la nube, hacen posible máquinas autónomas y sistemas inteligentes. Los datos pueden usarse para analizar patrones, anticipar cambios y alterar un objeto o entorno para obtener el resultado deseado, a menudo de forma autónoma. Como tal, el IoT permite interacciones no solo entre dispositivos y objetos, sino también entre individuos en entornos informáticos que pueden aprovechar servicios nuevos e innovadores (OCDE, 2016[1]; OCDE, 2017[3]). Una variedad de actores están involucrados en el mercado del IoT, incluidos fabricantes de productos y sensores, productores de software, diseñadores, proveedores de infraestructura y empresas de análisis de datos. Los datos disponibles muestran que el mercado del IoT para productos de consumo está aumentando rápidamente, impulsado por la creciente disponibilidad de una variedad de productos innovadores, que van desde "dispositivos portátiles" (como pulseras para ejercicio) hasta aplicaciones para "hogares inteligentes" que enlazan electrodomésticos y dispositivos para el hogar.

Además de ofrecer una mayor variedad de productos y conveniencia a los consumidores, se espera que el IoT revolucione la forma en que los procesos de diseño, fabricación y entrega de productos se supervisen, analicen y mejoren, incluso de manera remota.

Las agencias responsables de la política de seguridad de productos en todo el mundo intentan comprender cada vez más las implicaciones del IoT para la seguridad de los productos. Por un lado, existe interés en el potencial de que dichas tecnologías den lugar a nuevos riesgos de seguridad, y cuestionan si los regímenes regulatorios existentes de seguridad de productos y responsabilidad sean los adecuados. Por otro lado, existe un interés creciente en las oportunidades que ofrecen dichas tecnologías para mejorar la calidad de los productos, para ayudar a prevenir los peligros o daños a la seguridad de los productos de consumo y para crear mejores formas de gestionar la seguridad en la cadena de suministro y en el mercado. Esto, por sí mismo, da lugar a desafíos políticos, ya que surgen cuestiones sobre cómo la política regulatoria de seguridad de productos y responsabilidad puede, o debe, adaptarse para facilitar la entrega de estos beneficios a las comunidades de todo el mundo.

Garantizar que los consumidores puedan beneficiarse de productos habilitados por el IoT seguros será un punto clave para construir y mantener la confianza en este mercado emergente. El crecimiento requerirá, en particular, que los gobiernos y otros actores aumenten la cooperación de manera internacional y evalúen el cumplimiento de los nuevos modelos de negocios digitales del IoT con los marcos de políticas de seguridad de productos de consumo existentes (Ley 360 [Law 360], 2016). Tal como lo enfatizaron la comisionada de la CE, Jourova y el presidente Kaye, de la Comisión de Seguridad de Productos de Consumo de EE. UU. (CPSC, por sus siglas en inglés) en la sesión plenaria del IoT de la Organización Internacional de Seguridad y Salud de Productos de Consumo (ICPHSO, por sus siglas en inglés), celebrada en Bruselas en noviembre de 2016, el cómo dichos marcos tengan que ser adaptados para satisfacer las realidades de las cadenas de suministro globales transformadoras, sin sofocar la innovación, requerirá una atención especial. Esto puede incluir la revisión de cómo los conceptos clave de seguridad del producto de consumo (como "producto", "seguridad", "defecto", "daño" y "responsabilidad") pueden comprenderse en un entorno en el que: i) los productos pueden llegar a ser potencialmente defectuosos e inseguros como resultado de incidentes de seguridad digital; y en el que cada vez más pueden adoptar, anticipar y predecir decisiones sin intervención humana; y ii) los nuevos medios de comunicación y recopilación de datos pueden crear nuevas oportunidades pero también riesgos a los consumidores.

Este informe describe los desarrollos actuales y emergentes del IoT que pueden tener implicaciones para el diseño y la ejecución de políticas de seguridad de productos de consumo. Contiene tres secciones centradas respectivamente en: (i) conceptos del IoT y tendencias generales; (ii) beneficios clave y riesgos de seguridad de productos de consumo emergentes; y (iii) desafíos políticos relacionados. El documento pretende resaltar los problemas que enfrentan los responsables de políticas de seguridad de productos en esta importante área. No busca sacar conclusiones finales o hacer recomendaciones de políticas específicas; tampoco cubre en detalle los diversos problemas de la política del IoT que pueden tener implicaciones directas de seguridad del producto, pero que caen fuera del área de seguridad del producto de consumo, como la privacidad y la seguridad.

# 2. Conceptos y tendencias del IoT

A continuación se proporciona una descripción general de los conceptos y definiciones clave del IoT; también se identifican las principales categorías de productos del IoT para uso de los consumidores y las tendencias de mercado relacionadas.

## 2.1. Definiendo el IoT y conceptos relacionados

No existe una definición acordada de manera global de lo que el IoT abarca de manera interna. La OCDE lo ha descrito de manera extensa como *"un ecosistema en el que las aplicaciones y los servicios se basan en datos recopilados de dispositivos que detectan e interactúan con el mundo físico"* (OCDE, 2016[1]). Incluye (OCDE, 2015[2]):

> *... dispositivos y objetos cuyo estado se puede modificar a través de Internet, con o sin la participación activa de individuos. Esto incluye laptops, enrutadores, servidores, tabletas y teléfonos inteligentes, que a menudo se consideran parte del "Internet tradicional". Sin embargo, estos dispositivos son parte integral de la operación, lectura y análisis del estado de los dispositivos del IoT y frecuentemente constituyen el "corazón y cerebro" del sistema. Como tal, no sería correcto excluirlos.*

El IoT se entiende como una infraestructura de red global dinámica con capacidades de autoconfiguración basadas en protocolos de comunicación estándar e interoperativas donde los "objetos" virtuales y físicos tienen identidades, atributos físicos y personalidades virtuales, utilizan interfaces inteligentes y se integran sin problema en la red de información. (Alianza para la Innovación del Internet de las Cosas (AIOTI), 2015[4]). También se ha resumido que el IoT abarca los tres elementos siguientes: (1) los "sensores" que recopilan datos sobre nosotros y nuestro entorno (como los termostatos inteligentes, sensores de calles y autopistas); (2) los "inteligentes", que determinan qué significan los datos y cómo responder a ellos. Estos incluyen todos los procesadores de computadora en los dispositivos del IoT y, cada vez más, en la nube, así como la memoria que almacena toda esta información; y (3) los "actuadores" que afectan el dispositivo y el entorno; el punto de un termostato inteligente no se limita, por ejemplo, al registro de la temperatura, sino también a controlar otros dispositivos, como un aire acondicionado (Schneier, 2017[5]).

Algunos mencionan a menudo que el IoT es la "tercera ola" del internet, después de la revolución de internet de escritorio (la primera ola) y la conexión de personas a internet a través de sus dispositivos móviles (la segunda ola) (Jankowski, 2014[6])

Para los fines de este informe, se entiende que el IoT cubre los productos de consumo que están conectados, o al menos tienen la capacidad para conectarse, a internet y, a través de dicha conectividad el comportamiento de los productos puede ser alterado, incluyendo, potencialmente, su seguridad. A medida que se consideran las implicaciones políticas del IoT, es prudente suponer que las categorías de productos que abarca el IoT junto con las tecnologías utilizadas y las formas en que se utilizará la "conectividad" de tales productos, están sujetas a cambios y desarrollo constantes, quizás en formas que actualmente son impredecibles.

## 2.2. Tendencias en productos y mercados del IoT

Esta sección describe los principales dispositivos y aplicaciones habilitados para el IoT utilizados por los consumidores según el estado actual de la tecnología y la comercialización.

También examina las tecnologías que son compatibles, complementan y ayudan a mejorar el IoT y exploran las tendencias recientes del mercado.

### *2.2.1. Dispositivos y aplicaciones del IoT*

El mercado de consumo actualmente alberga una gran variedad de dispositivos y aplicaciones conectados al IoT. Dado que el IoT aún es naciente, muchas más tecnologías aún inimaginables pueden estar a la vuelta de la esquina, lo que podría generar cambios en la productividad, los impactos ambientales así como nuevos productos, servicios y modelos de negocios (OCDE, 2016[1]). A continuación, se incluyen descripciones de varias categorías generales de dispositivos que se encuentran actualmente en el mercado, los cuales incluyen: (i) dispositivos portátiles, monitores de salud y dispositivos implantables; (ii) aplicaciones domésticas inteligentes; (iii) juguetes y equipos de cuidado infantil; y (iv) automóviles conectados.

#### *Dispositivos portátiles, monitores de salud y dispositivos implantables*

Una de las categorías más importantes y de rápido desarrollo de dispositivos de IoT orientados al consumidor, en este momento, es la tecnología portátil. Son exactamente como suenan: dispositivos, conectados al IoT que usan los consumidores por diversas razones. Los dispositivos portátiles incluyen los reconocidos "relojes inteligentes" que a menudo se usan junto con un teléfono inteligente, así como los monitores de ejercicio y estado físico más básico. También se incluyen dispositivos que dan a conocer información no solo del funcionamiento del objeto en sí, sino también de las personas y otros objetos con las que interactúa. Este es especialmente el caso de los monitores de salud, que recopilan y analizan datos sobre la fisiología y la salud de un individuo. El mercado de los dispositivos portátiles también incluye un conjunto más amplio de productos emergentes, como anteojos tipo gafas que brindan información a los consumidores, despliegan cámaras y otras tecnologías de grabación o, utilizando tecnología en desarrollo, operan en el espacio de "realidad aumentada". También incluye productos que han instalado, por ejemplo, rastreadores del sistema de posicionamiento global (GPS) en productos, como zapatos o ropa.

En relación con dispositivos portátiles están los dispositivos que son ingeridos o implantados directamente en los consumidores. Conocidos como el "Internet de los Seres Vivos", estos dispositivos se están desarrollando principalmente para controlar enfermedades crónicas como la diabetes y las enfermedades cardiacas (Information Age, 2015[7]). También pueden utilizarse para detectar accidentes, ataques, convulsiones o ataques cardiacos y alertar a los servicios de emergencia. Además, dichos dispositivos pueden recopilar información sobre la toma de medicamentos, la actividad y los patrones de sueño de los pacientes, así como medir la presión arterial, los niveles de glucosa y la frecuencia cardiaca (OCDE, 2016[1]). Estos dispositivos ayudan en gran medida a los médicos en el desarrollo y la adaptación de los planes de tratamiento para sus pacientes, y también ayudan a garantizar que los centros de atención de urgencias estén reservados solo para verdaderas emergencias (OCDE, 2016[1]; Murray, 2015[8]).

Como se pondrá de manifiesto a partir de las descripciones anteriores, los dispositivos portátiles que tienen funciones relacionadas con la salud y el bienestar del consumidor pueden considerarse dispositivos médicos, y estarán sujetos a regulaciones específicas que existen en la mayoría de las jurisdicciones para esa clase de producto. El considerar las implicaciones de los productos que se encuentran dentro de dichos regímenes regulatorios se encuentra más allá del alcance de este artículo, con la excepción a la nota de que el

"cruce" de dispositivos portátiles en el campo de los dispositivos médicos, puede volverse más común a medida que los productos de consumo portátiles se vuelvan cada vez más funcionales y capaces de proporcionar una mayor variedad de datos para el consumidor.

CCS Insight predijo que el mercado de dispositivos portátiles alcanzaría los USD 14 mil millones para fines de 2016, y Business Insider espera que el mercado totalice 162.9 millones de unidades para fines de 2020 (Meola, 2016[9]). El mercado global de dispositivos portátiles se estima en un total de 230 millones de envíos de unidades en 2018, con un flujo de ingresos de USD 32 mil millones, frente a los USD 10 mil millones en 2013 (Walker y Roashan, 2015[10]).

### *Aplicaciones domésticas inteligentes*

Otra categoría importante y diversa de dispositivos y aplicaciones del IoT está en la configuración del hogar[2]. Los dispositivos incluyen: termostatos inteligentes que pueden rastrear el uso y los patrones de energía; electrodomésticos inteligentes que pueden regular las operaciones de forma remota (como hornos que los consumidores pueden encender antes de llegar a casa); cerraduras y otros sistemas de seguridad inteligentes; sensores para detectar inundaciones, humo o dióxido de carbono; televisores inteligentes; y los "concentradores domésticos" que están conectados y que aparte de proporcionar información a los consumidores, les pueden permitir controlar, mediante comandos de voz, otros dispositivos del IoT domésticos como iluminación inteligente, sistemas de seguridad, termostatos inteligentes y televisores inteligentes de alta definición.

El "hogar inteligente" es un sector de rápido desarrollo en el IoT, y es significativo desde la perspectiva de la política de seguridad de los productos, ya que incorpora productos domésticos "tradicionales" a esta área de nueva tecnología. A medida que los productos de uso diario, tales como electrodomésticos y pequeños aparatos eléctricos, se desarrollan con tecnologías que les permiten estar "conectados" y sus funciones afectadas por insumos externos, la gestión de la seguridad de esos productos se vuelve más complicada, y puede plantear nuevos problemas desde una perspectiva de políticas.

### *Juguetes y equipos de cuidado infantil*

Esta categoría abarca tanto los dispositivos utilizados por los niños para jugar, como los dispositivos utilizados por sus padres para controlar su seguridad y salud.

Actualmente, los juguetes avanzados para niños en el mercado incluyen variedades de muñecas y criaturas de juguete que pueden cambiar su comportamiento para entretener (como por ejemplo, recordar las respuestas dadas por un niño, saber qué hora es o dar un pronóstico del tiempo, y de otra manera adaptarse a las respuestas del niño); juegos de construcción que permiten a los niños construir aparatos programables; y tabletas especialmente diseñadas que tienen varias características que permiten a los niños interactuar con su entorno en diferentes maneras (incluso mediante la carga de fotos y documentos para personalizar) (Telefónica, 2016[11]). No obstante, productos aun más complejos y avanzados se encuentran en desarrollo. Por ejemplo, las impresoras 3D diseñadas para permitir que un niño haga sus propios juguetes simples en el hogar ya están en el mercado, con la probabilidad de que se desarrolle aún más esta tecnología.

Las clases de dispositivos relacionadas y que a menudo se superponen son aquellas que supervisan la seguridad y la salud de un niño. Algunos de estos dispositivos son simplemente cámaras o micrófonos conectados a internet para fines de supervisión remota. Otros pueden proporcionar más información, como un juguete que contiene un sensor que transmite simultáneamente a los padres información sobre la ubicación del niño, la temperatura

corporal y la frecuencia cardiaca. Otro ejemplo es un asiento de seguridad para niños que contiene sensores para alertar a los padres sobre la condición física de sus hijos, en el caso de que el niño se encuentre solo en un automóvil y este pueda sobrecalentarse. La naturaleza "conectada" de dichos productos brinda beneficios obvios para los consumidores, incluido un entorno más seguro para los niños.

Dada la naturaleza vulnerable del grupo objetivo de consumidores, las consideraciones de seguridad son particularmente graves en esta categoría. De las preocupaciones potenciales que se relacionan con los productos del IoT en general, hay algunas que se enfocan más en el contexto de los productos utilizados por los niños y dirigidos a ellos. La protección de datos y las preocupaciones sobre la privacidad con respecto a los datos personales de un niño (es decir, quién lo usa, quién tiene acceso a él y con qué propósito) pueden ser más sensibles, en particular cuando un niño pueda ser menos consciente de los riesgos al compartir ciertos datos personales en línea. Estas consideraciones pueden tener implicaciones de seguridad genuinas y al mismo tiempo plantean problemas de privacidad.

De manera más general, la funcionalidad de un juguete que permite modificar su funcionamiento a lo largo de su vida útil puede generar implicaciones de seguridad particulares. Por ejemplo, la funcionalidad nueva o modificada puede dar lugar a la necesidad de que se le den nuevas instrucciones al niño, lo que, por consecuencia, puede requerir un mayor nivel de supervisión por parte de un adulto en relación con el uso del juguete en general.

#### *Automóviles conectados*

Los automóviles se están conectando cada vez más a internet, por motivos tales como: advertencias a los conductores sobre condiciones meteorológicas o de camino peligrosas; diagnósticos en tiempo real de la condición del automóvil e incluso permitiendo que el vehículo sea operado de forma remota o autónoma (OCDE, 2016[1]). También se están desarrollando y comercializando tecnologías que permiten que el vehículo de un consumidor se conecte con otros dispositivos, incluso con tecnologías basadas en el hogar. Por mencionar, se está comercializando una tecnología que permite a los usuarios controlar productos domésticos inteligentes desde sus vehículos, por ejemplo: al activar acciones rutinarias personalizadas (como apagar las luces o ajustar el termostato); mostrar el estado de alarmas de humo o de seguridad; y hacer que la puerta del garaje se abra cuando el conductor se acerque a su casa.

La OCDE espera que esta mayor conectividad cambie de manera drástica el mercado automotriz global. La investigación de mercado sugiere que la participación de mercado de los automóviles automatizados y autónomos aumentará considerablemente en las próximas décadas; Cisco, por ejemplo, predice que crecerá de una participación de mercado del 0.1% en 2020 a más del 35% para 2040 (OCDE, 2016[1]).

### *2.2.2. Tecnologías complementarias*

El IoT también incorpora una gama de nuevas tecnologías que mejoran la funcionalidad de los productos y crean nuevas oportunidades para proporcionar beneficios a los consumidores e incluso crear nuevos mercados para productos que no existían anteriormente. Esto incluye tecnologías tales como inteligencia artificial, cadena de bloques, realidad aumentada y realidad virtual. Estas tecnologías complementan y mejoran el IoT, como se explica a continuación.

### *Inteligencia artificial*

No existe una definición aceptada mundialmente de inteligencia artificial (IA). En el Foro de Previsiones Tecnológicas 2016 de la OCDE, los participantes definieron la IA como la capacidad de un programa de computadora para realizar funciones generalmente asociadas con la inteligencia en los seres humanos, como aprender, comprender, razonar e interactuar, en otras palabras, *"hacer lo correcto en el momento adecuado"* (OCDE, 2017[12]).

Indudablemente, la IA tiene implicaciones para muchos aspectos de la vida humana, cuya extensión está más allá del alcance de este informe. Como es pertinente aquí, la IA a menudo se identifica con el segundo elemento básico del IoT: los elementos "inteligentes" que deciden cómo interpretar y actuar sobre los datos transmitidos por un dispositivo o aplicación. Las aplicaciones actuales de IA incluyen máquinas que comprenden el habla humana, compiten en juegos estratégicos, conducen automóviles de forma autónoma o interpretan datos complejos (OCDE, 2017[12]). Las aplicaciones de AI menos obvias incluyen la verificación de pagos con tarjeta de crédito, filtros de correo no deseado, asistentes personales electrónicos, sistemas de navegación GPS, motores de búsqueda, correctores de ortografía y gramática y dispositivos robóticos como robots aspiradores - limpiadores.

La velocidad del progreso realizado en este campo ha aumentado rápidamente. La percepción automatizada, incluida la visión, ya tiene un rendimiento cercano al nivel humano, y los avances en la percepción serán seguidos por mejoras algorítmicas en las capacidades de razonamiento de nivel superior, incluida la planificación o la predicción de peligro (Universidad de Stanford, 2016). Por ejemplo, un vehículo autónomo puede ser capaz de detectar una pelota que rebota en una calle, reconocer que esta puede ser seguida por un niño, planificar para esta situación, en caso de que suceda, y ajustar sus decisiones por consiguiente (The Engineer, 2017).

El desarrollo de la IA tiene un enorme potencial para la gestión de la seguridad de los productos de consumo. Los productos "inteligentes", con capacidades de "aprender", pueden diseñarse para adaptarse al comportamiento del consumidor. Al menos en teoría, esto podría significar que dichos productos podrían llegar a detectar patrones en el comportamiento del consumidor que el diseñador del producto puede no haber anticipado completamente y que pueden crear un riesgo de seguridad. En tales casos, el producto "inteligente" podría adaptar su propio funcionamiento para reducir o minimizar el riesgo, creando así mayores niveles de seguridad.

La IA también puede ser desarrollada e implementada para permitir a las empresas lidiar de manera más efectiva con la supervisión posterior a la comercialización, al: i) ayudar a identificar riesgos potenciales basados en los aportes de una amplia gama de fuentes de datos, incluidos los datos relacionados con el uso provenientes de los propios productos, así como otras fuentes, y ii) en el procesamiento de esos datos para ayudar a identificar soluciones.

### *Tecnología de cadena de bloques (blockchain)*

La cadena de bloques es una tecnología que permite a las partes, que no son de confianza, coordinarse entre sí sin la necesidad de confiar en un tercero de confianza, ya que las partes confían en que la infraestructura tecnológica subyacente funcionará según lo previsto (OCDE, 2017[12]). El ejemplo más conocido de la tecnología de cadenas de bloques es Bitcoin.

La tecnología de cadena de bloques se puede entender como un sistema de contabilidad descentralizado y distribuido que facilita las transacciones económicas y las interacciones

entre pares sin la necesidad de una autoridad confiable o un patrocinador intermediario. La tecnología de cadena de bloques permite a las partes almacenar y administrar datos a través de una red que se ejecuta en la lógica del software en lugar de un operador centralizado. Las redes construidas de esta manera son intrínsecamente solo para adjuntar, lo que las hace resistentes a la manipulación indebida ya que tales datos adjuntos no pueden ser eliminados o modificados posteriormente por ninguna parte. Los datos agregados a la cadena de bloques son autenticados, con marca de tiempo y almacenados cronológicamente por la red. En el contexto del IoT, la tecnología de cadena de bloques tiene el potencial de permitir que los dispositivos se comuniquen directamente entre sí e intercambien valor sin pasar por un intermediario (OCDE, 2017[12]). Por ejemplo, una lavadora conectada al IoT podría detectar que no tiene detergente y utilizar la tecnología de cadena de bloques para solicitar y pagar un nuevo detergente. Además, los beneficios potenciales de la tecnología de cadena de bloques para la seguridad del producto no son difíciles de imaginar —la capacidad de dar seguimiento y rastrear productos a través de la cadena de suministro podría tener efectos contundentes en el área de acciones correctivas y retiros, ayudando a las compañías a localizar y rastrear los productos afectados—.

También se están desarrollando proyectos nuevos y emergentes que utilizan la cadena de bloques para mejorar la seguridad del producto. Estos incluyen Project Manifest de Microsoft, que incluye patrocinadores como Mojix, Amazon, FedEx, Target y Home Depot, y tiene como objetivo dar seguimiento y rastrear una gama de productos (desde auto-partes hasta dispositivos médicos) a través de su cadena de suministro. Un aspecto de este proyecto involucra un concepto que activaría las funciones del "contrato inteligente"[3] cuando ocurren determinadas acciones (por ejemplo, envío de bienes, recepción por parte de minoristas) (del Castillo, 2017[13]). Además, GS1 (una sociedad global de estándares de comunicación comercial sin fines de lucro) ha anunciado recientemente esfuerzos de colaboración con IBM y Microsoft para integrar sus estándares de identificación y datos estructurados en las aplicaciones de cadena de bloques basadas en la cadena de suministro, con la intención de aumentar la integridad de los datos y reducir la duplicación y conciliación de datos (Nation, 2017[14]; GS1, 2017[15]).

Por lo tanto, los beneficios de la tecnología de cadena de bloques podrían ir más allá: ayudar a los consumidores y las empresas por igual al mejorar la transparencia en la cadena de suministro y permitiendo a los participantes ver y compartir información de manera rápida y confiable, y posiblemente aporte nuevos ángulos a los diversos problemas que enfrentan los actores de las cadenas de suministro en todo el mundo, incluyendo por ejemplo el etiquetado de "país de origen" o la credibilidad de las certificaciones.

### *Realidad aumentada y virtual*

Las tecnologías que mejoran, alteran o cambian por completo la percepción de un consumidor sobre sus alrededores —como la realidad aumentada y virtual— tienen el potencial de revolucionar la forma en la que los consumidores experimentan el mundo.

La realidad aumentada se refiere a una clase de tecnologías que recopila información sobre el mundo real, procesa esa información en tiempo real, la combina con información contextual útil y permite a los usuarios experimentar elementos generados por computadora, como imágenes, videos, textos o sonidos superpuestos a entornos reales utilizando dispositivos sensoriales móviles o portátiles. La realidad aumentada difiere de la realidad virtual, ya que es una combinación de elementos generados por computadora y en el mundo real (Tech Policy Lab, 2015[16]; Goldman y Falcone, 2016[17]; Inside Counsel, 2017[18]; Live Science, 2016[19]).

Las aplicaciones de realidad aumentada que ya se utilizan a diario incluyen programas de navegación de tráfico en tiempo real, sistemas de entretenimiento y juegos, programas educativos (como superposiciones de vida silvestre y astronómica) y aplicaciones de calificación que proporcionan revisiones para empresas locales (R Street, 2016[20]). Las futuras aplicaciones de realidad aumentada podrían ayudar a los discapacitados a describir escenas de televisión y películas para ciegos o superponiendo subtítulos para sordos.

La realidad virtual es una clase de tecnologías que permite a los usuarios experimentar e interactuar con un mundo digital totalmente envolvente utilizando dispositivos sensoriales. La realidad virtual difiere de la realidad aumentada en que la realidad virtual bloquea completamente el mundo exterior (Goldman y Falcone, 2016[17]; Live Science, 2016[19]).

Actualmente, la realidad virtual se ve principalmente en sistemas de juego y pronto se puede utilizar en una gama amplia de otras aplicaciones, por ejemplo, en terapias de apoyo para ayudar a los parapléjicos, las víctimas de accidentes cerebrovasculares, así como a las personas con trastorno de estrés postraumático y parálisis cerebral a sobrellevar sus afecciones (R Street, 2016[20]; Reed Smith LLP, 2017[21]). Tanto la realidad aumentada como la virtual también tienen el potencial de enseñar a las personas a conducir, capacitar a las personas para realizar trabajos considerados históricamente riesgosos (como la soldadura) o la cirugía.

Los consumidores actualmente experimentan estas tecnologías en gran medida a través de sus teléfonos móviles, tabletas y dispositivos especializados como consolas de videojuegos, pero las empresas están investigando nuevos dispositivos como auriculares de realidad aumentada, lentes de contacto y otros dispositivos portátiles. Últimamente, algunos observadores de mercado creen que existe la *"sensación de que los teléfonos y las tabletas serán reemplazados"* a medida que las empresas se dirigen hacia el objetivo de una inmersión cómoda y natural (Live Science, 2016[19]).

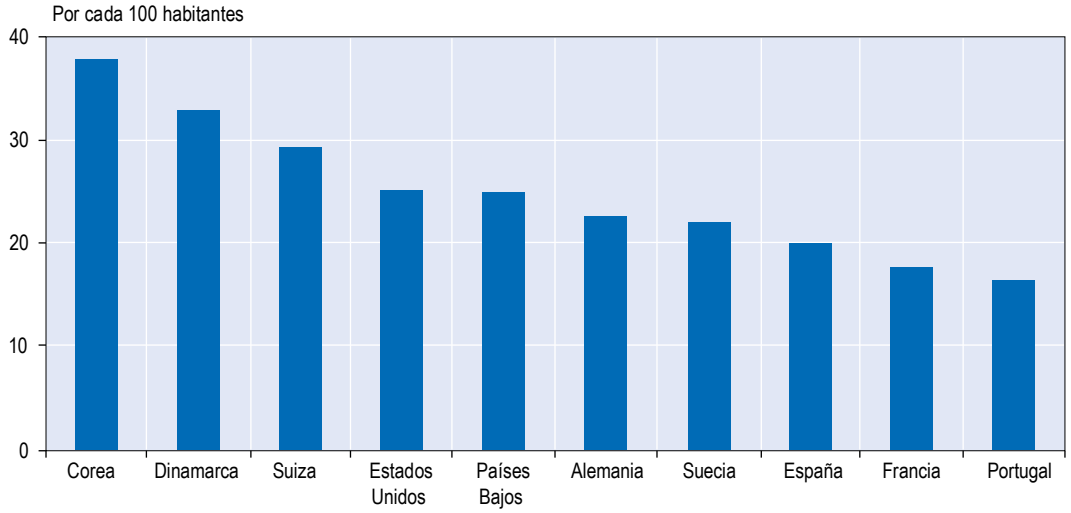
### *2.2.3. Tamaño y crecimiento del mercado*

Con el fin de estar en la mejor posición posible para evaluar cuál es la respuesta política adecuada para el desarrollo del IoT y cualquier problema de seguridad de los productos de consumo que surja, es importante comprender el tamaño del mercado de consumo de dispositivos conectados y evaluar la forma en la que probablemente se desarrolle. Cómo medir el mercado está directamente vinculado a cómo se está definiendo; sin embargo, como se mencionó anteriormente, *"[m]edir el crecimiento del Internet de las Cosas no es una tarea simple porque el IoT no tiene límites claros"* (OCDE, 2016[1]). Como resultado, se han adoptado diferentes métricas para medir y pronosticar el mercado de consumo de dispositivos conectados, como se refleja en los datos a continuación, los cuales son difíciles de comparar entre sí, y probablemente también incluyen dispositivos y aplicaciones conectados que están fuera del alcance del mercado de consumo (como dispositivos y aplicaciones para infraestructura y usos industriales). A pesar de la falta de comparabilidad, los datos disponibles sugieren que el mercado está creciendo a pasos agigantados. Las estimaciones disponibles sugieren que además del crecimiento en la cantidad de dispositivos que se conectarán a Internet en los próximos años, el valor del mercado del IoT debería aumentar rápidamente (OCDE, 2016[1]). Dicho crecimiento debe ser posible por una serie de factores, tales como: la eficiencia del proceso, servicio al cliente, rapidez en la toma de decisiones; ahorro de costos; consistencia en la entrega a través de los mercados; transparencia / previsibilidad de los costos; y el rendimiento en nuevos mercados.

### *Dispositivos y aplicaciones conectados*

Una forma útil de medir el crecimiento del mercado es el aumento de dispositivos y aplicaciones conectados de uso general. Debido a que *"los [e]sfuerzos para desarrollar métricas aún están en su infancia"*, la OCDE ha recopilado datos de los organismos autónomos sobre las suscripciones M2M y considera que esta métrica es*"[u]na de las medidas más precisas, aunque no completa"* (OCDE, 2016[1]). Entre 2012 y finales de 2016, estos datos mostraron que el número de tarjetas SIM M2M reales en uso en los países con seguimiento aumentó de 72 millones a 149 millones (OCDE, 2017[22]).[4] Otra fuente (Shodan, el primer motor de búsqueda del mundo para dispositivos conectados a Internet), proporciona una instantánea de los 10 principales países con la mayor cantidad de dispositivos del IoT conectados a internet por cada 100 habitantes (Figura 1). Shodan encontró que actualmente hay 363 millones de dispositivos conectados en todo el mundo, con 84 millones en la República Popular de China, 78 millones en los Estados Unidos, 18 millones en Corea, Brasil y Alemania y de 8 a 10 millones en Japón, España, Reino Unido y México en cada uno de estos países.

**Figura 1. Dispositivos en línea por cada 100 habitantes, principales países de la OCDE**




*Nota*: Última actualización: 29/mayo/2015.
*Fuente*: (OCDE, 2015[2]), utilizando datos de Shodan.

Otras organizaciones sugieren un crecimiento aún más dramático. La Comisión Europea (CE) predice que el número de conexiones al IoT dentro de los Estados Miembros de la UE aumentará de aproximadamente 1.8 mil millones en 2013 a casi 6 mil millones en 2020 (Cartwright, 2017[23]). Las proyecciones de Cisco muestran que para 2021, la cantidad de dispositivos móviles y conexiones aumentará a 11.6 mil millones, con 8.3 mil millones de dispositivos portátiles o personales listos para dispositivos móviles y 3.3 mil millones de conexiones M2M (Cisco, 2016[24]). Ericsson pronosticó que habría 16 mil millones de objetos conectados a nivel mundial en 2016 y que la cantidad alcanzaría los 29 mil millones para 2022, incluidos automóviles, máquinas, medidores, sensores, terminales de punto de venta, dispositivos electrónicos y portátiles, con este aumento impulsado por *"una gama cada vez mayor de casos de uso y modelos de negocio, y apoyados por la caída de los costos de los dispositivos"* (Ericsson, 2017[25]).

### *Ventas y proyecciones de mercado*

Otra medida útil es la cantidad de dinero que gastan los consumidores en el mercado del IoT. International Data Corporation estima que el valor de mercado del IoT alcanzará los USD 1.29 billones en 2020 (IDC, 2017[26]). McKinsey estima que en 2015 el tamaño del mercado del IoT fue de USD 900 millones, pero que aumentará a USD 3.7 mil millones para 2020 (McKinsey, 2016[27]). Este crecimiento podría generar un impacto potencial de USD 11.1 billones al año en valor económico para el año 2025 si las personas encargadas de dictar políticas y las empresas superan los obstáculos cruciales técnicos, organizativos y regulatorios (McKinsey, 2015[28]). General Electric estima que para 2025 dicha "internet industrial" alcanzará el 43% de la economía global que abarca los motores del crecimiento económico mundial: energía, salud, transporte y fabricación (Marco Annunziata y Economist, 2015[29]).

El mercado de tecnologías complementarias también es una métrica útil para estimar el impacto general del IoT. Analysis Group estima que, si la realidad aumentada y virtual se adopta completamente para 2020, podría impactar la economía global hasta en USD 126 mil millones (R Street, 2016[20]). Otros analistas predicen que el mercado combinado será de USD 162 mil millones para 2020, con la realidad aumentada representando la mayor parte del crecimiento (Inside Counsel, 2017[18]). Bank of America proyecta que solo la industria de la realidad virtual podría valorarse en USD 150 mil millones, con más de 300 millones de usuarios, para 2022 (R Street, 2016[20]).

# 3. Beneficios y riesgos de seguridad de los productos de consumo en el IoT

Esta sección describe los beneficios que el IoT puede brindar de igual manera a los consumidores y negocios. También se identifican los riesgos clave que han surgido de la mano con la propagación del IoT, los cuales probablemente se incrementarán por la complejidad aumentada de las cadenas de suministro mundiales de hoy en día.

## 3.1. Beneficios del IoT

El IoT tiene el potencial de otorgar beneficios importantes a los consumidores. Esto incluye el potencial para administrar de mejor manera la seguridad de productos de consumo y, de este modo, otorgar mejores niveles de protección para el consumidor.

Uno de los beneficios más obvios es que los dispositivos y aplicaciones compatibles con el IoT hacen que las vidas de los consumidores sean más sencillas y menos propensas a algún riesgo, además de promover la eficiencia y la sostenibilidad. Por ejemplo, un termostato conectado con el IoT permite que el consumidor ajuste de manera remota los controles ambientales de su hogar y, de este modo, reduzca el consumo innecesario de energía en los momentos en los que el consumidor no se encuentre allí. Este beneficio no solo ayuda al consumidor a reducir las facturas de energía, sino que también beneficia a la sociedad debido a que se reducen los recursos energéticos que se desperdician. Además, la habilidad de los fabricantes para realizar modificaciones de manera remota a los dispositivos y aplicaciones conectados al IoT significa que estos productos tienen el potencial de actualizarse incluso después de que los consumidores los adquieran. Por esa razón, el mismo termostato conectado podría obtener un rendimiento mejorado o incluso características completamente nuevas a lo largo de su vida en el hogar del consumidor (OCDE, 2016[1]).

Existen también beneficios para los dispositivos y aplicaciones conectadas al IoT que cuentan con el potencial para hacerlos más seguros de usar. Una característica de estar conectado al IoT es que dicho producto puede advertir a las partes responsables sobre condiciones inseguras y permitir que se atiendan estos problemas antes de que ocurra un desenlace negativo. Los sensores de asiento de un automóvil que funcionan a través de Bluetooth podrían, por ejemplo, utilizarse para evitar que los padres dejen solos a sus hijos en el automóvil, mandando una alerta a su teléfono inteligente. Si el problema es grave o no se puede solucionar de manera remota, los fabricantes pueden iniciar recordatorios de una manera oportuna y eficaz. De este modo, considerando el mismo ejemplo anterior, un termostato conectado al IoT podría ser supervisado, de manera remota, por el fabricante o un tercero, por cualquier problema. Por lo tanto, si surgiere un problema, se puede notificar inmediatamente al consumidor sobre el asunto y, si fuere necesario y posible, se podría actualizar o aplicar un parche al software del dispositivo. Y si no se pudiera arreglar el termostato de manera remota, se podría retirar el producto.

Los fabricantes podrían también hacer uso de las tecnologías que forman parte del IoT para rastrear e identificar sus productos a través de la cadena de suministro. En un nivel general, los fabricantes pueden identificar y mitigar los riesgos a sus cadenas de suministro y, de este modo, evitar situaciones que previamente hubieran provocado que su materia prima y suministros futuros o sus productos acabados se pierdan o retrasen. Los fabricantes pueden también rastrear productos o lotes individuales en la cadena de

suministro y, junto con la tecnología de cadena de bloques y los "contratos inteligentes" relacionados, asegurarse que el producto cumpla con los requisitos regulatorios así como recibir los pagos de manera automática cuando el producto se entregue (Iansiti y Lakhani, 2017[30]). Un "contrato inteligente"[5] es un tipo de contrato que inicia una acción (como la transferencia de dinero) cuando se cumplan las condiciones negociadas. Por ejemplo, si un "contrato inteligente" requiere la liberación de un pago al momento de la entrega de un lote de productos conectados con el IoT, el fabricante podría utilizar el IoT para identificar un lote que cumpla con las regulaciones locales del cliente, indicar que se envíe a la ubicación correcta y, de manera automática, recibir el pago cuando el comprador registre en una cadena de bloques, que este se recibió. Con el IoT, los fabricantes pueden asegurar el cumplimiento con las leyes locales y eliminar o reducir los costos, que de otra manera hubieran sido elevados para llevar a cabo sus negocios, como sucede con las estructuras de comercio tradicional junto con los contadores y abogados intermediarios.

## 3.2. Riesgos potenciales en torno a la seguridad para el producto

Junto con los beneficios anteriores de los dispositivos y aplicaciones del IoT, también existen riesgos potenciales relacionados con la seguridad de productos de consumo. Hoy en día, existen informes limitados de consumidores sobre incidentes de seguridad relacionados con los dispositivos y aplicaciones del IoT, posiblemente debido al hecho de que el mercado es nuevo y bastante complejo. Los consumidores quizá aún no han aceptado completamente los dispositivos y aplicaciones del IoT o si ya lo hicieron, puede que la complejidad del mercado les deje con una incertidumbre sobre a quién contactar para solucionar problemas. Sin embargo, en 2017, la Comisión de Seguridad de Productos del Consumidor de los EE. UU. identificó diversas categorías de riesgos potenciales de seguridad de productos, incluyendo: una pérdida de las características de seguridad del producto debido al funcionamiento deficiente o un cambio en el rendimiento debido a actualizaciones del software, una pérdida de conexión a internet y la pérdida de la función correspondiente, la corrupción de datos que se utilicen para que una característica de seguridad sea compatible, así como daños físicos potenciales a dispositivos y aplicaciones portátiles del IoT (Comisión de Seguridad de Productos del Consumidor, CPSC, por sus siglas y nombre en inglés) (EE. UU., 2017[31]). Otras fuentes desarrollaron y ampliaron estas categorías, tal como se menciona a continuación.

### *3.2.1. Mal funcionamiento por defecto o actualización*

Un dispositivo o aplicación con IoT podría presentar un funcionamiento deficiente, ya sea por un defecto que existía cuando el producto se vendió o incluso por una actualización o parche recientemente lanzado por el fabricante. La capacidad de actualizar el software después de que un dispositivo o aplicación con IoT haya dejado la fábrica produce tanto oportunidades como riesgos. Por ejemplo, un dispositivo defectuoso como consecuencia de un software defectuoso podría arreglarse mediante una actualización descargada de internet si el dispositivo estuviere conectado. De la misma manera, un dispositivo no defectuoso cualquiera podría descomponerse por una actualización de software que en sí sea defectuosa. Si una aplicación tiene malfuncionamiento, esta podría provocar que un dispositivo actúe o reaccione de una manera no anticipada y potencialmente insegura. Además, una aplicación que está siendo intervenida ilícitamente por un delincuente podría también afectar la seguridad del dispositivo, si dicha intrusión fuera, por ejemplo, a aumentar o reducir la velocidad del aparato, lo cual provocaría una avería mecánica o sobrecalentamiento (CertifiGroup, 2016[32]).

La complejidad aumenta: las modificaciones del software pueden afectar el funcionamiento del dispositivo o la aplicación de manera directa o pueden generar un funcionamiento defectuoso de manera indirecta, si el dispositivo o la aplicación trabaja necesariamente con otra tecnología y la actualización interrumpe su habilidad para hacerlo. Dicho defecto podría manifestarse involuntariamente desactivando un mecanismo de seguridad u otra tecnología conectada al dispositivo de seguridad o provocando que el dispositivo o la aplicación conectada al IoT funcionen de una manera contraria al funcionamiento seguro de los dispositivos, aplicaciones o tecnologías complementarias.

### *3.2.2. Pérdida de conectividad y obsolescencia del producto*

Se presenta un segundo riesgo en forma de la pérdida de conectividad, lo cual puede impedir que el dispositivo o aplicación con el IoT funcione correctamente. Si el producto depende de la conexión al IoT para que funcione de manera segura, esto podría conllevar implicaciones de seguridad potenciales si el producto no fuese diseñado con un "seguro a prueba de averías" en caso de que pierda la conectividad. El problema será más grave cuando el dispositivo en sí cuente con una función de protección, diseñada para eliminar o reducir un riesgo (p. ej., un sistema de seguridad residencial), y dicha avería en el sistema de protección que controla el funcionamiento adecuado, provoca por sí misma un riesgo de seguridad.

También se han planteado preocupaciones sobre el uso del IoT desde una perspectiva de "obsolescencia planeada" (es decir, empresas que utilizan el IoT para hacer que sus productos de versiones anteriores sean obsoletos o lentos para que los consumidores estén forzados a comprar versiones más nuevas). Esto no es exclusivo de los dispositivos con el IoT, ya que también se ha planteado la misma cuestión con respecto a productos como los microondas y automóviles en el pasado, pero el IoT en teoría aumentaría el control del fabricante sobre su capacidad para "terminar" con la vida de un producto en un momento en particular. No obstante, la capacidad de hacerlo también podría ayudar a los fabricantes a evitar que los usuarios continúen utilizando productos que son inseguros y/o que plantean riesgos al consumidor. Por lo tanto, el desarrollo de los dispositivos conectados, que es a su vez compatible con otras tecnologías, brinda mayores oportunidades para que los fabricantes gestionen la seguridad al final de la vida del producto, y así asegurar de mejor manera la seguridad durante todo el ciclo de vida del producto.

### *3.2.3. Cuestiones de la calidad e integridad de los datos*

Otro peligro es la calidad e integridad de los datos que se utilizan para que una función de seguridad sea compatible. En la medida en que la característica de seguridad dependa de ciertos datos, es imperativo que los datos sean precisos y no se corrompan ya que, de otra manera, la característica de seguridad podría no funcionar.

La calidad de los datos, es en particular un problema emergente con el IoT, en específico cuando los datos que se utilizan en las decisiones automatizadas provienen de terceros sin una reputación confiable, o los datos carecen de atributos o información existente (McAfee, 2013[33]). Por ejemplo, los códigos de barras son útiles como números legibles por máquina que identifican a un fabricante o producto, pero las formas en las que muchas aplicaciones de terceros acceden a los metadatos a veces no son claras y, por lo tanto, la información proporcionada por un código de barras podría ser incorrecta. De la misma manera en la que se corrompen los datos, si los metadatos son incorrectos o erróneos, podrían provocar que los dispositivos y aplicaciones con IoT se comporten de manera inesperada o insegura. Tal como se mencionó previamente, los beneficios de la tecnología de cadena de bloques

podrían funcionar muy bien en esta área y ayudarían a tratar con algunas de las cuestiones: los datos y la información que se almacenan en un cadena de bloques es mucho menos, si no es que nada, susceptible a los piratas informáticos y a la corrupción debido a su naturaleza descentralizada.

De igual forma, pueden existir peligros cuando un dispositivo conectado con el IoT funciona junto a una aplicación de realidad aumentada. En un posible ejemplo, la combinación podría identificar erróneamente un objeto en el mundo real y, por lo tanto, provocar que un humano actúe de manera insegura. Este podría ser el caso, por ejemplo, en un suceso en el que la tecnología provoque que un mecánico reemplace incorrectamente una pieza de un automóvil descompuesto por una pieza incorrecta y el error provoque un daño al conductor o transeúnte (Tech Policy Lab, 2015[16]; R Street, 2016[20]).

La seguridad digital, por lo tanto, es una cuestión importante en materia de política de seguridad del producto conforme el IoT continúa desarrollándose. Esto va más allá de las cuestiones de la privacidad del consumidor, ya que el mantenimiento de la integridad de los datos puede ser una cuestión crítica para asegurar el funcionamiento seguro y adecuado de los productos.

Tanto la Comisión Federal de Comercio de los Estados Unidos (US FTC, por sus siglas en inglés) como el Parlamento Europeo, han expresado sus preocupaciones en relación con las implicaciones potenciales de la seguridad digital desde una perspectiva de la seguridad del producto. Por ejemplo, la US FTC (2015[34]) publicó un informe que mencionaba que (entre otros riesgos) *"las personas no autorizadas podrían aprovecharse de las vulnerabilidades de seguridad para generar riesgos para la seguridad física en algunos casos"*. La US FTC propuso distintas recomendaciones, incluyendo que las empresas deben incorporar medidas de seguridad digital en sus dispositivos desde el comienzo, asegurar que sus prácticas relativas al personal promuevan la buena seguridad digital, buscar y proporcionar vigilancia a proveedores de servicio capaces, implementar múltiples capas de medidas de seguridad, restringir el acceso a los dispositivos por usuarios no autorizados, y supervisar productos durante su ciclo de vida para corregir vulnerabilidades conocidas (Comisión Federal de Comercio de EE. UU., 2015[34]).

### *3.2.4. Peligros físicos*

Los dispositivos y las aplicaciones con IoT invasivos, no invasivos o cercanos al cuerpo, como por ejemplo los dispositivos portátiles, tienen el potencial de lesionar físicamente a los consumidores. La CPSC de los EE. UU. (2017[31]) identificó una variedad de peligros potenciales en esta categoría, incluyendo: pérdida de audición de un dispositivo auditivo implantado que tiene malfuncionamiento o reproduce señales de otra fuente, quemaduras químicas o térmicas e irritación cutánea debido a baterías con fugas o defectuosas u otros materiales reactivos del dispositivo o la aplicación; e incluso distensiones musculares debido a que exoesqueletos mecánicos se mueven fuera del rango natural de movimiento de una persona. Los dispositivos de realidad aumentada y virtual podrían además provocar vista cansada, traumatismo ocular, problemas en el desarrollo ocular o mareo (R Street, 2016[20]). En casos más extremos, estos dispositivos podrían incluso provocar ataques epilépticos (Reed Smith LLP, 2017[21]).

Además, los dispositivos conectados con el IoT podrían distraer a los consumidores— o los usuarios podrían confiar en información que dicho dispositivo proporcionó por error— y provocar que se lesionen o que lesionen a terceros como consecuencia (Tech Policy Lab, 2015[16]). Por ejemplo, un automóvil equipado con una pantalla frontal que funciona con una aplicación de realidad aumentada podría reemplazar una señal de alto por un anuncio

virtual y, de este modo, provocar un accidente. O un usuario podría lesionarse solo por tropezar con un objeto del mundo real, mientras se encuentra en una realidad aumentada o virtual, y caer (R Street, 2016[20]). Los consumidores podrían también dañar la propiedad al utilizar dispositivos conectados con el IoT, como al manipular sensores equipados con realidad aumentada o virtual, sin el espacio físico suficiente, en el mundo real para realizar el movimiento deseado (Reed Smith LLP, 2017[21]).

El Parlamento Europeo expresó su preocupación en torno a las implicaciones potenciales de la seguridad física del aumento de la robótica, como parte de sus recomendaciones para la Comisión sobre Normas de Derecho Civil sobre Robótica (2015/2102(INL)). Por ejemplo, los humanos pueden exponerse a peligros físicos *"cuando el código de un robot resulte inexacto"* o las *"consecuencias potenciales de la avería del sistema o la intrusión en robots o sistemas robóticos conectados en el momento en el que las aplicaciones cada vez más autónomas se estén utilizando"* (p. ej., peligros relacionados con vehículos robóticos, robots de cuidado o robots que se utilizan para mantener el orden público).

# 4. Desafíos políticos: Reformulando las leyes de seguridad y responsabilidad civil derivada de productos defectuosos

El simple hecho de que una nueva tecnología de producto pueda presentar riesgos a los consumidores no crea, por sí mismo, una necesidad de una respuesta normativa. En un número creciente de países alrededor del mundo, los consumidores están, en general, bien protegidos por las estrictas leyes, regulaciones y normas en materia de seguridad del producto que cubren una gama amplia de riesgos. En la mayoría de los países, dichas reglas y regulaciones de seguridad son respaldadas por los sistemas jurídicos mediante los cuales los consumidores que resulten lesionados por productos inseguros pueden obtener una indemnización por parte del fabricante o vendedor responsable de poner dicho producto en el mercado. Puede ser que dichos regímenes existentes en materia de seguridad y responsabilidad civil derivada de productos defectuosos estén bien adaptados para manejar los desafíos que las nuevas tecnologías plantean, incluyendo los relacionados con el IoT. En su informe del 2015, la Alianza para la Innovación del Internet de las Cosas (AIOTI, por sus siglas en inglés) concluyó que, aunque existían ciertas consideraciones especiales en las áreas de cumplimiento del producto, responsabilidad civil derivada de productos defectuosos y cuestiones relacionadas con el seguro para ciertos productos con el IoT, no existía una necesidad clara para crear una nueva legislación o reglamento (AIOTI, 2015[4]). Debido a que muchos de los riesgos de responsabilidad civil derivada de productos defectuosos que se recalcan no son exclusivos de los productos y plataformas con el IoT, se consideró que se debe llevar a cabo una reflexión y dialogo cuidadoso antes de realizar cualquier modificación al régimen existente, y que el objetivo de lograr la seguridad del consumidor deberá estar balanceado con la necesidad de estimular la innovación en el mercado del IoT (AIOTI, 2015[4]). Esto no es un concepto nuevo, ya que ha sido durante mucho tiempo el desafío de los regímenes en materia de regulación del producto para asegurar que estos son suficientemente adaptables para soportar el desarrollo tecnológico adecuado. El desafío principal reciente en la era del IoT es, por sí mismo, el ritmo del desarrollo tecnológico, el cual presiona a cualquier régimen regulatorio a que se adapte con la velocidad y visión suficiente para mantener la protección de los consumidores mientras se permite que se obtengan los beneficios de la tecnología.

Esta sección resume los tres desafíos principales de la política que surgen por la adopción del IoT, así como las implicaciones potenciales que estos desafíos tienen sobre la seguridad del producto y las leyes de responsabilidad, además de las regulaciones, a nivel mundial (las cuales se consideran por separado a continuación). Los tres desafíos de la política son:

- El impacto del IoT respecto a la distinción entre “hardware” y “software”, y “productos” y “servicios”.
- La cuestión sobre quién es responsable de la seguridad de los productos, cuál es el alcance de la responsabilidad y cómo se establece la responsabilidad en caso de avería; y
- La comunicación de la seguridad para los consumidores.

Se incluyen ejemplos de cómo los gobiernos y las partes interesadas alrededor del mundo manejan estos desafíos, tal como se revela por las iniciativas, la litigación reciente y la ejecución de las acciones de diversas jurisdicciones. Para comenzar, la CPSC de los EE. UU. ofrece una buena idea de la complejidad de la tarea con la que se enfrentan los gobiernos e

inspectores, al indicar que cada dispositivo o aplicación conectada al IoT se debe considerar como "única", y que posiblemente no será un planteamiento global para regular el IoT (Colegio de Abogados de los EE. UU., 2017[35]). La colaboración con los consumidores y la industria será clave para este planteamiento. También será importante que exista un nivel superior de coordinación entre los legisladores en todo el mundo. Intrínsecamente, el IoT transciende fronteras geográficas y políticas. También, los mercados para dichas tecnologías son cada vez más globales. Para aprovechar por completo el potencial de la tecnología del IoT, se necesita una coordinación internacional para evitar ineficiencias, así como para asegurar una experiencia consistente para los consumidores, incluyendo la protección de su seguridad. De hecho, algunos comentaristas han solicitado la creación de una nueva organización internacional que regule el IoT; que trabaje a través de las fronteras y que consista, en contraste con la regulación del internet, de un *"marco institucional en materia de política multipolar descentralizada, el cual consideraría las necesidad de todas las partes interesadas relacionadas y que sea administrado por varias entidades"* (Weber, 2009[36]).

## 4.1. La interacción entre "hardware", "software", "productos" y "servicios"

Los componentes típicos de los dispositivos con el IoT incluyen hardware, software y protocolos/normas de comunicación. En general, "hardware" en este contexto podría considerarse como un dispositivo o conjunto de dispositivos u objetos físicos que son sensibles en su naturaleza y que cuentan con la capacidad de recuperar datos y seguir instrucciones. "Software" es el conjunto de programas que permiten la recolección, almacenamiento, procesamiento, manipulación de datos, así como las órdenes provenientes de los componentes del hardware, y para los mismos. El IoT ha generado oportunidades adicionales en el espacio del hardware y software, a través del cual los usuarios pueden acceder a datos "inteligentes" y controlar el sistema de manera remota, y, por el cual, los dispositivos pueden "aprender" de manera autónoma a través de datos que no necesariamente son controlados por el diseñador o usuario del producto.

Típicamente, los regímenes en materia de regulación de seguridad y responsabilidad civil derivada de productos defectuosos establecen una distinción entre el suministro de "bienes" y la prestación de "servicios", y cada escenario se regula de manera distinta. En el sector tecnológico, la distinción ha dado pie a un debate y controversia legal alrededor de la distinción entre "hardware" y "software" —en particular en relación a si debe considerarse un software como un "bien"— y como consecuencia, estar sujeto a los regímenes de seguridad y responsabilidad civil derivada de productos defectuosos (AIOTI, 2015[4]). El IoT no plantea nuevas cuestiones de manera obvia sobre este tema. Sin embargo, el IoT conlleva un mayor nivel de complejidad en la interacción entre el hardware y el software que lo impulsa, con el comportamiento de los productos en muchos sectores siendo cada vez más dependiente del software y datos modificables que se almacenan tanto en el producto como de manera externa.

Estos factores no cambian necesariamente el análisis fundamental de la distinción, sino que potencializan la necesidad de una distinción clara y la hacen más aguda, que a su vez, se convierte en un desafío para los legisladores y responsables de hacer cumplir las políticas. Debido a que un dispositivo o aplicación con IoT puede ser una combinación de bienes y servicios, el alcance en el que se aplican las leyes en materia de seguridad del producto y responsabilidad civil derivada de productos defectuosos, puede ser un tema complicado en determinar para los tribunales o agencias enfocadas en la seguridad del producto. Por ejemplo, los regímenes existentes de responsabilidad del producto pueden omitir la acción

de *"proporcionar datos mediante un sistema con el IoT"* ya que se considera como un servicio (Medium, 2017[37]). En algunos territorios (como Austria, Alemania y Suiza), los tribunales han manejado los productos de contenido digital en general de la misma manera que los bienes; sin embargo, otros, como el Reino Unido, hacen una distinción entre el software suministrado como un medio tangible (como un CD) y el software suministrado a través de un medio intangible (como el software descargado del internet). El primer ejemplo se considera como una venta de bienes, mientras que el segundo no (OCDE, 2013[38]). Esto tiene implicaciones importantes para los derechos y recursos del consumidor, ya que a una venta de bienes se le otorga generalmente una protección jurídica mayor que a la prestación de servicios. Si un consumidor resulta dañado por un bien defectuoso, este comúnmente tendrá el derecho de que se le reemplace el producto, recibir un reembolso o reclamar daños y perjuicios por dicha pérdida. No obstante, las mismas reglas pueden no ser aplicables si el "objeto" que dañó al consumidor se considera como un "servicio", en cuyo caso el consumidor podría necesitar basarse en principios menos protectores para reclamar daños y perjuicios.

En cuanto al contexto de la responsabilidad civil derivada de productos defectuosos, estas cuestiones son importantes en especial ya que varias competencias, como la Unión Europea y los Estados Unidos, han establecido regímenes de "sin avería" o de responsabilidad objetiva para manejar reclamaciones en materia de responsabilidad civil derivada de productos defectuosos (AIOTI, 2015[4]).

Además, la intersección del hardware y software en los dispositivos y aplicaciones conectadas con el IoT presenta oportunidades únicas al igual que desafíos, desde la perspectiva de la protección de la seguridad del consumidor. Tradicionalmente, un desarrollador de hardware se enfocaría en lanzar una versión final y perfecta de un producto para intentar evitar distintas consecuencias negativas potenciales que pueden surgir en caso de un defecto. Los desarrolladores de software han tenido la capacidad de llevar un producto nuevo al mercado conscientes de que si se descubre cualquier defecto, es probable que sea fácil solucionarlo mediante un parche de software, con poca o ninguna interrupción para el consumidor (y en algunos casos sin que este lo sepa), en circunstancias en las que tanto los consumidores como su software, son fácilmente rastreables. En caso de que un producto resulte defectuoso, los fabricantes podrían utilizar una cadena de bloques, por ejemplo, para rastrear e identificar mejor el defecto y permitir una medida correctiva más eficaz.

El desarrollo de productos con el IoT indica la llegada al mercado de una amplia gama de productos que se ubican en medio de estas dos posiciones tradicionales. El hecho de que el rendimiento y la funcionalidad de dichos productos sea cada vez más controlada por software, significa que los defectos inesperados debido al software son cada vez más posibles (o al menos solucionados por software), y dichos defectos pueden solucionarse de manera remota con poca interrupción para los consumidores. Estas nuevas complejidades plantean cuestiones de política interesantes y potencialmente importantes cuando se considera cómo se debe manejar la responsabilidad para asegurar la seguridad del producto, y cómo se debe determinar la responsabilidad en caso de que un producto provoque lesiones.

## 4.2. Responsabilidad

Tal como se enfatiza en la Recomendación acerca de la Protección al Consumidor en el Comercio Electrónico modificada de la OCDE de 2016 ("la Recomendación de la OCDE en materia de Comercio Electrónico"), que indica que *"la adecuada distribución de la responsabilidad para la protección de los consumidores entre los actores pertinentes del comercio electrónico es clave para promover el bienestar del consumidor y mejorar su*

*confianza"* (OCDE, 2016[39]). Los principios tradicionales de la seguridad y responsabilidad del producto podrían, sin embargo, no estar delimitados claramente en el nuevo mundo de los dispositivos y aplicaciones conectadas con el IoT. Tal como se mencionó anteriormente, estos productos podrían resultar defectuosos e inseguros de muchas maneras, como a través de una vulneración de datos o debido a que un dispositivo o aplicación externa funcionó defectuosamente. Además, los dispositivos podrían depender de la conectividad sin interrupciones, sin que dicha seguridad del dispositivo se comprometa (o se mantenga, si el dispositivo es defectuoso y espera una actualización de software para solucionar el defecto). Impulsados por la IA, estos dispositivos y aplicaciones pueden, además, adoptar, anticipar y predecir decisiones sin la interacción humana. Por lo tanto, es posible que las regulaciones y normas en materia de seguridad del producto para el consumidor, así como las reglas de responsabilidad, no traten eficazmente las cuestiones que resulten en torno a la seguridad del producto.

### *4.2.1. ¿Quién es responsable de la seguridad de los productos?*

Por ejemplo, si un software externo que se integra en un producto no es defectuoso cuando se comercializó por primera vez pero, como resultado de una actualización por parte del tercero, el producto desarrolla un riesgo inesperado para la seguridad del producto, quizá no sea tan claro siempre de quién es la responsabilidad. Los asuntos pueden incluso ser más complicados cuando el rendimiento de un producto está influenciado o controlado por los datos que se producen mediante la IA. Debido a que la IA depende de grandes cantidades de datos de una amplia gama de fuentes, podría ser difícil o casi imposible para cualquiera de las partes el entender por qué un producto actuó de la manera en la que lo hizo.

A un nivel de cumplimiento de seguridad del producto, dado el alto nivel de integración entre los dispositivos y aplicaciones, así como la complejidad del ecosistema del IoT, podría ser difícil determinar inicialmente quién deberá certificar la seguridad y cumplimiento del producto, la medida en la que se requiere la certificación y por cuánto tiempo dicha parte es responsable de la seguridad del producto. De hecho, la CE marcó estas cuestiones como asuntos particularmente problemáticos en su informe sobre "el Avance del Internet de las Cosas en Europa" (Comisión Europea, 2016[40]). Estas cuestiones no son nuevas, ni son exclusivas del IoT, pero de nuevo, la complejidad de la tecnología del IoT y la gran medida en la que dichos productos son controlados por software y datos hacen que estas cuestiones sean más consideradas desde una perspectiva normativa.

Un factor que complica las cosas, por lo tanto, es que los dispositivos y aplicaciones con el IoT son generalmente, debido a la naturaleza de su diseño, dependientes de tecnología de terceros para llevar a cabo sus funciones básicas y maximizar el beneficio para el consumidor (AIOTI, 2015[4]), y el desempeño y seguridad de un producto podrían alterarse por la participación de terceros luego de que se haya colocado el producto en el mercado (potencialmente en circunstancias más allá del conocimiento o control del fabricante). Esto ha llamado la atención de los reguladores en los Estados Unidos. Por ejemplo, la CPSC de los EE. UU. (2017[31]) declaró que se enfocará en *"no solamente los productos [que funcionan] seguros, sino en [aquellos] productos que tampoco afectan de manera adversa la operación de otros dispositivos "*. Además, estas interdependencias pueden incrementarse y volverse incluso más complejas durante la vida del dispositivo o la aplicación.

Por lo demás, surgen también cuestiones en cuanto a la medida en la que un proveedor de hardware o software debería ser responsable de asegurar que el producto esté protegido de manera continua ante un ataque digital contra su seguridad. Esto puede volverse particularmente desafiante en un mundo en donde los *ciberdelincuentes*, de manera

constante, están ideando nuevas maneras de acceder a datos de manera ilícita para cometer sus delitos, lo cual obliga a los creadores de productos a desarrollar continuamente parches y protecciones para asegurar la protección continua de los productos en el mercado.

### *4.2.2. ¿Cómo se puede asignar la responsabilidad?*

Sobreponiéndose a las consideraciones en torno a la seguridad del producto, se encuentra la cuestión de cómo determinar la responsabilidad para pagar la indemnización en caso de que un defecto o avería en un producto provoque daños. Esta superposición es importante, debido a que se crearán ineficiencias si la política en materia de seguridad del producto se desarrolla de tal manera que existan diferencias entre el régimen de la seguridad del producto y el de la responsabilidad civil derivada de productos defectuosos (i) con respecto a la identificación de las partes responsables de la seguridad y el cumplimiento, y el alcance de dichas responsabilidades; y (ii) con respecto a la cuestión de cuál es un nivel aceptable de seguridad.

La interdependencia de los productores, actores y consumidores de bienes y servicios en el ecosistema del IoT significa que la responsabilidad podría ser difícil de determinar, ya que existen desafíos para *"la identificación de la causa principal de las averías del producto"* (Comisión Europea, 2016[40]). Por ejemplo, en el caso de un accidente de tránsito que involucre un vehículo autónomo, varios actores del IoT podrán ser responsables por completo, o parcialmente, por el accidente; estos podrían incluir a la aplicación que determina el movimiento del automóvil, el fabricante de los sensores, el operador de la red sensorial, el operador de tránsito y el tercero que proporcionó el software (Medium, 2017[37]).

Para justificar su reclamación, un consumidor debe, generalmente, mostrar ambos el defecto, el daño; y comprobar que el defecto provocó el daño. Distintas competencias han establecido diferentes pruebas para estos elementos. Por ejemplo, para justificar un defecto, tanto la Unión Europea como los Estados Unidos aplican variaciones de una prueba de "expectativa razonable", donde un tribunal compara el producto puesto en entredicho a cómo un consumidor habría esperado que dicho producto se comportara.

Pero incluso con dicha prueba general, la aplicación específica puede variar ampliamente, aun dentro de una jurisdicción, como entre los Estados Miembros de la UE o los estados de los EE. UU. Los regímenes de responsabilidad civil derivada de productos defectuosos podrían también proporcionar protecciones para el fabricante (como la justificación de que su producto se encontraba acorde a los "avances tecnológicos" disponibles en el momento en el que se comercializó), así como restringir la responsabilidad solo para ciertas categorías de daños, como la muerte, daño físico o daño a otra propiedad. Todo lo considerado en los puntos anteriores genera desafíos para la determinación precisa y eficiente de la responsabilidad en caso de un producto defectuoso.

Estas cuestiones se encuentran bajo una consideración activa en algunos territorios y regiones. Por ejemplo, la CE actualmente está llevando a cabo una revisión de la Directiva de Responsabilidad Civil Derivada de Productos Defectuosos de la CE, enfocándose expresamente en si sus disposiciones, que no se han modificado considerablemente desde 1985, continúan siendo aptas para efectos de considerar los desafíos de las nuevas tecnologías (Comisión Europea, 2016[41]). Con base en los resultados que la CE recibió a través de una consulta pública sobre el tema, aproximadamente la mitad de los participantes consideraron que la Directiva necesitaba adaptarse a los productos innovadores (Comisión Europea, 2017[42]).

El Parlamento Europeo también está involucrado en el manejo del problema de la determinación de responsabilidad en el IoT. En febrero del 2017, sus Miembros votaron

para solicitar a la CE que, de manera urgente, propusiera reglas sobre la robótica y la IA para clarificar las cuestiones de responsabilidad.

Algunos han sugerido que parte de estas cuestiones de responsabilidad para los fabricantes y otras partes involucradas en la cadena de producción podrían, quizá, tratarse con una solución basada en un seguro en el cual las partes involucradas "combinarían" el riesgo, y de manera conjunta asegurarían a los dispositivos y aplicaciones conectadas al IoT. En su informe SONAR anual, Swiss Re (2017[43]) consideró la posibilidad de una nueva personalidad jurídica para las "personas electrónicas". Esto podría parecer disparatado, pero podría proporcionar un "simple punto focal" a seguir en caso de una controversia relacionada con la responsabilidad civil derivada de productos defectuosos, en particular si se combina con un régimen de responsabilidad objetiva y aseguramiento obligatorio, en vez de pensar en la compleja cuestión de determinar la responsabilidad en el caso de un accidente de tránsito en donde un vehículo autónomo está involucrado —en el que la responsabilidad podría ser del conductor, fabricante automotriz, software y/o el proveedor de datos— (Kidman y Turner, 2017[44]). Sin embargo, esta discusión resalta el hecho de que las cuestiones de determinación de responsabilidad para el cumplimiento y de la responsabilidad en caso de lesiones, son temas complejos que plantean consideraciones particulares en cuanto a las políticas en un contexto del IoT.

Debido a estos desafíos, surge una cuestión fundamental en torno a si los regímenes existentes de seguridad y responsabilidad del producto alrededor del mundo son aptos para la era del IoT. Por una parte, puede que se haya dicho que el IoT no necesariamente plantea cuestiones que son completamente nuevas. Es bastante frecuente que los productos que se venden puedan adaptarse o modificarse por terceros, o incluso por los mismos consumidores. Por otra parte, se podría decir que, por los motivos descritos anteriormente, los regímenes existentes de regulación y responsabilidad podrían necesitar adaptarse para manejar adecuadamente estos nuevos conceptos y desafíos. Estas son cuestiones importantes para los legisladores. El incumplimiento de los legisladores para identificar e introducir cualesquier adaptaciones necesarias podría conducir a una rápida comercialización de las categorías de productos sin una supervisión adecuada de la seguridad y el rendimiento, y dichos consumidores se enfrentarían a un riesgo mayor. Al considerar estos dos enfoques, será necesario establecer un equilibrio entre el aseguramiento de: i) un alto nivel de seguridad del producto para el consumidor en el IoT, y ii) que la innovación no sea innecesariamente sofocada, lo que dará como resultado la privación a los consumidores de nuevas tecnologías que podrían mejorar la seguridad del producto.

## 4.3. Comunicando la seguridad a los consumidores

A través del IoT, los fabricantes y proveedores de productos cuentan con capacidades sin precedentes para conectarse con la base de consumidores de manera más rápida y eficaz, en especial en el caso de una retirada del producto. Típicamente, la interacción de los consumidores con los dispositivos con IoT se realiza a través de una aplicación (app) o un servicio remoto en el dispositivo basado en software, el cual le brinda a la empresa encargada de controlar el software la habilidad única para conectarse con el usuario activo del producto, sin importar que el usuario sea el comprador original del producto o no.

A través de estos medios, se espera que se produzcan oportunidades únicas para que los proveedores de productos comuniquen información importante de seguridad a los consumidores, tanto al momento en el que se activa por primera vez el producto como durante el ciclo de vida completo del producto. Esto podría incluir la comunicación de instrucciones para la instalación y configuración segura, recordatorios continuos sobre el uso seguro del producto cuando esté en uso, actualizaciones sobre las instrucciones de

seguridad al momento en el que lleguen nuevos datos a los fabricantes, información sobre retiradas del producto o modificaciones de seguridad, así como información oportuna sobre los requisitos de mantenimiento y cuestiones de la vida final del producto.

El desafío para los legisladores radica, primero, en asegurar que las regulaciones y las prácticas de aplicación sean suficientemente flexibles para incentivar el uso de dicha tecnología, de esta manera, para mejorar la seguridad. Como un ejemplo, la modificación más reciente de la "Guía Azul" de la Comisión Europea sobre la interpretación de las regulaciones de la UE en materia de seguridad del producto incluyó por primera vez una referencia que sugiere que siempre se deben entregar advertencias de seguridad a los consumidores, las cuales deberán ir por escrito en un papel que acompañe al producto (Comisión Europea, 2016[45]). En la era del IoT, esta guía ya parece anticuada, al menos para los productos que cuentan con formas mucho más efectivas de proporcionar advertencia críticas de seguridad e instrucciones a los consumidores.

De manera más general, tal como se comentó anteriormente, estas capacidades plantean cuestiones sobre el alcance de las responsabilidades de los operadores económicos responsables del desarrollo y comercialización de productos con el IoT, en relación con las maneras en las que la información de seguridad se comunica, el plazo de dicha información y las obligaciones en caso de que surjan cuestiones inesperadas de seguridad.

# *Referencias*


Alianza para la Innovación del Internet de las Cosas (AIOTI) (2015), *Working group 4 Report on Policy Issues*, https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf. [4]

American Bar Association (2017), *Consumer Product Safety Administration seeks collaboration in managing internet of things*, https://www.americanbar.org/news/abanews/aba-news-archives/2017/05/consumer_productsaf.html (consultada el 13 de octubre de 2017). [35]

Annunziata, Marco; (2015), *The Moment For Industry*, http://gereports.cdnist.com/wp-content/uploads/2015/09/29153350/Annunziata_Moment-for-industry_Final1.pdf (consultada el 12 de octubre de 2017). [50]

Barboutov, K. et al. (2017), *Ericsson Mobility Report*, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (consultada el 12 de octubre de 2017). [49]

Business Insider (2016), *Wearable technology and IoT wearable devices*, Business Insider, http://www.businessinsider.fr/uk/wearable-technology-iot-devices-2016-8/ (consultada el 12 de octubre de 2017). [56]

Cartwright, J. (2017), *Product liability and the internet of things | Charles Russell Speechlys*, https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/ (consultada el 12 de octubre de 2017). [23]

CertifiGroup (2016), www.CertifiGroup.com *Experts in UL, CSA, CE & International Regulatory Compliance*, http://certifigroup.com/whitepapers/product-safety-and-iot.pdf (consultada el 12 de octubre de 2017). [32]

Charles Russell Speechlys (2017), *Product liability and the internet of things* |, https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/commercial/2017/product-liability-and-the-internet-of-things/ (consultada el 12 de octubre de 2017). [68]

Cisco (2016), *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (consultada el 12 de octubre de 2017). [24]

Cisco (2017), "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update The Cisco ® Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update", https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (consultada el 12 de octubre de 2017). [69]

CNET (2016), *Virtual reality doesn't mean what you think it means - CNET*, https://www.cnet.com/uk/news/virtual-reality-terminology-vr-vs-ar-vs-360-video/ (consultada el 12 de octubre de 2017). [66]

Coindesk (2017), *Microsoft's Blockchain Supply Chain Project Grows to 13 Partners - CoinDesk*, https://www.coindesk.com/microsofts-blockchain-supply-chain-project-grows-to-13-partners/ (consultada el 12 de octubre de 2017). [63]

Comisión de Seguridad de Productos del Consumidor (CPSC) (EE. UU.) (2017), *Potential Hazards Associated with Emerging and Future Technologies*, https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf (consultada el 13 de octubre de 2017). [31]

Comisión de Seguridad de Productos del Consumidor de los Estados Unidos de América (2017), *Staff Report - Potential Hazards Associated with Emerging and Future Technologies*, https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf (consultada el 12 de octubre de 2017). [47]

del Castillo, M. (2017), *Microsoft's Blockchain Supply Chain Project Grows to 13 Partners*, CoinDesk, https://www.coindesk.com/microsofts-blockchain-supply-chain-project-grows-to-13-partners/ (consultada el 12 de octubre de 2017). [13]

DiClerico, D. (2014), *Nest Protect Recall | Smoke and CO Alarm Reviews - Consumer Reports News*, https://www.consumerreports.org/cro/news/2014/05/nest-labs-recalls-nest-protect-smoke-co-alarm/index.htm (consultada el 12 de octubre de 2017). [48]

Ericsson (2017), *Ericsson Mobility Report*, https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (consultada el 12 de octubre de 2017). [25]

Comisión Europea (2016), *Advancing the Internet of Things in Europe*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN. (consultada el 12 de octubre de 2017). [40]

Comisión Europea (2016), "Evaluation and Fitness Check (FC) Roadmap Evaluation of the Directive 85/374/EEC Concerning Liability for Defective Products", http://ec.europa.eu/smart-regulation/evaluation/index_en.htm (consultada el 12 de octubre de 2017). [41]

Comisión Europea (2016), *The 'Blue Guide' on the implementation of EU product rules 2016*, Comisión Europea, http://ec.europa.eu/DocsRoom/documents/18027 (consultada el 12 de octubre de 2017). [45]

Comisión Europea (2017), *Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product*. [42]

Comisión Federal de Comercio de los EE. UU. (2015), *Internet of Things Privacy and Security in a Connected World FTC Staa Report*, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (consultada el 12 de octubre de 2017). [34]

Goldman Sachs (2014), *Goldman Sachs | Our Thinking - The IoT as the Third Wave of the Internet*, http://www.goldmansachs.com/our-thinking/pages/iot-video.html. [57]

Goldman, J. y J. Falcone (2016), *Virtual reality doesn't mean what you think it means - CNET*, https://www.cnet.com/uk/news/virtual-reality-terminology-vr-vs-ar-vs-360-video/ (consultada el 12 de octubre de 2017). [17]

GS1 - The Global Language of Business (n.d.), *Blockchain: GS1, IBM and Microsoft collaborate to leverage standards | GS1*, https://www.gs1.org/articles/2256/blockchain-gs1-ibm-and-microsoft-collaborate-leverage-standards. [54]

GS1 (2017), *Blockchain: GS1, IBM and Microsoft collaborate to leverage standards*, https://www.gs1.org/articles/2256/blockchain-gs1-ibm-and-microsoft-collaborate-leverage-standards. [15]

Iansiti, M. y K. Lakhani (2017), *The Truth About Blockchain*, https://hbr.org/2017/01/the-truth-about-blockchain. [51]

Iansiti, M. y K. Lakhani (2017), *The Truth About Blockchain*, Harvard Business Review, https://hbr.org/2017/01/the-truth-about-blockchain (consultada el 13 de octubre de 2017). [30]

IDC (2017), *Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide*, https://www.idc.com/getdoc.jsp?containerId=prUS42209117 (consultada el 13 de octubre de 2017). [26]

IHS Markit (2015), "Global Shipment and Revenue Market Forecast for Wearable Technology The Small Revolution is Making Big Waves", http://dx.doi.org/10.0. [58]

Information Age (2015), *Who is liable when the Internet of Things goes wrong?*, http://www.information-age.com/who-liable-when-internet-things-goes-wrong-123460320/ (consultada el 13 de octubre de 2017). [7]

Information age (2017), *Who is liable when the Internet of Things goes wrong?*, http://www.information-age.com/who-liable-when-internet-things-goes-wrong-123460320/ (consultada el 13 de octubre de 2017). [55]

Inside Counsel (2017), *Augmented Reality and IoT: Enjoying the Ride, While Avoiding Legal Snafus*, http://www.insidecounsel.com/2017/03/29/augmented-reality-and-iot-enjoying-the-ride-while?slreturn=1507888346 (consultada el 13 de octubre de 2017). [18]

Jankowski, S. (2014), *Our Thinking - The IoT as the Third Wave of the Internet*, Goldman Sachs, http://www.goldmansachs.com/our-thinking/pages/iot-video.html. [6]

Kidman, D. y S. Turner (2017), *Electronic persons: time for a new legal personality?*, New Law Journal, https://www.newlawjournal.co.uk/content/electronic-persons-time-new-legal-personality-0 (consultada el 15 de octubre de 2017). [44]

Law 360 (2016), *CPSC Chair Kaye Eyes Safety Risks In New Technologies - Law360*, https://www.law360.com/articles/824104/cpsc-chair-kaye-eyes-safety-risks-in-new-technologies (consultada el 13 de octubre de 2017). [71]

Live Science (2016), *What is Augmented Reality?*, https://www.livescience.com/34843-augmented-reality.html (consultada el 13 de octubre de 2017). [19]

Marco Annunziata, B. y C. Economist (2015), *The Moment For Industry*, General Electric, http://gereports.cdnist.com/wp-content/uploads/2015/09/29153350/Annunziata_Moment-for-industry_Final1.pdf (consultada el 13 de octubre de 2017). [29]

McAfee (2013), *Data Quality in the Internet of Things*, https://securingtomorrow.mcafee.com/business/data-quality-in-the-internet-of-things/ (consultada el 13 de octubre de 2017). [33]

McKinsey & Company (2016), *Unlocking the potential of the Internet of Things | McKinsey & Company*, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (consultada el 13 de octubre de 2017). [70]

McKinsey (2015), *Unlocking the potential of the Internet of Things*, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (consultada el 13 de octubre de 2017). [28]

McKinsey (2016), *Internet of Things: The IoT opportunity - Are you ready to capture a once-in-a- lifetime value pool?*, http://hk-iot-conference.gs1hk.org/2016/pdf/_04_Mc%20Kinsey%20-%20(Chris%20Ip%20)%20ppt%20part%20%201%20_IoT%20-%20Capturing%20the%20Opportunity%20vF%20-%2021%20June%202016.1pptx.pdf (consultada el 13 de octubre de 2017). [27]

Medium (2017), *IoT Raises New Challenges for Assigning Liability*, https://medium.com/iotforall/iot-raises-new-challenges-for-assigning-liability-7387b65decd0 (consultada el 13 de octubre de 2017). [37]

Meola, A. (2016), *Wearable technology and IoT wearable devices*, Business Insider, http://www.businessinsider.fr/uk/wearable-technology-iot-devices-2016-8/ (consultada el 12 de octubre de 2017). [9]

Murray, S. (2015), *How the internet of things can speed up health delivery*, https://www.ft.com/content/8ad4d226-bdcc-11e4-8cf3-00144feab7de?mhq5j=e7 (consultada el 13 de octubre de 2017). [8]

Nation, J. (2017), *IBM, Microsoft, And GS1 Will Create Supply-Line Blockchain Standards*, ETHNews.com, https://www.ethnews.com/ibm-microsoft-and-gs1-will-create-supply-line-blockchain-standards (consultada el 12 de octubre de 2017). [14]

Nation, J. (2017), *IBM, Microsoft, And GS1 Will Create Supply-Line Blockchain Standards - ETHNews.com*, https://www.ethnews.com/ibm-microsoft-and-gs1-will-create-supply-line-blockchain-standards (consultada el 12 de octubre de 2017). [64]

OCDE (2013), "Protecting and Empowering Consumers in the Purchase of Digital Content Products", *OECD Digital Economy Papers*, No. 219, OECD Publishing, París, http://dx.doi.org/10.1787/5k49czlc7wd3-en. [38]

OCDE (2015), *Digital Economy Outlook 2015*, OECD Publishing, http://dx.doi.org/10.1787/9789264232440-en. [46]

OCDE (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, París, http://dx.doi.org/10.1787/9789264232440-en. [2]

OCDE (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, París, http://dx.doi.org/10.1787/5jlwvzz8td0n-en. [1]

OCDE (2016), *Recommendation on Consumer Protection in E-Commerce*, OECD Publishing, París, http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf (consultada el 15 de octubre de 2017). [39]

OCDE (2017), *The Next Production Revolution: Implications for Governments and Business*, OECD Publishing, París, http://dx.doi.org/10.1787/9789264271036-en. [3]

OCDE (2017), "OECD Digital Economy Outlook 2017", http://www.oecd- ilibrary.org/docserver/download/9317011e.pdf?expires=1507887341&id=id&accname=ocid84004878&checksum=2FD899553D50E7BE04BFBD9687A93D0B (consultada el 13 de octubre de 2017). [12]

OCDE (2017), *Summary of the CDEP Technology Foresight Forum Economic and Social Implications of Artificial Intelligence*, https://www.oecd.org/sti/ieconomy/DSTI-CDEP(2016)17-ENG.pdf (consultada el 13 de octubre de 2017). [60]

OCDE (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, París, http://dx.doi.org/10.1787/9789264232440-en. [22]

R Street (2016), "Reality Check: The Regulatory Landscape for Virtual and Augmented Reality", *R Street Policy Study*, Vol. 9/69, https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf (consultada el 13 de octubre de 2017). [20]

R Street (2016), *Reality Check: The Regulatory Landscape for Virtual and Augmented Reality*, https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf (consultada el 13 de octubre de 2017). [67]

Reed Smith LLP (2017), *Augmented and Virtual Reality - Emerging Legal Implications of "The Final Platform" | Perspectives | Reed Smith LLP*, https://www.reedsmith.com/en/perspectives/2017/08/augmented-and-virtual-reality (consultada el 13 de octubre de 2017). [21]

Schneier, B. (2017), *Click Here to Kill Everyone with The Internet of Things*, http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html (consultada el 13 de octubre de 2017). [5]

Stanford University (2016), "ARTIFICIAL INTELLIGENCE AND LIFE IN 2030", https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf (consultada el 13 de octubre de 2017). [61]

Swiss Re (2017), *New Emerging Risks Insights 2017*, http://www.swissre.com/library/expertise-publication/swiss_re_sonar_new_emerging_risks_insights_2017.html (consultada el 15 de octubre de 2017). [43]

Tech Policy Lab University of Washington (2015), "Augmented Reality: A Technology and Policy Primer", http://techpolicylab.org/wp-content/uploads/2016/02/Augmented_Reality_Primer-TechPolicyLab.pdf (consultada el 13 de octubre de 2017). [65]

Tech Policy Lab (2015), *Augmented Reality: A Technology and Policy Primer*, Universidad de Washington, http://techpolicylab.org/wp-content/uploads/2016/02/Augmented_Reality_Primer-TechPolicyLab.pdf (consultada el 13 de octubre de 2017). [16]

Telefonica (2016), *5 Amazing Things made reality by IoT technology*, https://iot.telefonica.com/blog/5-amazing-things-made-reality-by-iot-technology-toys-edition (consultada el 13 de octubre de 2017). [11]

Telefonica (2016), *5 Amazing Things made reality by IoT technology. Toys Edition | Welcome to The IoT World of Telefónica*, https://iot.telefonica.com/blog/5-amazing-things-made-reality-by-iot-technology-toys-edition (consultada el 13 de octubre de 2017). [59]

The Engineer (2017), *How AI is Paving the Way for Fully Autonomous Cars - The Engineer*, https://www.theengineer.co.uk/ai-autonomous-cars/ (consultada el 13 de octubre de 2017). [62]

Torchia, M. (2017), *Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by Manufacturing, Transportation, and Utilities Investments, According to New IDC Spending Guide*, https://www.idc.com/getdoc.jsp?containerId=prUS42209117. [52]

Walker, S. y R. Roashan (2015), "Global Shipment and Revenue Market Forecast for Wearable Technology The Small Revolution is Making Big Waves", http://dx.doi.org/10.0. [53]

Walker, S. y R. Roashan (2015), *Wearable Technology: The Small Revolution is Making Big Waves*, IHS, https://technology.ihs.com/515418 (consultada el 13 de octubre de 2017). [10]

Weber, R. (2009), "Internet of things – Need for a new legal environment?", *Computer Law & Security Review*, Vol. 25/6, pp. 522-527, http://dx.doi.org/10.1016/j.clsr.2009.09.002. [36]

# *Notas*

[1] El M2M se entiende como comunicaciones de punto a punto entre los dispositivos que llevan a cabo acciones sin la asistencia manual de humanos, haciendo uso de módulos integrados de hardware y redes celulares o por cable. Las comunicaciones M2M son solo un elemento del IoT y solo se vuelven "inteligentes" cuando se combinan con la lógica de los servicios en la nube y de operación e interacción remota (OCDE, 2016[1]).

[2] Más información sobre los dispositivos domésticos inteligentes y las características clave se encuentra disponible en el documento de debate que se elaboró para ayudar a la discusión conforme a la sesión 3 (Consumidores en la Casa Inteligente) de la mesa redonda del CCP/WP sobre Consumidores Conectados.

[3] Una cadena de bloques puede almacenar "contratos inteligentes", los cuales son programas de software que se ejecutan de manera autónoma y distribuida por los mineros de una red basada en una cadena de bloques. Un ejemplo es OpenBazaar, el cual es un mercado descentralizado que depende de la tecnología de cadena de bloques para permitir que los compradores y vendedores interactúen directamente con el otro, sin tener que pasar por cualquier intermediario centralizado. Una vez que un comprador le solicita un producto a un vendedor, se crea una cuenta fiduciaria en la cadena de bloques de Bitcoin para asegurar que los fondos solo se liberarán luego de que el comprador haya recibido el producto (OCDE, 2017[12]).

[4] Se debe señalar que el número de tarjetas SIM/módulos de M2M solo indica el número de dispositivos de M2M que utilizan la conectividad móvil. Sin embargo, la comunicación M2M podría basarse en todo tipo de conectividad, y la conectividad móvil solo representa una pequeña parte de la conectividad que se utiliza en la comunicación M2M (OCDE, 2016[1]).

[5] Una cadena de bloques puede almacenar "contratos inteligentes", los cuales son programas de software que se ejecutan de manera autónoma y distribuida por los mineros de una red basada en una cadena de bloques. Un ejemplo es OpenBazaar, el cual es un mercado descentralizado que depende de la tecnología de cadena de bloques para permitir que los compradores y vendedores interactúen directamente con el otro, sin tener que pasar por cualquier intermediario centralizado. Una vez que un comprador le solicita un producto a un vendedor, se crea una cuenta fiduciaria en la cadena de bloques de Bitcoin para asegurar que los fondos solo se liberarán luego de que el comprador haya recibido el producto (OCDE, 2017[12]).