UNIVERSIDAD DEL CEMA
Buenos Aires
Argentina

Serie
DOCUMENTOS DE TRABAJO

Área: Ingeniería en Informática

INTERNET OF THINGS EN LA VIDA COTIDIANA

Ignacio Madrid

Noviembre 2017
Nro. 665

https://ucema.edu.ar/publicaciones/doc_trabajo.php
UCEMA: Av. Córdoba 374, C1054AAP Buenos Aires, Argentina
ISSN 1668-4575 (impreso), ISSN 1668-4583 (en línea)
Editor: Jorge M. Streb; asistente editorial: Valeria Dowding <jae@cema.edu.ar>

Internet of Things en la vida cotidiana

Ignacio Madrid*

Abstract: La internet de las cosas es la próxima revolución tecnológica que comenzó con la masificación de las computadoras entre las décadas del 70 y 80. Esta revolución va a introducir nuevas tecnologías, que va a dejar obsoletas a muchas otras existentes el día de hoy. Estas tecnologías también van a eliminar muchas fuentes de trabajo, pero a su vez, va a crear nuevos tipos de trabajo que hoy ni siquiera existen. No solo la educación, los gobiernos y los negocios van a tener que replantearse o volver a trazar rumbos, también se van a ver afectados los comportamientos de las personas y las normas sociales. La tecnología lo va a afectar todo, desde la manera en que la gente vota, come en un restaurante o se va de vacaciones. Sin embargo, todo este potencial puede traer efectos involuntarios, como la creación de nuevos tipos de crimen, armas o guerras. También hará que la sociedad se plantee algunas cuestiones relacionadas a la privacidad y a la seguridad. Mientras es imposible saber dónde exactamente nos lleve Internet of Things, está totalmente claro que un mundo centrado en la tecnología es inminente. Vamos a vivir en casas automatizadas, viajaremos en vehículos que se conducen solos, compraremos productos en negocios interactivos y estaremos conectados a un sistema de medicina y bienestar que van a redefinir el concepto de salud. Dentro de unos años, nuestro día a día va ser totalmente diferente.

* Los puntos de vista del autor no necesariamente representan la posición de la Universidad del Cema.

Introducción

El término “Internet of Things” fue usado por primera vez en 1999 por el pionero tecnológico británico Kevin Ashton en una presentación que realizó para la empresa Procter&Gamble. En esta presentación, Ashton describió un sistema en el que objetos físicos podían ser conectados a internet mediante sensores[1]. Ashton utilizó el término para ilustrar el poder de la radiofrecuencia (RFID) usado por cadenas de suministros corporativas, que utilizaban esta tecnología para poder administrar artículos sin la necesidad de que un humano intervenga. Hoy en día, Internet of Things se volvió un término popular para describir escenarios en los cuales la conectividad a internet y la capacidad computacional se extendieron a una variedad de objetos, dispositivos, sensores y artículos diarios.

Mientras el concepto de “Internet of Things” es relativamente nuevo, el concepto de combinar computadoras y redes para monitorear y controlar dispositivos ha estado entre nosotros por décadas. Para finales de los 70 por ejemplo, se habían implementado sistemas de control remoto en la red eléctrica a través de líneas telefónicas[2]. En los 90, avances en la tecnología inalámbrica permitieron “Máquina a Máquina” (M2M) soluciones empresariales e industriales para monitoreo de equipamiento. Estas soluciones tardaron poco tiempo en expandirse y volverse populares. Sin embargo, muchas de estas soluciones manejaban sus propios protocolos con estándares específicos[3], lejanos al protocolo IP.

Usar el protocolo IP para conectar dispositivos no computadoras a internet no es nuevo. El primer dispositivo conectado a internet fue una tostadora durante una conferencia de internet en 1990[4]. En los años siguientes, otros dispositivos fueron conectándose a internet, incluyendo una máquina expendedora de gaseosas en la Universidad de Carnegie Mellon[5] y una cafetera[6] en la universidad de Cambridge en el Reino Unido.

Si la idea de conectar objetos con otros objetos no es nueva es razonable preguntar, “Porque Internet of things es tan popular hoy en día?”.

[1] “That 'Internet of Things' Thing”. Kevin Ashton. http://www.rfidjournal.com/articles/view?4986
[2] “Sensor monitoring device”. Theodore G. Paraskevakos. https://patents.google.com/patent/US3842208
[3] “Know the Difference Between IoT and M2M.” Polsonetti, Chantal. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m
[4] "The Internet Toaster." Living Internet. http://www.livinginternet.com/i/ia_myths_toast.htm
[5] “The "Only" Coke Machine on the Internet." Carnegie Mellon University Computer Science Department. https://www.cs.cmu.edu/~coke/history_long.txt
[6] "The Trojan Room Coffee Pot." Stafford-Fraser, Quentin. http://www.cl.cam.ac.uk/cof

Desde una perspectiva bastante amplia, la confluencia de varias tecnologías y ciertas tendencias del mercado están haciendo posible conectar pequeños dispositivos en forma más económica y sencilla[7]:

- Conectividad omnipresente: Barata y de alta velocidad, las redes wireless y la tecnología hacen todo prácticamente "conectable".
- La adopción del protocolo IP como estándar de comunicación, que proporciona una plataforma sencilla y económica que puede ser incorporada en una gran cantidad de dispositivos.
- Economía de la computación: Impulsada por la inversión de la industria en investigación, desarrollo y fabricación, la ley de Moore[8] sigue entregando gran poder computacional por costos y consumos de energía pequeños.
- Miniaturización: Los avances en la fabricación de dispositivos le permiten a la tecnología ser incorporada a objetos muy pequeños. Junto con la economía de la computación, han impulsado el avance de pequeños y económicos sensores, que son el combustible de muchas aplicaciones IoT[9].
- Avances en análisis de información: Nuevos algoritmos, aumento en el poder de procesamiento, almacenamiento y servicios en la nube habilitan nuevas formas de análisis de grandes cantidades de información. Estas grandes cantidades de datos proveen nuevas oportunidades de extraer información y conocimiento[10].
- Ascenso de Cloud Computing: El Cloud Computing permite procesar, administrar y almacenar información remotamente, lo que habilita a pequeños dispositivos sin tanta potencia interactuar con poderosas herramientas analíticas de back-end[11].

[7] "The IoT will be as fundamental as the Internet itself." Conant, Susan. http://radar.oreilly.com/2015/06/the-iot-will-be-as-fundamental-as-the-internet-itself.html
[8] "Moore's Law." Gordon E. Moore. http://www.umsl.edu/~siegelj/information_theory/projects/Bajramovic/www.umsl.edu/_abdcf/Cs4890/link1.html
[9] "Miniaturized Electronics". Harry K. Charles Jr. http://www.jhuapl.edu/techdigest/TD/td2604/Charles.pdf
[10] "Who needs faster computers?". John Naughton. https://www.theguardian.com/commentisfree/2016/feb/14/moores-law-no-more-computer-industry-processing-power-semiconductors
[11] "The Rise of Cloud Computing". David Byrnea, Carol Corradob, Daniel Sichelc. https://bea.gov/about/pdf/acm/2017/the-rise-of-cloud-computing-minding-your-ps-and-qs.pdf

Desde esta perspectiva, el IoT representa la convergencia de una variedad de tendencias relacionadas a la computación y conectividad, que vienen evolucionando desde hace varias décadas. En el presente, un amplio abanico de sectores industriales - incluyendo el automotriz, salud, manufactura, hogar y muchos más - están considerando el potencial de incorporar tecnología IoT dentro de sus productos, servicios y operaciones[12].

En el artículo "Unlocking the Potential of the Internet of Things"[13], el McKinsey Global Institute describe un amplio rango de aplicaciones potenciales donde se espera que IoT pueda agregar valor.

Entornos donde se puede aplicar Internet of Things[14]

Industria	Descripción	Ejemplos
Salud	Dispositivos unidos al cuerpo humano o colocados dentro del mismo.	Dispositivos (para vestir e ingeribles) para monitorear y mantener la salud y el bienestar de las personas, manejar enfermedades, aumentar la aptitud física y la productividad.
Hogar	Edificios o casas	Controladores y sistemas de seguridad para el hogar.
Puntos de venta	Espacios comerciales	Negocios, bancos, restaurantes, estadios, cualquier lugar donde los consumidores consideren y compren; sistemas de autopago, optimización del inventario.
Trabajo	Espacios donde trabajan personas	Gestión de la energía y la seguridad en los edificios de oficinas; mejora de la productividad, incluso para los empleados móviles.
Fábricas	Entornos de producción estandarizados	Lugares con rutinas de trabajo repetitivas, como hospitales y granjas; eficiencia

[12] "IoT market research: Which industries are leading the curve?". Juan Jose Bello. http://www.ioti.com/strategy/iot-market-research-which-industries-are-leading-curve

[13] "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

[14] "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

		operativa, optimización del uso de los equipos y el inventario.
Obras	Entornos de producción a medida	Minería, petróleo y gas, construcción; eficiencia operativa, mantenimiento predictivo, salud y seguridad
Vehículos	Sistemas dentro de vehículos	Vehículos, incluyendo automóviles, camiones, barcos, aviones y trenes; mantenimiento basado en la condición, diseño, basado en el uso, conducción autónoma
Ciudades	Entornos urbanos	Espacios públicos e infraestructura en entornos urbanos; sistemas de control adaptativo de tráfico, contadores inteligentes, monitoreo ambiental, gestión de recursos
Exteriores	Entre entornos urbanos y rurales	Los usos exteriores incluyen las vías de ferrocarril, los vehículos autónomos (fuera de ciudades) y la navegación aérea; el enrutamiento en tiempo real, la navegación conectada, el seguimiento de envíos

Ilustración 1 - Entornos donde puede ser utilizado IoT

Muchas organizaciones han desarrollado sus propias taxonomías y categorizaciones de aplicaciones IoT. Por ejemplo, "Industrial IoT" es un término comúnmente usado por compañías y asociaciones para describir aplicaciones relacionadas a la producción de bienes y servicios, incluyendo manufacturas y servicios[15]. Otros discuten IoT por tipo de dispositivo, como dispositivos usables[16] y electrodomésticos[17]. También existen otros enfoques, como el de smart homes[18] o smart cities[19]. Sea cual sea la aplicación, está claro que IoT se podría expandir a casi cualquier aspecto de nuestras vidas.

[15] "What's Missing from the Industrial Internet of Things Conversation? Software." Cicciari, Matt http://www.wired.com/insights/2014/11/industrial-internet-of-things-software/
[16] "Internet of Things: Wearables." Paper realizado por Application Developers Alliance. http://www.appdevelopersalliance.org/internet-of-things/wearables/
[17] "Appliance Science: The Internet of Toasters (and Other Things)." Baguley, Richard, and Colin McDonald. http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/

Así como la cantidad de dispositivos conectados a internet crece, se espera que la cantidad de tráfico que estos generan se incremente significativamente. Por ejemplo, Cisco estima que la cantidad de tráfico generado por dispositivos no computadoras alcance a triplicar la población mundial para el año 2021[20]. Una implicancia de estas tendencias es que en los próximos años podríamos ver un cambio en la noción popular de lo que significa "estar en Internet". Como señaló el Profesor Neil Gershenfied del MIT, "El rápido crecimiento de la internet puede haber sido sólo el disparador que ahora está desencadenando la explosión real, como las cosas que se empiezan a usar en red"[21].

Las tecnologías Web facilitan la mayor parte de las interacciones entre las personas y los contenidos, haciéndola la característica más notoria de la experiencia internet actual. La experiencia basada en la Web es en gran parte caracterizada por el compromiso de las descargas y la generación de contenido que los usuarios realizan a través de sus computadoras y smartphones. Si las proyecciones realizadas sobre IoT se vuelven realidad, se podría llegar a ver un cambio hacia una interacción más pasiva de los usuarios con Internet. Objetos como componentes de autos, electrodomésticos y dispositivos de monitoreo; estos objetos enviarían y recibirían información en lugar de los usuarios, prácticamente con poca o nula asistencia de un ser humano.

IoT puede forzar un cambio en el pensamiento si la interacción más común con Internet y la información derivada e intercambiada de esta operación, viene de una forma pasiva de los dispositivos conectados a internet. La realización potencial de este resultado "Un mundo hiperconectado" es un testimonio de la naturaleza de la arquitectura de Internet misma, que no impone limitaciones a las aplicaciones o servicios que pueden hacer uso de la tecnología[22].

---

[18] "What Is A Smart Home?". Dann Albright. https://www.makeuseof.com/tag/smart-home/

[19] "What Is a Smart City?". CISCO. https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html

[20] "Cisco Visual Networking Index: Forecast and Methodology, 2016–2021." Cisco http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf

[21] "History of the Internet of Things- Postscapes." Postscapes http://postscapes.com/internet-of-things-history

[22] "Internet Invariants: What Really Matters." Internet Society. https://www.internetsociety.org/wp-content/uploads/2017/08/Internet20Invariants-20What20Really20Matters.pdf

Marco Teórico

A pesar de lo global y popular que se volvió Internet of Things, no hay una palabra o definición aceptada para el término. Diferentes definiciones son usadas por varios grupos para describir o promover una visión particular de lo que Internet of Things significa y sus características más importantes. Algunas definiciones especifican el concepto de Internet o de el Internet Protocol (IP), mientras otros, no lo hacen. Por ejemplo, para The Internet Architecture Board (IAB) el término "Internet of Things" (IOT) denota una tendencia cuando un número largo de dispositivos embebidos utilizan los servicios de comunicación ofrecidos por los protocolos de Internet. Muchos de estos dispositivos, frecuentemente llamados "Smart Objects", no son operados directamente por humanos, pero existen como componentes en edificios o vehículos, o están dispersos en el medio ambiente. [23]

Mientras, para Internet Engineering Task Force (IETF), el término "Smart object networking" es comúnmente usado en referencia para Internet of Things. En este contexto, "Smart Objects" son dispositivos que generalmente tienen limitaciones, como limitada energía, memoria, poder de procesamiento, o ancho de banda[24].

Publicado en 2012, the International Telecommunication Union (ITU) ITU-T Recommendation Y.2060, Overview of the Internet of Things, [25] menciona el concepto de interconectividad, pero no especifica particularmente el IoT con la Internet:

3.2.2 Internet of things (IoT): Una infraestructura para la sociedad de información, habilitando servicios avanzados interconectando cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables existentes y en evolución.

Nota 1- A través de la explotación de las capacidades de identificación, captura de datos, procesamiento y comunicación, el IoT aprovecha plenamente "las cosas" para ofrecer servicios a todo tipo de aplicaciones, al tiempo que garantiza que se cumplan los requisitos de seguridad y privacidad.

[23] "Architectural Considerations in Smart Object Networking." H. Tschofenig, J. Arkko, D. Thaler, D. McPherson. https://tools.ietf.org/html/rfc7452
[24] "Architectural Considerations in Smart Object Networking." H. Tschofenig, J. Arkko, D. Thaler, D. McPherson. https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf
[25] "Overview of the Internet of Things." ITU. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

Nota 2-Desde una perspectiva más amplia, el IoT puede ser percibido como una visión con implicaciones tecnológicas y sociales.

Otra definición se puede encontrar en el paper publicado en la IEEE Communications Magazine, donde se vincula el IoT a los servicios en la nube. Explica que IoT es un marco en el que todas las cosas tienen una representación y una presencia en Internet. Más específicamente, Internet de las Cosas tiene como objetivo ofrecer nuevas aplicaciones y servicios que generen puentes entre los mundos físicos y virtuales, en el que las comunicaciones máquina a máquina representan la comunicación de línea de base que permite las interacciones entre las cosas y las aplicaciones en la nube.[26]

Los diccionarios de Oxford[27] ofrecen una definición concisa que invoca a la Internet como un elemento de IoT:

La interconexión a través de Internet de dispositivos informáticos incorporados en objetos cotidianos, permitiéndoles enviar y recibir datos.

Todas las definiciones describen escenarios en cuales la conectividad y la capacidad computacional se extienden a una infinidad de objetos, dispositivos, sensores, e ítems no computadoras. En la mayoría se describe la capacidad que tienen estos dispositivos generar, intercambiar y consumir información, casi sin intervención del ser humano. Que existan varias definiciones de IoT no necesariamente quiere decir que estén en desacuerdo, más bien tratan de enfatizar diferentes aspectos del fenómeno IoT desde diferentes puntos de vista y casos de uso.

Sin embargo, la cantidad de definiciones dispares podrían ser fuente de confusión cuando se habla de IoT, particularmente en conversaciones entre usuarios o segmentos de la industria. Hace unos años hubo una confusión similar acerca de la neutralidad de la red[28] y el cloud computing[29], cuando diferentes interpretaciones de los términos ocasionalmente presentaban obstáculos para dialogar. Mientras sea probablemente innecesario desarrollar una sola definición de IoT, debería ser reconocido que hay diferentes perspectivas al ser tenidas en cuenta al momento de dialogar sobre el tema.

---

[26] "IEEE Communications Magazine - March 2018". IEEE
http://digital.comsoc.org/system/files/magazines/ci/2018/march/index.html
[27] "Internet of Things." Oxford Dictionaries.
http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things
[28]"One law professor's overview of the confusing net neutrality debate". Orin Kerr.
https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/11/28/one-law-professors-overview-of-the-confusing-net-neutrality-debate/?noredirect=on&utm_term=.c08a3ef76d57
[29] "Clueless CIO cloud confusion continues". Steven J. Vaughan-Nichols.
https://www.computerworld.com/article/3132950/cloud-computing/clueless-cio-cloud-confusion-continues.html

En este trabajo, los términos "Internet of Things" e "IoT" van a hacer referencia a la extensión de la conectividad y a la capacidad computacional que tienen los objetos, dispositivos y sensores, que a su vez, requieren mínima intervención humana para generar, intercambiar y consumir información.

Protocolos utilizados

Antes de avanzar con los modelos de comunicación utilizados por IoT, es necesario repasar cuales son los protocolos utilizados en estos.

Protocolo IP

Si bien existen varios protocolos usados en los modelos de comunicación de IoT, podemos decir que el principal es el IP. Cuando utilizamos Internet para cualquier actividad, ya sea para enviar un correo electrónico, transmitir datos, navegar, descargar archivos, imágenes o vídeos o cualquier otro servicio o aplicación, la comunicación entre los diferentes elementos de la red y nuestra propia computadora, notebook o smartphone, utiliza un protocolo: El IP (protocolo de Internet) que especifica el formato técnico de los paquetes y el esquema de direccionamiento para que las computadoras se comunican a través de una red[30].

Con el fin de conectarse a Internet, los dispositivos necesitan una dirección IP. La primera versión de un Protocolo de Internet utilizado públicamente fue IPv4[31] (protocolo de Internet versión 4). Este protocolo fue creado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA)[32]. DARPA es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de las tecnologías emergentes, principalmente para aplicaciones militares creada en 1958. IPv4 incluyó un sistema de direccionamiento que utiliza identificadores numéricos que constan de 32 bits. El uso de direcciones con una longitud de 32 bits limita el número total de posibles direcciones a un número de aproximadamente 4,3 mil millones de direcciones para los dispositivos conectados a Internet en todo el mundo. El número de dispositivos conectados a Internet pronto será más grande que el número de direcciones proporcionadas por IPv4. Por esta razón, y en previsión de la situación, el organismo responsable de la estandarización de los protocolos de Internet: El IETF (Internet

[30] "What IP Means and How It Works". Nadeem Unuth. https://www.lifewire.com/internet-protocol-explained-3426713
[31] "Internet Protocol." DARPA. https://tools.ietf.org/html/rfc791
[32] "About DARPA". DARPA. https://www.darpa.mil/about-us/about-darpa

Engineering Task Force) ha estado trabajando en una nueva versión de IP desde 1998: El IPv6, el protocolo sucesor que está destinado a sustituir IPv4, fue descrito formalmente en el documento estándar de Internet RFC 2460[33].

IPv6 utiliza un formato de dirección de 128 bits, lo que permite 2^{128}, o aproximadamente $3{,}4x10^{38}$ direcciones, aproximadamente 8 10^{28} veces más que IPv4. Si bien el aumento del conjunto de direcciones es uno de los beneficios más importantes de IPv6, hay otros cambios importantes tecnológicos en IPv6 que mejoran el protocolo IP: administración más fácil, mejor enrutamiento, un formato de cabecera más simple e integración de la autenticación[34].

IPv6 coexistirá con IPv4 durante algún tiempo. El despliegue de IPv6 se hará gradualmente en una convivencia ordenada con IPv4. Los dispositivos cliente, equipos de red, aplicaciones, contenidos y servicios tienen de adaptarse a la nueva versión del protocolo de Internet IPv6. Por otra parte, la transición de IPv4 a IPv6 establecerá un conjunto común de normas entre las empresas, los sistemas educativos, etc. en todo el mundo[35].

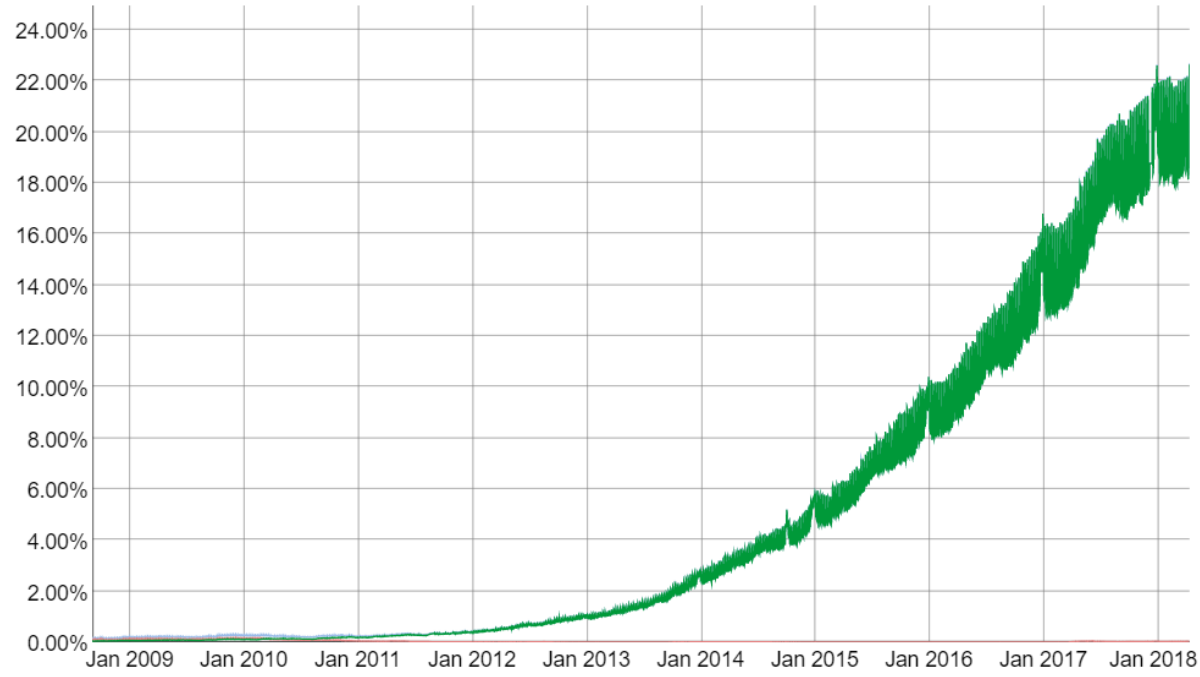

Ilustración 2 - Porcentaje de usuarios que acceden a Google a través de IPv6 desde el 2009.[36]

[33] "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460
[34] "Importance and Benefits of IPV6 over IPV4: A Study". Palukuru Venkata Praneeth Reddy, Kavali Mohammed Imran Ali, B. Sandeep, T.Ravi http://www.ijsrp.org/research-paper-1212/ijsrp-p1288.pdf
[35] "IPv6 Transition/Coexistence Security Considerations". IETF. https://tools.ietf.org/html/rfc4942
[36] Google IPv6. https://www.google.com/intl/es/ipv6/statistics.html

Las direcciones IPv6 se representan como ocho grupos de cuatro dígitos hexadecimales. Estos grupos están separados por dos puntos. El formato de la cabecera Ipv6 se puede observar en la siguiente figura:

Versión	Clase de tráfico	Nivel de flujo
Longitud de carga	Cabecera siguiente	Límite de salto
Dirección origen		
Dirección destino		

Ilustración 3 - Formato de cabecera IPv6[37]

Estructura de cabecera de IPv6	
Versión	4-bit Internet Protocol version = 6
Clase de Tráfico	8-bit campo de clase de tráfico.
Nivel de flujo	20-bit de nivel de flujo.
Longitud de carga	16-bit enteros sin signo. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue esta cabecera IPv6, en octetos.
Siguiente cabecera	8-bit selector. Identifica el tipo de cabecera inmediatamente después de la cabecera IPv6. Utiliza los mismos valores que el campo de protocolo IPv4.
Salto de Límite	8-bit enteros sin signo. Disminuye en 1 por cada nodo que reenvía el paquete. El paquete se descarta si se reduce a cero.
Dirección orígen	128-bit dirección del remitente del paquete
Dirección destino	Address 128-bit dirección del destinatario del paquete (posiblemente no es el destinatario final si un encabezado de enrutamiento está presente).

Ilustración 4 - Estructura de cabecera de IPv6[38]

[37] "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460
[38] "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460

El protocolo IPv6 ha resuelto algunos de los problemas de seguridad que se encuentran en las redes IPv4 mediante la adición obligatoria del IPsec (seguridad IP). Como resultado, IPv6 es más eficiente. IPsec mejora el protocolo IP original al proporcionar la autenticidad, integridad, confidencialidad y control de acceso a cada paquete IP a través de la utilización de dos protocolos: AH (encabezamiento de autenticación) y ESP (carga útil de seguridad de encapsulación). Por otra parte, la expansión del número de bits en el campo de dirección de 128 bits que ofrece IPv6 crea una barrera significativa para los atacantes que desean realizar el escaneo de puertos completo. Además, es posible vincular una clave pública de firma a una dirección IPv6: CGA (Dirección generada criptográficamente). IPv6 ofrece también mejoras en la seguridad de la movilidad. A pesar de que el protocolo de Internet MobileIP está disponible en IPv4 e IPv6, en IPv6 fue construido en el protocolo en lugar de ser añadido como una nueva función en IPv4. Esto significa que cualquier nodo IPv6 puede utilizar una IP móvil tanto como sea necesario. Mobile IPv6 utiliza dos extensiones titulares: Una cabecera de enrutamiento para el registro y un objetivo principal para la entrega de datos entre nodos móviles y sus nodos fijos correspondientes.[39]

Otros protocolos utilizados por IoT

La cantidad de protocolos que pueden ser utilizados por los dispositivos IoT es bastante amplia. Hoy en día existe una multitud de tecnologías de transmisión inalámbrica de datos, como por ejemplo Wi-Fi, Bluetooth, ZigBee, 2G/3G/4G, etcétera.

A estos sistemas más establecidos, hay que sumarles nuevas redes emergentes como Thread, una alternativa en el campo de la domótica, o tecnologías que utilizan la "banda blanca"[40] liberada por la televisión digital terrestre para implementar soluciones de acceso IoT en áreas extensas.

Dependiendo de la aplicación, los factores como el alcance, velocidad de transferencia, seguridad, potencia y autonomía se podrá establecer cuál es la mejor alternativa a la hora de elegir una red inalámbrica u otra. Estas son algunas de las principales tecnologías de comunicación que pueden elegir los desarrolladores:

[39] "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460
[40] "What is White Space?". The Centre for White Space Communications, University of Strathclyde. https://www.wirelesswhitespace.org/more/what-is-white-space/

ZigBee

ZigBee es una tecnología inalámbrica más centrada en aplicaciones domóticas e industriales[41]. Los perfiles ZigBee PRO y ZigBee Remote Control (RF4CE) se basan en el protocolo IEEE 802.15.4, una tecnología de red inalámbrica que opera a 2,4GHz en aplicaciones que requieren comunicaciones con baja tasa de envío de datos dentro de áreas delimitadas con un alcance de 100 metros, como viviendas o edificios.

ZigBee/RF4CE tiene algunas ventajas significativas como el bajo consumo en sistemas complejos, seguridad, robustez, alta escalabilidad y capacidad para soportar un gran número de nodos. Así, es una tecnología bien posicionada para marcar el camino del control wireless y las redes de sensores en aplicaciones IoT y M2M.

La última versión de Zigbee es la 3.0, ha sido lanzada recientemente y básicamente es la consolidación de ZigBee en un único standard.

Este protocolo es usado por Philips, en su línea de productos Hue[42]. El Hue es un sistema inalámbrico de iluminación, que permite al usuario poder administrar remotamente (a través de su celular e internet) la iluminación de su hogar. Para realizar estas tareas, Philips desarrolló un "hub", que permite la comunicación con el foco de luz. Esta comunicación se realiza a través de ZigBee.

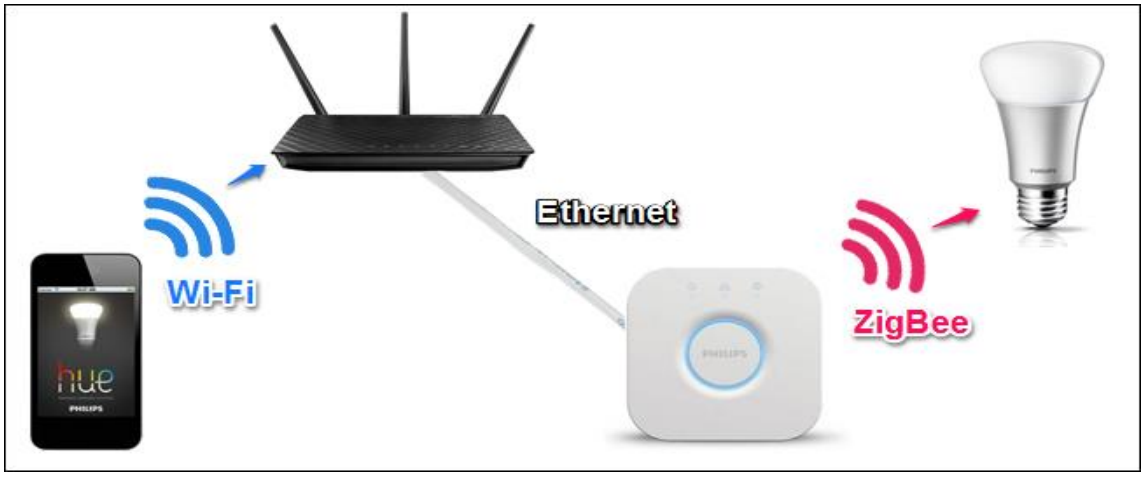

Ilustración 5 - Modelo de comunicación de Philips Hue utilizando ZigBee[43]

[41] ZigBee. http://www.zigbee.org/zigbee-for-developers/zigbee-3-0/
[42] Philips hue. https://www2.meethue.com/en-us/about-hue
[43] "What Are "ZigBee" and "Z-Wave" Smarthome Products?". Craig Lloyd. https://www.howtogeek.com/250614/what-are-zigbee-and-z-wave-smarthome-products/

WiFi

Normalmente la conectividad WiFi es la opción más elegida por los desarrolladores dada la omnipresencia que tiene en entornos domésticos y comerciales: existe en la actualidad una extensa infraestructura ya instalada que transfiere datos con rapidez y permite manejar grandes cantidades de datos. Actualmente, el standard WiFi más habitual utilizado en los hogares y en muchas empresas es el 802.11n, ofreciendo un rendimiento significativo en un rango de cientos de megabits por segundo, muy adecuado para la transferencia de archivos, pero que consume demasiada potencia para desarrollar aplicaciones IoT.

Bluetooth

Bluetooth es una de las tecnologías de transmisión de datos de corto alcance más establecidas, muy importante en el ámbito de la electrónica de consumo. Las expectativas apuntan a que será clave para desarrollar dispositivos de uso cotidiano, ya que permitirá el establecimiento de conexiones IoT, probablemente a través de un smartphone.

El nuevo Bluetooth de baja energía, también conocido como Bluetooth LE o Bluetooth Smart, es otro protocolo importante para desarrollar aplicaciones IoT[44]. Se caracteriza por ofrecer un alcance similar al de la tecnología Bluetooth normal pero con un consumo de energía significativamente reducido. Sin embargo, hay que tener en cuenta que Bluetooth LE no está diseñado para transferir archivos y es más adecuado para fragmentos de datos. Desde el punto de vista de los dispositivos de uso personal y, comparado con otras tecnologías, tiene la gran ventaja del alto grado de integración de esta tecnología en smartphones y dispositivos móviles. Según el Bluetooth Special Interest Group (SIG)[45], se espera que en el año 2018 más del 90 por ciento de los smartphones dispongan de Bluetooth "Smart Ready".

Los dispositivos que utilizan Bluetooth Smart incorporan el núcleo de Bluetooth en su versión 5.0 (la última versión a la fecha) que combina transmisión de datos básicos con una configuración de bajo consumo. Es importante destacar que desde la versión 4.0, gracias a la incorporación del Internet

[44] "Bluetooth Low Energy: It's Not Bluetooth. It's Better – Much Better". Craig Mathias. https://www.networkworld.com/article/2224506/smartphones/bluetooth-low-energy--it-s-not-bluetooth--it-s-better---much-better.html

[45] "ECSM2015-Proceedings of the 2nd European Conference on Social Media 2015". https://books.google.com.ar/books?id=VDU7CgAAQBAJ&lpg=PA398&ots=D-PIAxyjlL&dq=Bluetooth Special Interest Group (SIG) 2018 90%25&hl=es&pg=PP1 - v=onepage&q&f=false

Protocol Support Profile, permite conectarse directamente a internet mediante IPv6/6LoWPAN[46]. Esto facilita el uso de la infraestructura IP existente para gestionar dispositivos Bluetooth Smart basados en "edge computing"[47].

Thread

En la actualidad, el protocolo de red más innovador basado en IPv6 es Thread[48]. Diseñado para domótica, está basado en 6LowPAN, y del mismo modo que este último, no es un protocolo de aplicaciones IoT como Bluetooth o ZigBee. Se diseñó como un complemento WiFi, puesto que aunque la tecnología Wi-Fi funciona muy bien en dispositivos de consumo, tiene limitaciones al utilizarse en configuraciones de domótica.

Lanzado a mediados del 2014 por Thread Group, este protocolo sin canon de uso se basa en varios protocolos como IEEE 802.15.4, IPv6 y 6LoWPAN. Es una solución resistente basada en IP para aplicaciones IoT.

Diseñado para trabajar sobre chips IEEE 802.15.4 ya existentes de fabricantes como Freescale y Silicon Labs, Thread es compatible con redes de topología de malla al utilizar radio transceptores IEEE802.15.4, siendo capaz de manejar hasta 250 nodos con altos niveles de autenticación y cifrado. Actualmente, es el protocolo que utilizan los dispositivos Nest[49].

Red de telefonía móvil

Cualquier aplicación IoT que necesite funcionar en grandes áreas puede beneficiarse de las ventajas de la comunicación móvil GSM/3G/4G. La red de telefonía móvil es capaz de enviar grandes cantidades de datos, especialmente a través de 4G, aunque el consumo de energía y el coste económico de la conexión podrían ser demasiado altos para muchas aplicaciones. Sin embargo, puede ser ideal para proyectos que integren sensores y que no requieran un ancho de banda muy grande para enviar datos por Internet.

[46] "IPv6 over BLUETOOTH(R) Low Energy". IETF. https://tools.ietf.org/html/rfc7668
[47] "Edge-centric Computing: Vision and Challenges". ACM SIGCOMM Computer Communication Review. https://dl.acm.org/citation.cfm?id=2831347.2831354
[48] WHAT IS THREAD?. Thread. https://www.threadgroup.org/What-is-Thread/Overview
[49] Nest. https://developers.nest.com/

Sigfox

Una alternativa de amplio alcance es Sigfox[50], que en términos de distancia está entre Wi-Fi y la comunicación móvil. Utiliza bandas ISM, que se pueden utilizar sin necesidad de adquirir licencias.

Sigfox responde a las necesidades de muchas aplicaciones M2M[51] que funcionan con una batería pequeña y solo requieren niveles menores de transferencia de datos, donde Wi-Fi no es la mejor opción y la comunicación móvil es muy costosa, además de que consume demasiada energía. Un ejemplo de esto podría ser un dispositivo que envía registros de temperatura.

Sigfox utiliza una tecnología llamada Ultra Narrow Band (UNB) diseñada para funcionar con bajas velocidades de transferencias de 10 a 1.000 bits por segundo. Solo consume 50 microvatios (la comunicación móvil consume 5.000 microvatios) además de poder mantenerse en stand-by 20 años con una batería 2.5Ah (0,2 años para comunicaciones móviles). Ya se ha implementado en miles de objetos conectados y la red se está instalando en las principales ciudades de Europa.

Esta tecnología es robusta, energéticamente eficiente y funciona como una red escalable que puede comunicarse con millones de dispositivos móviles a lo largo de muchos kilómetros cuadrados. Así pues, es adecuada para aplicaciones M2M como: contadores inteligentes, monitores médicos, dispositivos de seguridad, alumbrado público y sensores ambientales. El sistema Sigfox utiliza los transceptores inalámbricos que funcionan en la banda sub-1GHz ofreciendo un rendimiento excepcional, mayor alcance y un consumo mínimo.

Neul

El concepto de este sistema es similar al de Sigfox y funciona en la banda sub-1GHz[52]. Neul aprovecha pequeños fragmentos de la “banda blanca” de las estaciones de TV para ofrecer alta escalabilidad, amplia cobertura y bajo costo.

[50] Sigfox. https://www.sigfox.com/en
[51] “M2M communications: A Systems Approach”. What is M2M? p.2. David Boswarthick,Omar Elloumi,Olivier Hersent. https://books.google.com.ar/books?id=bVaqAFpH6EgC&printsec=frontcover&redir_esc=y#v=onepage&q&f=falsehttps://books.google.com.ar/books?id=bVaqAFpH6EgC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false
[52] Neul. http://neul.com/

Este sistema se basa en el chip Iceni[53], que se comunica utilizando la "banda blanca" para acceder al espectro UHF de alta calidad.

La tecnología de comunicaciones que utiliza se llama Weightless[54], que es una nueva tecnología de red inalámbrica ampliada diseñada para aplicaciones IoT que compite contra las soluciones GPRS, 3G, CDMA y LTE WAN.

La velocidad de transferencia de datos puede ir de unos bits por segundo hasta 100 Mbps en el mismo enlace. Desde el punto de vista del consumo, los dispositivos consumen tan solo de 20 a 30 mA, es decir, de 10 a 15 años de autonomía con 2 pilas AA.

Para poder emplear esta tecnología hay que tener en cuenta la decisión que se haya tomado acerca del uso de las frecuencias de la banda blanda.

En ese sentido, en el Reino Unido, el organismo regulador Ofcom ha decido liberar esa banda para su uso sin licencia[55].

6LoWPAN

6LowPAN (IPv6 Low-power wireless Personal Area Network) es una tecnología inalámbrica basada en IP. En vez de tratarse de una tecnología de protocolos de aplicaciones IoT, como Bluetooth o ZigBee, 6LowPAN es un protocolo de red que permite mecanismos de encapsulado y compresión de cabeceras. Esta tecnología ofrece libertad de banda de frecuencia y capa física, por lo que se puede utilizar a través de múltiples plataformas de comunicaciones, como Ethernet, Wi-Fi, 802.15.4 y sub-1GHz ISM[56].

Una característica clave es la introducción de la pila IPv6 (protocolo de internet versión 6). Como ya mencionamos previamente, es una innovación clave en el avance de IoT para los próximos años, ya que con IPv6 se ofrecen aproximadamente 5 x 1028 direcciones IP a nivel global, permitiendo que cualquier objeto o dispositivo embebido tenga su propia dirección IP única para conectarse a Internet.

[53] "Iceni – Product Brief". http://www.neul.com/neul/wp-content/uploads/2013/06/NL-000874-PB-5-Iceni-Product-Brief.pdf
[54] "What is Weightless?". http://www.weightless.org/about/what-is-weightless
[55] "Ofcom gives green light for 'TV white space' wireless technology". Ofcom. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/tvws-statement
[56] "6LoWPAN: An Open IoT Networking Protocol". Stefan Schmidt. https://events.static.linuxfound.org/sites/events/files/slides/6lowpan-openiot-2016.pdf

Ha sido diseñada especialmente para el hogar y la automatización de edificios proporcionando un mecanismo de transporte básico para producir sistemas de control complejos e interconexión de dispositivos de un modo económico a través de una red inalámbrica de bajo consumo.

Diseñada para enviar paquetes IPv6 sobre redes IEEE 802.15.4, para luego implementar protocolos superiores como TCP, UDP, HTTP, COAP, MQTT y websockets, 6LowPAN es una red de topología en malla robusta, escalable y auto-regenerativa.

LoRaWAN

Esta tecnología se parece en algunos aspectos a Sigfox y a Neul. LoRaWAN está diseñada para implementar redes de área amplia (WAN) con características específicas para soportar comunicaciones móviles, bidireccionales, económicas y seguras para aplicaciones de IoT, M2M, ciudades inteligentes y aplicaciones industriales[57].

Optimizada para bajo consumo de energía y para ofrecer amplias redes con millones y millones de dispositivos, sus velocidades de transferencia de datos van desde 0,3 kbps hasta 50 kbps.

Z-Wave

Z-Wave es una tecnología RF de bajo consumo diseñada inicialmente para productos de domótica como controladores de iluminación y sensores[58]. Optimizado para la comunicación fiable de baja latencia de pequeños paquetes de datos, alcanza velocidades de datos de hasta 100kbit/s, opera en la banda de sub-1 GHz y es robusta frente a interferencias de Wi-Fi y otras tecnologías inalámbricas en el rango 2,4 GHz como Bluetooth o ZigBee. Es totalmente compatible con redes de topología de malla, no necesita un nodo coordinador y es muy escalable, permitiendo controlar hasta 232 dispositivos.

Z-Wave utiliza un protocolo más simple que otras tecnologías lo que permite una mayor rapidez en el desarrollo, pero el único fabricante de chips compatibles es la empresa Sigma Design, en comparación con la multitud de empresas que ofrecen productos de otras tecnologías inalámbricas como ZigBee o Bluetooth.

[57] "What is LoRaWAN?". https://www.lora-alliance.org/technology
[58] "Z-Wave". http://www.z-wave.com/about

NFC

NFC (Near Field Communication) es una tecnología que permite dos vías simultáneas de interacción segura entre dispositivos electrónicos, siendo especialmente adecuada para smartphones, permitiendo a los consumidores realizar transacciones de pago, acceder al contenido digital y conectar dispositivos electrónicos, todo esto sin contacto. Esencialmente, amplía la capacidad de la tecnología contacless de las tarjetas inteligentes permitiendo conexiones punto a punto y modos de funcionamiento activos y pasivos[59].

Protocolo	Estandar	Frecuencia	Alcance	Velocidad de transferencia
WiFi	Basado en 802.11n	2,4GHz y 5GHz	Aproximadamente 50m	hasta 600 Mbps, pero lo habitual es 150-200Mbps
Bluetooth	Bluetooth 5	2,4GHz	50-150m	2000Mbps
Z-Wave	Z-Wave Alliance ZAD12837 / ITU-T G.9959	900MHz	30m	9,6/40/100kbit/s
Zigbee	ZigBee 3.0 basado en IEEE 802.15.4	2.4GHz	10-100m	250kbps
Thread	Thread, basado en IEEE802.15.4 y 6LowPAN	2,4GHz	30m	250kbps
LoRaWAN	LoRaWAN	Depende el país	2-5km (entorno urbano), 15km (entorno rural)	50 kbps.
NFC	ISO/IEC 18000-3	13.56MHz	10cm	420kbps
Sigfox	Sigfox	900MHz	30-50km (ambientes rurales), 3-10km (ambientes urbanos)	1000bps

[59] "What is NFC? Everything you need to know". Cameron Faulkner. https://www.techradar.com/news/what-is-nfc

Red de telefonía móvil	GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)	900 / 1800 / 1900 / 2100	hasta 35km para GSM; hasta 200km para HSPA	35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)
Neul	Neul	900MHz, 458MHz, 470-790MHz	10km	100kbps
6LoWPAN	RFC6282	adaptable a múltiples capas físicas como Bluetooth Smart (2.4GHz), ZigBee o comunicación RF de bajo consumo (sub-1GHz)	200m	250kbps

Ilustración 6 - Cuadro comparativo de protocolos

También se pueden separar los protocolos según su utilización dependiendo su rango de alcance:

Utilizado para	Protocolos
Redes hogareñas	RFID WiFi NFC Z-Wave ZigBee LoWPAN Neul Bluetooth Thread
Redes locales de corto alcance	LoRa SIGFOX Weightless DECT Wavenis
Redes de area amplia	SIGFOX LoRa GSM GPRS 3G 4G

Ilustración 7 - Utilización de protocolos según su rango de acción.

(los cuadros fueron realizados con la información disponible en los sitios de los desarrolladores y mencionados en la notas de pie de cada protocolo.)

Modelos de comunicación de IoT

Desde una perspectiva operacional, es útil pensar como los dispositivos IoT se conectan y se comunican en términos de sus respectivos modelos de comunicación. En marzo del 2015, el IAB (Internet Architecture Board) lanzó un documento[60] que explica un modelo basado básicamente en 4 paradigmas comunicacionales usados por dispositivos IoT.

Comunicaciones dispositivo a dispositivo

El modelo de comunicación dispositivo a dispositivo representa a dos o más dispositivos que directamente se conectan y se comunican entre ellos. No se utiliza un servidor de aplicaciones como intermediario. Estos dispositivos se comunican sobre muchos tipos de redes, incluyendo redes IP o Internet. Frecuentemente, estos dispositivos también utilizan protocolos como Bluetooth, Z-Wave o ZigBee para establecer una comunicación directa entre los dispositivos, como se puede observar en el gráfico a continuación:

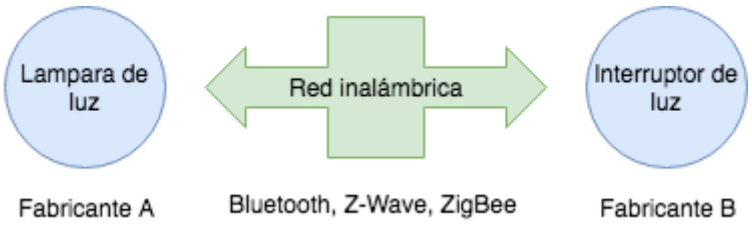

Ilustración 8 - Comunicaciones dispositivo a dispositivo.[61]

Estas redes dispositivo a dispositivo, permiten a los dispositivos adherirse a un protocolo de comunicación particular e intercambiar información para cumplir con su función. Este modelo de comunicación es comúnmente usado en aplicaciones como sistemas de automatización del hogar, que generalmente no suelen usar grandes cantidades de información, ya que la cantidad de datos que requieren estos dispositivos no son muy elevados. Los dispositivos IoT hogareños como lámparas,

[60] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. https://www.rfc-editor.org/rfc/rfc7452.txt
[61] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.4. https://www.rfc-editor.org/rfc/rfc7452.txt

interruptores, termostatos y cerraduras normalmente envían pequeñas cantidades de información, como por ejemplo un mensaje con el estado de la cerradura o prender o apagar una luz [62].

Este enfoque a la comunicación de dispositivo a dispositivo ilustra muchos de los desafíos de interoperabilidad que luego vamos a tratar en este trabajo. Como describe el artículo del IETF Journal "Estos dispositivos frecuentemente tienen una relación directa, generalmente tienen incorporados mecanismos de seguridad, pero también usan modelos específicos de datos que requieren mucho esfuerzo de desarrollo"[63]. Esto significa que los fabricantes de dispositivos necesitan invertir mucho dinero para poder implementar formatos específicos de datos en vez de utilizar enfoques abiertos que permiten utilizar formatos de datos estándares.

Desde el punto de vista del usuario, esto frecuentemente significa que los protocolos de comunicación dispositivo a dispositivo no son compatibles, forzando al usuario a elegir una familia de dispositivos que utilicen el mismo protocolo. Por ejemplo, la familia de dispositivos que utilizan el protocolo Z-Wave no son nativamente compatibles con los dispositivos de la familia ZigBee. Si bien estas incompatibilidades limitan la elección del usuario a dispositivos dentro de una familia de protocolos determinada, el usuario se beneficia al saber que los productos dentro de una familia en particular tienden a comunicarse bien.

Comunicaciones dispositivo a nube

En el modelo de comunicación dispositivo a nube[64], el dispositivo IoT se comunica directamente con un servicio en la nube[65] como un proveedor de servicios de aplicaciones para intercambiar datos y controlar el tráfico de los mensajes. Este enfoque frecuentemente se aprovecha de los mecanismos de comunicación existentes, como las tradicionales conexiones por cable Ethernet o Wi-Fi, para establecer una conexión entre el dispositivo y la red IP, que finalmente se conecta al servicio en la nube:

[62] Ibid.
[63] "IAB Releases Guidelines for Internet-of-Things Developers." Duffy Marsan, Carolyn. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf
[64] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.5. https://www.rfc-editor.org/rfc/rfc7452.txt
[65] "¿Qué es la informática en la nube?". Amazon. https://aws.amazon.com/es/what-is-cloud-computing/

Ilustración 9 - Comunicación de dispositivo a nube [66]

Este modelo de comunicación es empleado por algunos dispositivos populares de IoT como el Nest Labs Learning Thermostat[67] y el Samsung SmartTV[68].

En el caso del Nest Learning Thermostat, el dispositivo transmite información a una base de datos en la nube donde los datos pueden usarse para analizar el consumo de energía doméstica. Además, esta conexión en la nube permite al usuario obtener acceso remoto a su termostato a través de un teléfono inteligente o interfaz Web, y también admite actualizaciones de software para el termostato. De manera similar, con la tecnología SmartTV de Samsung, la televisión utiliza una conexión a Internet para transmitir información de visualización del usuario a Samsung para su análisis y para activar las características de reconocimiento de voz interactivas de la TV.

En estos casos, el modelo de dispositivo a nube agrega valor al usuario final ampliando las capacidades del dispositivo más allá de sus características nativas[69].

Sin embargo, pueden surgir problemas de interoperabilidad al intentar integrar dispositivos fabricados por diferentes empresas. Con frecuencia, el dispositivo y el servicio en la nube son del mismo proveedor. Si se utilizan protocolos de datos propietarios entre el dispositivo y el servicio en la nube, el propietario o usuario del dispositivo puede estar vinculado a un servicio en la nube específico, limitando o impidiendo el uso de proveedores de servicios alternativos. Esto se conoce comúnmente

[66] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.5. https://www.rfc-editor.org/rfc/rfc7452.txt
[67] "Meet the Nest Thermostat." Nest Labs. https://nest.com/thermostat/meet-nest-thermostat/
[68] "Samsung Privacy Policy--SmartTV Supplement." Samsung Corp. http://www.samsung.com/sg/info/privacy/smarttv.html
[69] "Why Move To The Cloud? 10 Benefits Of Cloud Computing". Salesforce UK. https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html

como "bloqueo del proveedor"[70], un término que abarca otras facetas de la relación con el proveedor, como la propiedad y el acceso a los datos. Al mismo tiempo, los usuarios generalmente pueden confiar en que los dispositivos diseñados para la plataforma específica pueden ser integrados.

Comunicaciones dispositivo a puerta de enlace

En el modelo de dispositivo a puerta de enlace[71], el dispositivo IoT se conecta a través de un servicio ALG, ubicado en otro dispositivo. Este servicio cumple con la función de túnel, para que el dispositivo IoT pueda llegar a un servicio en la nube. En términos más sencillos, esto significa que hay un software de aplicación que funciona en otro dispositivo diferente al dispositivo IoT. Este dispositivo actúa como intermediario entre el dispositivo IoT y el servicio en la nube, brindando seguridad y otras funciones, como la traducción de datos o protocolo.

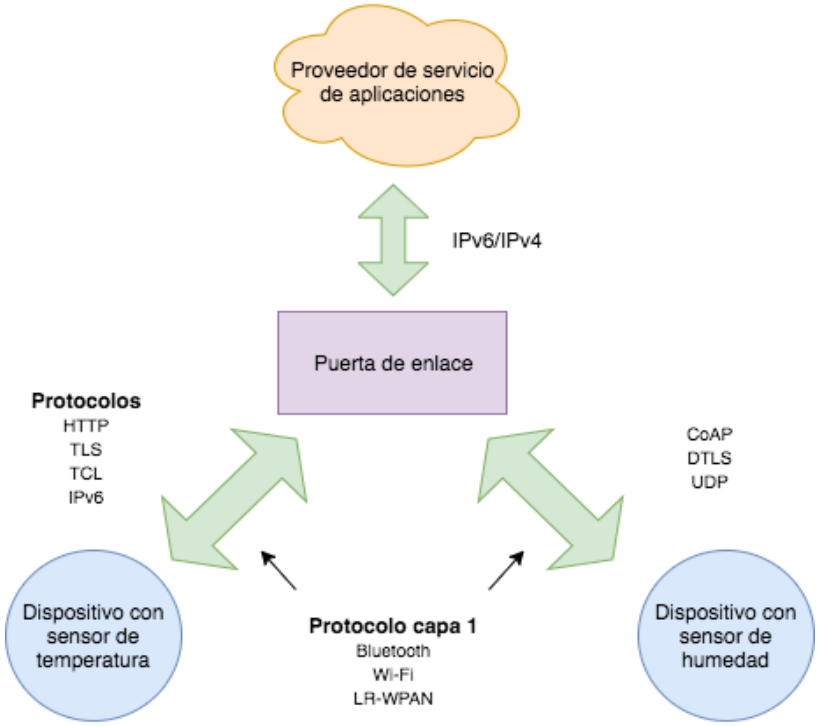

Ilustración 10 - Comunicación de dispositivo a puerta de enlace. [72]

[70] The concept of vendor lock-in and how it relates to cloud computing. CA Community. https://www.ca.com/en/blog-highlight/the-concept-of-vendor-lock-in-and-how-it-relates-to-cloud-computing.html

[71] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.6. https://www.rfc-editor.org/rfc/rfc7452.txt

[72] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.6. https://www.rfc-editor.org/rfc/rfc7452.txt

Varias formas de este modelo se pueden encontrar en dispositivos utilizados por personas en el día a día. En muchos casos, el dispositivo puerta de enlace es un smartphone corriendo una aplicación que se comunica con otro dispositivo y retransmite datos a un servicio en la nube. Este modelo es usado frecuentemente con dispositivos bastante populares como los que se utilizan para realizar ejercicio, por ejemplo el FitBit[73]. FitBit básicamente es una pulsera que recolecta información sobre nuestra actividad física y calidad de sueño. La pulsera es dependiente de un smartphone, ya que sin este es imposible configurar y enviar los datos a la nube[74]. Una vez en la nube, la aplicación nativa del mismo le permite al usuario poder acceder a su información histórica, sugerirle rutinas o nuevos hábitos.
Este tipo de dispositivos no poseen la habilidad nativa de comunicarse directamente con un servicio en la nube, por lo que dependen de una aplicación instalada en un smartphone que oficie de intermediario para conectar el dispositivo a la nube.

Existe otra forma de este modelo, que utiliza dispositivos "concentradores" y generalmente se utilizan en aplicaciones de automatización del hogar. Estos dispositivos sirven de puerta de enlace local entre dispositivos IoT y un servicio en la nube, pero también pueden superar la brecha de interoperabilidad entre los propios dispositivos. Por ejemplo, el dispositivo SmartThings puede utilizar tanto los protocolos Z-Wave como Zigbee, que le permite operar con las dos familias de dispositivos[75]. Se conectan al servicio de nube del dispositivo SmartThings, permitiendo al usuario ganar acceso a los dispositivos utilizando solamente una aplicación en el smartphone y acceso a internet.
Desde una perspectiva más técnica, el artículo de el IETF Journal explica el beneficio de este modelo:

"Este modelo de comunicación es usado en situaciones donde objetos inteligentes requieren interoperabilidad con dispositivos no IP. A veces, este enfoque se toma para integrar dispositivos IPv6 únicamente, lo que significa que una puerta de enlace es necesaria para los dispositivos y servicios heredados de IPv4." [76]

En otras palabras, este modelo de comunicación es frecuentemente usado para integrar nuevos dispositivos inteligentes en un sistema heredado con otros dispositivos que no son nativamente interoperables con estos. Un inconveniente de este enfoque es que el desarrollo necesario de software y del sistema de puerta de enlace de capa de aplicación agrega complejidad y costo al sistema en general.

[73] FitBit. https://www.fitbit.com/whyfitbit
[74] "How do I set up my Fitbit device?". FitBit Help. http://help.fitbit.com/articles/en_US/Help_article/1873
[75] "How It Works." SmartThings. http://www.smartthings.com/how-it-works
[76] "IAB Releases Guidelines for Internet-of-Things Developers." Duffy Marsan, Carolyn. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

El documento de IAB RFC7452 sugiere las perspectivas para este modelo:

"Se espera que en el futuro, los gateways más genéricos se desplegarán para reducir el costo y la complejidad de la infraestructura para los consumidores finales, las empresas y los entornos industriales. Tales gateways genéricos tienen más probabilidades de existir si los diseños de dispositivos IOT hacen uso de protocolos genéricos de Internet y no requieren gateways de capa de aplicación que traducen un protocolo de capa de aplicación a otro. El uso de gateways de capa de aplicación, en general, conducirá a un despliegue más frágil, como se ha observado en el pasado." [77]

La evolución de sistemas usando el modelo de comunicación dispositivo a puerta de enlace y su papel principal en el abordaje de los desafíos que presenta la interoperabilidad de dispositivos IoT es un punto que se sigue desarrollando en la actualidad.

Modelo de intercambio de datos Back-End

El modelo de intercambio de datos Back-End hace referencia a una arquitectura comunicacional que le permite al usuario exportar y analizar información de dispositivos inteligentes desde un servicio en la nube en combinación con otras fuentes de datos. Este enfoque es una extensión del modelo de comunicación dispositivo a nube, donde un servicio en la nube se encarga de recolectar la información de un dispositivo IoT, pero que a su vez, disponibiliza la misma a otros servicios. [78]

Por ejemplo, un persona a cargo de un complejo de oficinas estaría interesado en consolidar y analizar los datos de consumo de energía y servicios producidos por todos los sensores de IoT y sistemas de utilidad habilitados para Internet en las instalaciones. A menudo, en el modelo comunicación de dispositivo a nube, los datos que cada sensor de IoT o sistema produce se almacenan en un silo de datos independiente. Una arquitectura de intercambio de datos de Back-End permitiría a la empresa acceder y analizar fácilmente los datos en la nube producidos por todo el espectro de dispositivos en el edificio. Además, este tipo de arquitectura facilita las necesidades de portabilidad de datos. Las arquitecturas de datasharing de back-end eficaces permiten a los usuarios mover sus datos cuando cambian entre los servicios de IoT, rompiendo barreras de silo de datos tradicionales.

[77] "Architectural Considerations in Smart Object Networking". Tschofenig, H. https://tools.ietf.org/html/rfc7452
[78] Tschofenig, H., et. al., p. 9. https://tools.ietf.org/html/rfc7452

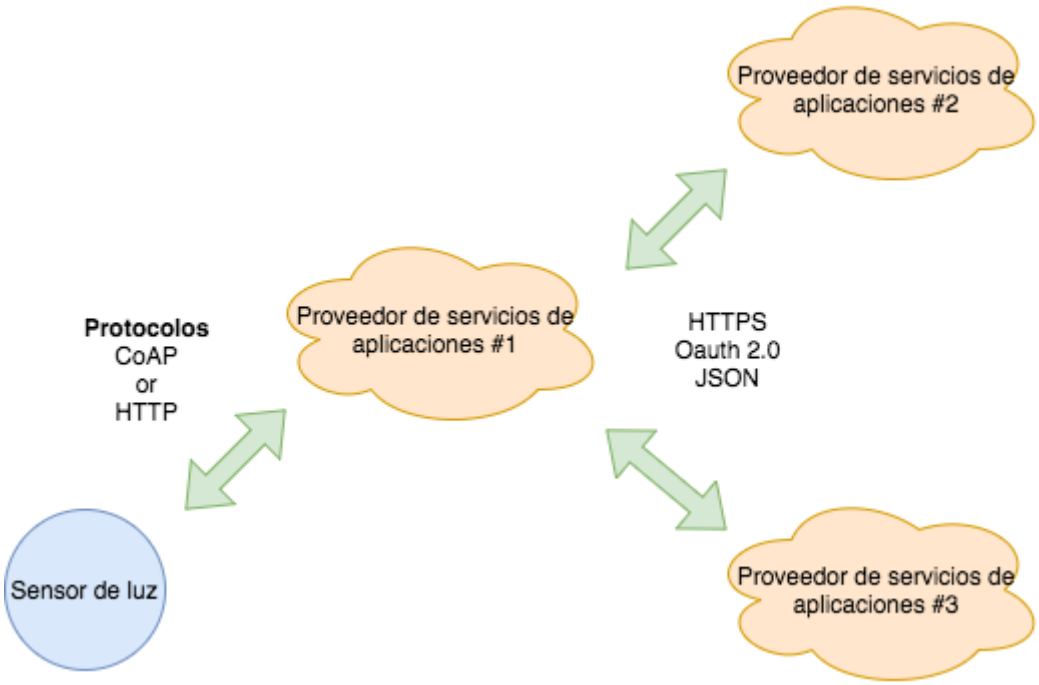

Ilustración 11 - Modelo de intercambio de datos Back-End. [79]

Este modelo de arquitectura es un enfoque para lograr interoperabilidad entre estos sistemas de back-end. Como sugiere el IETF Journal, "los protocolos estándares pueden ayudar, pero no son suficientes para eliminar los silos de datos dado que entre proveedores son necesarios modelos de información comunes"[80]. Dicho de otra manera, este modelo de comunicación es apenas tan eficaz como los diseños de los sistemas subyacentes de la IoT. Las arquitecturas de intercambio de datos a través del back-end no pueden superar completamente los diseños de los sistemas cerrados.

Los cuatro modelos básicos de comunicación muestran las estrategias de diseño utilizadas para permitir que los dispositivos de la Internet of Things se comuniquen. Además de ciertas consideraciones técnicas, el uso de estos modelos está influenciado en gran parte por la naturaleza abierta versus propietaria de los dispositivos de la IoT que se conectan en red. En el caso del modelo 'dispositivo a puerta de enlace', su principal característica es la capacidad de superar las restricciones que implica la conexión de dispositivos propietarios a la IoT. Esto significa que la interoperabilidad de los dispositivos y los estándares abiertos son consideraciones clave para el diseño y el desarrollo de sistemas de Internet of Things.

[79] "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. p.6. https://www.rfc-editor.org/rfc/rfc7452.txt
[80] "IETF Journal July of 2015". Carolyn Duffy Marsan, p.6.-p.8. https://wp.internetsociety.org/ietfjournal/wp-content/uploads/sites/22/2015/07/201507-ietf-journal-vol11-1-en.pdf

Desde el punto de vista del usuario en general, estos modelos de comunicación sirven para ilustrar la capacidad de agregar valor que tienen los dispositivos conectados en red. Al permitir que el usuario logre un mejor acceso a un dispositivo de Internet of Things y a sus datos, el valor global del dispositivo aumenta. Por ejemplo, en tres de los cuatro modelos de comunicación descritos, en última instancia los dispositivos se conectan a servicios de análisis de datos en un entorno de cómputo en la nube. Al crear conductos para comunicar datos a la nube, los usuarios y los proveedores de servicios pueden subir información, analizar grandes volúmenes de datos y visualizar datos más fácilmente; además, las tecnologías de análisis predictivo obtienen más valor de los datos de la IoT del que pueden obtener las aplicaciones de silos de datos tradicionales. En otras palabras, las arquitecturas de comunicación eficaces son un importante generador de valor para el usuario final, ya que abren la posibilidad de utilizar la información de nuevas formas. Sin embargo, cabe señalar que estos beneficios no vienen sin desventajas. Al considerar una arquitectura determinada, es necesario considerar cuidadosamente los costos que deben incurrir los usuarios para conectarse a recursos en la nube, especialmente en las regiones donde los costos de conectividad del usuario son elevados.

Los modelos de comunicación efectivos benefician al usuario final, pero también cabe mencionar que los modelos eficaces de comunicación de la IoT también mejoran la innovación técnica y las oportunidades para el crecimiento comercial. Se pueden diseñar nuevos productos y servicios que aprovechen los flujos de datos de la IoT que antes no existían, y estos podrían disparar la innovación.

Impacto de Internet of Things en la vida cotidiana

Sería imposible abarcar el universo de temas relacionados con Internet de las Cosas en un solo trabajo. No obstante, este trabajo busca resumir en cinco puntos que generalmente suelen surgir con frecuencia cuando hablamos de IoT. Estos temas son: Seguridad, privacidad, interoperabilidad y estándares, aspectos legales y economías emergentes y desarrollo.

Seguridad

Tal como se menciona en este trabajo, garantizar la seguridad, la confiabilidad, la resiliencia y la estabilidad de las aplicaciones y servicios de Internet es fundamental para fomentar la confianza y el uso de Internet. Como usuarios de Internet, tenemos que tener un alto grado de confianza en que Internet, sus aplicaciones y los dispositivos conectados a la red son lo suficientemente seguros como para realizar en línea todo el abanico de actividades que deseamos en relación con la tolerancia al riesgo asociado con tales actividades. En este sentido, la Internet de las cosas no es diferente y la seguridad de la IoT está fundamentalmente relacionada con la capacidad de los usuarios de confiar en su entorno. Si los usuarios no creen que los dispositivos que tienen conectados y su información está razonablemente protegida contra el mal uso o los daños, el desgaste de la confianza resultante provoca una negación a usar Internet. Esto tiene consecuencias globales para el comercio electrónico, la innovación técnica, la libertad de expresión y prácticamente para todos los demás aspectos de las actividades realizadas en internet. En efecto, para garantizar la seguridad en los productos y servicios de la IoT, el sector debe considerar la seguridad como una de sus máximas prioridades[81].

A medida que conectamos cada vez más dispositivos a Internet, surgen nuevas oportunidades para explotar potenciales vulnerabilidades de seguridad. Los dispositivos de la IoT mal asegurados sirven como puntos de entrada para ciber ataques, permitiendo que personas malintencionadas reprogramen un dispositivo o perjudiquen su funcionamiento. Los dispositivos defectuosos o que no funcionan bien también pueden crear vulnerabilidades o exponer los datos de los usuarios a robos de información. Los desafíos que impone la competitividad de los costos y las limitaciones técnicas de la IoT hacen que para los fabricantes de dispositivos no sea fácil diseñar funciones de seguridad adecuadas, potencialmente generando, a largo plazo, vulnerabilidades en la seguridad y dificultades en el mantenimiento. Junto con posibles deficiencias en el diseño de la seguridad, el enorme aumento del

[81] "Security in the Internet of Things". Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer. https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

número y la variedad de los dispositivos de la IoT podría aumentar las oportunidades de ataque. Sumado a la naturaleza altamente interconectada de los dispositivos de la IoT, cada dispositivo mal asegurado conectado en línea podría potencialmente afectar la seguridad y la resistencia de Internet a nivel global, no solo a nivel local. Por ejemplo, una heladera sin protección e infectada con malware que se encuentre en Estados Unidos puede enviar miles de correos electrónicos no deseados y dañinos a destinatarios de todo el mundo usando la conexión Wi-Fi de la casa[82].

Para hacer las cosas todavía más difíciles, en un mundo hiperconectado, nuestra capacidad de funcionar diariamente sin dispositivos o sistemas conectados a Internet probablemente disminuirá. De hecho, es cada vez más difícil comprar ciertos productos sin conexión a Internet, ya que algunos fabricantes solo venden productos por esta vía. Cada vez estamos más conectados y dependemos más de los dispositivos de IoT para muchos servicios esenciales, por lo que necesitamos que los dispositivos sean seguros. Pero también reconocemos que ningún dispositivo puede ser absolutamente seguro. Este creciente nivel de dependencia de los dispositivos de IoT y de los servicios de Internet con los cuales interactúan también aumenta las formas que tienen los delincuentes para acceder a los dispositivos. Si se ven comprometidos en un ataque cibernético, quizá podríamos desenchufar nuestros televisores conectados a Internet, pero no es tan fácil apagar un medidor inteligente de energía eléctrica, un sistema de control de tráfico o un marcapasos si estos dispositivos son víctimas de un ataque malicioso.[83]

Esta es la razón por la cual la seguridad de los dispositivos y servicios de la IoT debe ser un importante punto de discusión y un tema crítico. Dependemos cada vez más de estos dispositivos para servicios esenciales, por lo que su comportamiento puede tener un alcance y un impacto global.[84]

Al pensar en los dispositivos IoT, es importante entender que la seguridad de estos dispositivos no es infranqueable. La seguridad de los dispositivos de la IoT no es una proposición binaria de tipo seguro/inseguro. Por el contrario, resulta útil conceptualizar la seguridad de IoT como un espectro de vulnerabilidad según los dispositivos. Según una publicación de CISCO, el espectro va desde dispositivos totalmente desprotegidos sin ninguna función de seguridad hasta sistemas muy seguros con múltiples capas de elementos de seguridad[85]. A medida que las nuevas amenazas de seguridad

[82] "Fridge Caught Sending Spam Emails in Botnet Attack - CNET." Starr, Michelle. http://www.cnet.com/news/fridge-caught-sending-spamemails-in-botnet-attack/
[83] "The rise of IoT hacking: New dangers, new solutions". Conner Forrest. https://www.zdnet.com/article/the-rise-of-iot-hacking-new-dangers-new-solutions/
[84] "Why IoT Security Is So Critical". Ben Dickson. https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/
[85] "Securing the Internet of Things: A Proposed Framework". CISCO. https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

evolucionan, los fabricantes de dispositivos y los operadores de redes responden para hacer frente a las nuevas amenazas[86].

La seguridad general y la resiliencia de Internet of Things depende en gran parte de cómo se evalúen y gestionen los riesgos de seguridad. La seguridad de un dispositivo se puede medir en función del riesgo en el que se vea comprometido, del daño que tal situación provocaría y del tiempo y los recursos necesarios para lograr cierto nivel de protección. Si un usuario no puede tolerar un alto grado de riesgo (por ejemplo, un operador de un sistema de control de tráfico o una persona a quien se le ha implantado un dispositivo médico que está conectado a Internet), puede que para dicho usuario se justifique gastar una cantidad considerable de recursos para proteger el sistema o el dispositivo contra un ataque. Del mismo modo, si a la persona no le preocupa que su heladera pueda ser hackeada y utilizada para enviar spam, puede que no se sienta obligado a pagar por un modelo que tenga un diseño de seguridad más sofisticado si esto hace que el dispositivo sea más costoso o complejo. En esta evaluación y cálculo de la mitigación de los riesgos influyen diferentes factores. Estos factores incluyen una comprensión clara de los riesgos de seguridad actuales y posibles riesgos futuros, la estimación de los costos económicos y otros tipos de daño si los riesgos se hacen realidad, y el costo estimado de la mitigación de los riesgos[87].

Si bien este tipo de concesiones de seguridad muchas veces se realizan desde la perspectiva de los usuarios individuales y las organizaciones, también es importante tener en cuenta la interrelación de los dispositivos de la loT como parte de un ecosistema mayor. La conectividad en red de los dispositivos de la IoT significa que las decisiones de seguridad que se toman a nivel local con respecto a un dispositivo pueden tener impactos globales sobre otros dispositivos[88].

Como principio, quienes desarrollan objetos inteligentes para la Internet de las Cosas tienen la obligación de garantizar que estos dispositivos no expongan los bienes de sus propios usuarios ni de otras personas a potenciales daños. Como cuestión de negocios y de economía, los fabricantes desean reducir sus costos, su complejidad y su tiempo de comercialización. Por ejemplo, son cada vez más comunes los dispositivos de la IoT de alto volumen y bajo margen de ganancia y que ya representan

[86] "Hackers and defenders continue cybersecurity game of cat and mouse". Colin Barker. https://www.zdnet.com/article/hackers-and-defenders-continue-cyber-security-game-of-cat-and-mouse/

[87] Varias organizaciones han desarrollado guías para la evaluación de riesgos. Por ejemplo, en 2012 el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) emitió una serie de directrices, http://www.nist.gov/customcf/ get_pdf.cfm?pub_id=912091, mientras que la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron la norma ISO/IEC 31010:2009 "Gestión de riesgos – Técnicas de evaluación de riesgos". http://www.iso.org/ iso/catalogue_detail?csnumber=51073

[88] "Hacking critical infrastructure via a vending machine? The IOT reality". Myles Bray. https://www.scmagazineuk.com/hacking-critical-infrastructure-via-a-vending-machine-the-iot-reality/article/740222/

un costo adicional para los productos en los que están embebidos; añadir más memoria y un procesador más rápido para implementar medidas de seguridad podría hacer que el producto ya no fuera competitivo[89].

A nivel económico, el resultado de falta de seguridad en los dispositivos de IoT puede generar una externalidad negativa[90], donde una o más partes imponen un costo sobre otras. Un ejemplo clásico es el de la contaminación del medio ambiente, donde los costos de los daños y la limpieza (externalidades negativas) resultantes de las acciones de quien contamina son asumidos por otras partes. El hecho es que el costo de la externalidad impuesto a los demás normalmente no se considera en el proceso de toma de decisiones, a menos que, como es el caso de la contaminación, se aplique un impuesto que sirva de estímulo para reducir la contaminación.

De acuerdo con Bruce Schneier[91], en el caso de la seguridad de la información surge una externalidad cuando el proveedor que crea el producto no corre con los costos que ocasionan las potenciales inseguridades; en este caso, una ley de responsabilidad puede convencer a los vendedores para que tomen en cuenta la externalidad y desarrollen productos con un standard de seguridad más alto. Estas consideraciones de seguridad no son nuevas en el contexto de la tecnología de la información, pero la magnitud de los desafíos que pueden surgir en las implementaciones de la IoT las vuelve extremadamente significativas. Estos desafíos se pueden clasificar de la siguiente manera:

- Muchos dispositivos de IoT (por ejemplo, los sensores y los artículos de consumo) están diseñados para ser desplegados a una escala masiva que es significativamente superior a la de los dispositivos tradicionalmente conectados a Internet. Por consiguiente, la potencial cantidad de enlaces interconectados entre estos dispositivos no tiene precedentes. Además, muchos de estos dispositivos podrán establecer enlaces y comunicarse con otros dispositivos por sí mismos, de manera impredecible y dinámica. Por lo tanto, puede ser necesario considerar nuevamente las herramientas, métodos y estrategias existentes asociadas con la seguridad de la IoT[92].

- Muchos desarrollos de IoT consistirán en colecciones de dispositivos idénticos o prácticamente idénticos. Esta homogeneidad amplifica el potencial de impacto de cualquier

[89] "The internet of things: convenience at a price". Nicole Kobie. https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security
[90] "EXTERNALIDADES Y MEDIOAMBIENTE". Víctor Manuel Vázquez Manzanares. http://www.eumed.net/rev/ibemark/02/medioambiente.html
[91] "Information Security and Externalities". Bruce Schneier https://www.schneier.com/essays/archives/2007/01/information_security_1.html
[92] "Will utilities drive IoT security market growth?". Donal Power. https://www.ibm.com/blogs/internet-of-things/will-utilities-drive-iot-security-market-growth/

vulnerabilidad de seguridad simplemente por la gran cantidad de dispositivos que tienen las mismas características. Por ejemplo, una vulnerabilidad en el protocolo de comunicación de una marca de focos de luz conectadas a Internet se podría extender a todas las marcas y modelos de dispositivos que utilizan el mismo protocolo o que comparten características de diseño o fabricación[93].

- Muchos de los dispositivos de IoT que se van a desarrollar y se desarrollan, tienen una vida útil muy superior a la que típicamente se espera para los equipos de alta tecnología. Además, estos dispositivos se podrían desplegar en circunstancias en las que se haría muy difícil o imposible reconfigurarlos o actualizarlos; o bien estos dispositivos podrían sobrevivir a la empresa que los creó, lo que los dejaría huérfanos y sin soporte a largo plazo. Estos escenarios ilustran que los mecanismos de seguridad que son adecuados al momento del desarrollo podrían no ser adecuados durante toda la vida útil del dispositivo y a medida que las amenazas a la seguridad evolucionen. Esta situación podría crear vulnerabilidades que podrían persistir por mucho tiempo. Esto contrasta con el paradigma de los sistemas de computadoras tradicionales en los cuales normalmente se aplican actualizaciones al sistema operativo durante toda la vida de servicio de los equipos para hacer frente a las amenazas de seguridad. El apoyo y la gestión a largo plazo de los dispositivos de la IoT representa un importante reto de seguridad[94].

- Muchos dispositivos de la IoT están diseñados intencionadamente sin ninguna posibilidad de actualización; en otros, el proceso de actualización es engorroso o poco práctico. Por ejemplo, consideremos la llamada a revisión de 1.4 millones de automóviles Fiat Chrysler 2015 para arreglar una vulnerabilidad que potencialmente permitiría hackear el vehículo en forma inalámbrica[95]. Estos vehículos se deben llevar a un concesionario Fiat Chrysler para que les realicen una actualización manual del software, o bien los propietarios deben actualizar el software por su cuenta usando una memoria USB. La realidad es que un alto porcentaje de estos automóviles probablemente no se actualizará porque el proceso de actualización representa un inconveniente para los propietarios, y esto los deja permanentemente vulnerables a las amenazas de seguridad cibernética, sobre todo porque el automóvil parece estar funcionando sin inconvenientes.

[93] "Should I worry about my Philips Hue? Smart lights hacked by fly-by drone attack". Thomas Newton. http://uk.pcmag.com/philips-hue-connected-bulb/85962/news/should-i-worry-about-my-philips-hue-smart-lights-hacked-by-f
[94] "Why Do IoT Devices Die?". Leor Grebler. https://medium.com/iotforall/why-do-iot-devices-die-e4df0c7a075d
[95] "Fiat Chrysler recalls 1.4m vehicles in wake of Jeep hacking revelation". https://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking

- La mayoría de los dispositivos de la IoT funcionan de modo que es escasa o nula la visibilidad que tiene el usuario de su funcionamiento interno o de los flujos de datos que producen. Si un usuario cree que un dispositivo está ejecutando ciertas funciones pero en realidad está ejecutando funciones no deseadas o recogiendo más información de la que el usuario desea, se crea una vulnerabilidad. Las funciones del dispositivo también podrían cambiar sin previo aviso cuando el fabricante ofrece una actualización, lo que deja al usuario vulnerable a cualquier cambio que realice el fabricante[96].

- Algunos dispositivos de IoT probablemente son y serán implementados en lugares donde sea difícil o imposible lograr la seguridad física. Los atacantes pueden tener acceso físico directo a los dispositivos. Para garantizar la seguridad será necesario considerar el uso de protección contra manipulaciones y otras innovaciones de diseño[97].

- Al igual que muchos sensores ambientales, algunos dispositivos de IoT han sido diseñados para ser integrados discretamente en su entorno, donde los usuarios apenas se den cuenta de su presencia y funcionamiento. Además, los dispositivos pueden no tener una forma clara de alertar al usuario cuando surge un problema de seguridad, por lo que es difícil para un usuario saber que la seguridad de un dispositivo ha sido vulnerada. Esta situación podría persistir por mucho tiempo antes de ser detectada y corregida; incluso podría darse el caso de que no fuera posible o práctico implementar una corrección o mitigación. Del mismo modo, el usuario podría no ser consciente de que existe un sensor en su entorno, por lo que potencialmente un fallo de seguridad podría persistir por mucho tiempo sin ser detectado[98].

- Cuando uno habla de Internet of Things, uno se imagina que los dispositivos son construidos por producto de grandes empresas de tecnología. Sin embargo, en el futuro "construir su propia Internet de las Cosas" (Build Your own Internet of Things, BYIoT) podría convertirse en algo habitual, como lo demuestra el crecimiento de las comunidades de desarrolladores de Arduino y Raspberry Pi[99]. Estos desarrollos podrán o no aplicar los estándares de mejores prácticas de seguridad de la industria.

---

[96] "IoT security: the majority of IoT devices is not monitored in real time". I-SCOOP. https://www.i-scoop.eu/iot-security-majority-iot-devices-not-monitored-real-time/

[97] "IoT in Physical Security: Understanding Threats and Concerns". Bernhard Mehl. https://www.getkisi.com/blog/secure-iot-physical-security-whitepaper-free-pdf-download

[98] "The silent, lethal rise of the 'shadow Internet of Things'". John E Dunn. https://www.techworld.com/security/silent-lethal-rise-of-shadow-internet-of-things-3614910/

[99] Ver también la comunidad de código abierto Arduino http://www.arduino.cc y la Fundación Raspberry Pi http://www.raspberrypi.org/

Privacidad

Antecedentes de la privacidad en la Internet de las Cosas

El respeto por la privacidad es fundamental para asegurar la confianza en Internet; además, también afecta la capacidad de las personas de hablar, conectarse y elegir de formas significativas. Estos derechos se suelen enmarcar en términos del manejo ético de los datos[100], que hace hincapié en la importancia de respetar la privacidad del individuo y el uso legítimo de sus datos. La Internet de las Cosas puede desafiar nuestras expectativas de privacidad.

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra capacidad colectiva de confiar en Internet.

Como se ha mencionado previamente, la IoT suele referirse a una amplia red de dispositivos con sensores diseñados para recopilar datos acerca de su entorno, que muchas veces incluyen datos relacionados a las personas. Estos datos presumiblemente proporcionan un beneficio al propietario del dispositivo, pero muchas veces también benefician al fabricante o proveedor. La recopilación y el uso de los datos se convierte en una consideración de privacidad cuando las expectativas de privacidad de quienes son observados por los dispositivos de la IoT difieren de las de quienes recogerán y usarán estos datos[101].

También hay combinaciones de flujos de datos de IoT que, aparentemente inocentes también pueden poner en riesgo la privacidad. Cuando se combinan o correlacionan flujos de datos individuales, el retrato digital que se obtiene de las personas puede ser más invasivo que el que se puede obtener a partir de un flujo de datos individual. Por ejemplo, un cepillo de dientes con conexión a Internet puede recoger y transmitir información sobre los hábitos de cepillado de una persona, algo bastante intrascendente. En cambio, si la heladera de este mismo usuario informa el listado de los alimentos que consume, y si además el dispositivo que el usuario utiliza para monitorear su actividad física también informa los datos correspondientes, la combinación de toda esta información genera una descripción mucho más detallada y privada de la salud general de la persona. Este combinación de datos puede ser particularmente potente en el caso de los dispositivos de la IoT, dado que muchos

[100] "Four Ethical Issues in Online Trust." Wilton, Robin.
https://www.internetsociety.org/sites/default/files/Ethical Data-handling - v2.0.pdf
[101] "60% of IoT devices falling short on privacy and data protection". Sarah Wray.
https://inform.tmforum.org/news/2016/09/60-iot-devices-falling-short-privacy-data-protection/

producen otros metadatos como por ejemplo marcas de tiempo e información de geolocalización, lo que aumenta aún más la especificidad del usuario[102].

En otras situaciones, el usuario puede no estar al tanto de que un dispositivo está recolectando datos sobre su persona y potencialmente compartiéndolos con terceros. Este tipo de recolección de datos es cada vez más frecuente en los dispositivos de consumo, como por ejemplo los denominados altavoces inteligentes. Estos dispositivos realizan tareas que van desde reproducir música o hacer un pedido de comida. Tienen características de reconocimiento de voz, que permanentemente escuchan las conversaciones en una habitación y selectivamente transmiten los datos recogidos a un servicio en la nube para su procesamiento, donde a veces participa un tercero. Una persona podría estar en presencia de este tipo de dispositivos sin saber que sus conversaciones o actividades están siendo monitoreadas o que sus datos están siendo registrados. Este tipo de características puede ser de beneficio para un usuario informado, pero pueden plantear un problema de privacidad para quienes no son conscientes de la presencia de estos dispositivos y no pueden influir significativamente sobre la forma en que se utiliza la información recogida[103].

Sin importar si el usuario está al tanto de que los dispositivos de la IoT recogen y analizan sus datos, estas situaciones ponen al descubierto el valor que tienen estos flujos de datos personalizados para empresas y organizaciones que buscan recoger y sacar provecho de la información obtenida a través de Internet of Things. La demanda de esta información deja en evidencia los desafíos legales y regulatorios que enfrentan las leyes de protección de datos y privacidad.[104]

Es fundamental abordar estos tipos de problemas de privacidad, dado que tienen implicaciones sobre nuestros derechos básicos y nuestra capacidad colectiva de confiar en Internet. Desde una perspectiva más amplia, las personas reconocen que su privacidad es un valor intrínseco y tienen expectativas con respecto a los datos personales que se pueden recoger y cómo estos datos pueden ser utilizados por terceros[105]. Este concepto general acerca de la privacidad también vale para los datos recogidos por los dispositivos de la Internet de las Cosas, ya que estos pueden vulnerar la capacidad del usuario de expresar y hacer cumplir sus preferencias de privacidad. Si el hecho de que sus preferencias de

[102] "Your New Fridge Is Spying on You". Harrison Cramer https://tcf.org/content/commentary/new-fridge-spying/
[103] "Is Alexa Really Eavesdropping on You?". Brad Stone. https://www.bloomberg.com/news/articles/2017-12-11/is-alexa-really-eavesdropping-on-you-jb25c6vc
[104] "Why the fight over IoT data is just getting started". Gary Eastwood. https://www.networkworld.com/article/3234367/internet-of-things/why-the-fight-over-iot-data-is-just-getting-started.html
[105] "People are really worried about IoT data privacy and security—and they should be". Fredric Paul. https://www.networkworld.com/article/3267065/internet-of-things/people-are-really-worried-about-iot-data-privacy-and-securityand-they-should-be.html

privacidad no sean respetadas por Internet of Things hace que los usuarios pierdan su confianza en Internet, entonces podría disminuir el mayor valor que tiene esta.

Puntos relacionados a la privacidad y que solo aplican a IoT

En general, a medida que IoT aumenta su popularidad, también aumentan los problemas relacionados a la privacidad. Las características de los dispositivos de Internet of Things y las formas en que se utilizan redefinen el debate sobre los temas de privacidad, ya que modifican drásticamente cómo se recogen, analizan, utilizan y protegen los datos personales. Por ejemplo:

- El típico modelo de privacidad de "notificación y consentimiento" en que los usuarios hacen valer sus preferencias de privacidad interactuando directamente con información que aparece en la pantalla de una computadora o dispositivo móvil (por ejemplo, haciendo click en "Acepto") deja de ser válido cuando los sistemas no le ofrecen al usuario ningún mecanismo de interacción. Muchas veces los dispositivos de la IoT no tienen una interfaz de usuario para configurar las preferencias de privacidad, y en muchas configuraciones los usuarios no tienen conocimiento ni controlan la forma en que se recogen y utilizan sus datos personales. Esto provoca una brecha entre las preferencias de privacidad del usuario y el comportamiento de recolección de datos del dispositivo. Si consideran que los datos recopilados no son datos personales, es posible que los proveedores de dispositivos de Internet of Things se sientan menos incentivados a ofrecer a los usuarios un mecanismo para que expresen sus preferencias de privacidad. Sin embargo, la experiencia demuestra que, en realidad, los datos que tradicionalmente no se consideran personales podrían ser o convertirse en datos personales si se combinan con otros.[106]

- Supongamos que se pudiera desarrollar un mecanismo eficaz que permitiera que un usuario exprese sus preferencias de privacidad. Este mecanismo debería poder manejar la gran cantidad de dispositivos de IoT que debe controlar cada usuario. No es practico ni realista pensar que un usuario interactuará directamente con cada uno de los dispositivos con que se encuentre a lo largo del día para expresar sus preferencias de privacidad. Por el contrario, las interfaces de privacidad se deben poder escalar de acuerdo con el tamaño del problema, sin dejar de ser completas y prácticas desde la perspectiva del usuario.

- Internet of things puede poner en riesgo las expectativas de los usuarios con respecto a la privacidad en situaciones cotidianas. Las normas sociales y expectativas de privacidad

[106] "IoT silliness: 'Headless' devices without UI". Galem Gruman. https://www.infoworld.com/article/2867356/internet-of-things/beware-this-iot-fallacy-the-headless-device.html

difieren en los espacios públicos frente a los espacios privados; los dispositivos de Internet of Things desafían estas normas. Por ejemplo, las tecnologías de vigilancia que utiliza Internet of Things como las cámaras de vigilancia o los sistemas de trazabilidad de ubicación que normalmente funcionan en espacios públicos están migrando hacia espacios tradicionalmente privados como el hogar o los vehículos particulares, donde nuestras expectativas de privacidad son muy diferentes. Al hacerlo, desafían lo que muchas sociedades reconocen como el derecho a la privacidad en el hogar o los espacios privados. [107]

- Muchas veces los dispositivos de Internet de las Cosas funcionan en contextos donde la cercanía expone a múltiples personas a una misma actividad de recolección de datos. Por ejemplo, el sensor de seguimiento por geolocalización de un auto podría registrar los datos de localización de todos los pasajeros del vehículo, sin importar si estas personas desean que lo haga o no. Incluso podría realizar un seguimiento de las personas que viajan en otros vehículos cercanos. En este tipo de situaciones podría ser difícil, imposible distinguir y mucho menos respetar las preferencias de privacidad de cada una de estas personas.

- El análisis de información personal consolidada a gran escala de por sí representa un riesgo sustancial de invasión a la privacidad y potencial discriminación. Este riesgo se amplifica en IoT debido a la escala y a la mayor intimidad de la recolección de datos personales. Los dispositivos de Internet de las Cosas pueden recoger información personal con un grado de especificidad y penetración sin precedente; agregar y correlacionar estos datos permite crear perfiles personales detallados que generan un potencial para la discriminación y otros daños. Un ejemplo de esto se da en la industria del seguro, donde se utilizan los datos recolectados por IoT para ser tenidos en cuenta al momento ver si se le otorga una póliza a alguien o no. La sofisticación de esta tecnología puede crear situaciones que expongan al individuo a daños físicos, penales, financieros o de reputación.[108]

- La familiaridad y aceptación social de muchos dispositivos de Internet de las Cosas pueden crear una falsa sensación de seguridad y alentar a las personas a divulgar información confidencial o privada sin pleno conocimiento o apreciación de las posibles consecuencias.[109]

[107] "The psychology of privacy in the era of the Internet of Things". Susan Scutti. https://edition.cnn.com/2017/03/22/health/psychology-privacy-wikileaks-internet-of-things/index.html
[108] "Insurance industry lags behind in using IoT data to boost business value". Alison DeNisco Rayome. https://www.techrepublic.com/article/insurance-industry-lags-behind-in-using-iot-data-to-boost-business-value/
[109] "Putting Privacy Concerns about the Internet of Things in Perspective". Adam Thierer. https://iapp.org/news/a/putting-privacy-concerns-about-the-internet-of-things-in-perspective/

Interoperabilidad

En la Internet tradicional, la interoperabilidad es el valor central más importante; el primer requisito de la conectividad a Internet es que los sistemas "conectados" deben poder "hablar el mismo idioma" en cuanto a protocolos y codificaciones[110]. La interoperabilidad es tan fundamental que los primeros talleres para fabricantes de equipos de Internet se denominaban "Interops"[111]; además, es el objetivo explícito de todo el aparato de estandarización de Internet concentrado en el Grupo de Trabajo en Ingeniería de Internet (IETF[112]).

La interoperabilidad es también una de las piedras angulares de la Internet abierta[113]. Las barreras que puedan llegar a surgir para obstruir el intercambio de información puede afectar la capacidad de los usuarios de Internet de conectarse, hablar, compartir e innovar. También llamadas "jardines vallados[114]'', las plataformas cerradas en las que los usuarios solo pueden interactuar con un subconjunto seleccionado de sitios y servicios pueden disminuir considerablemente los beneficios sociales, políticos y económicos que permite el acceso a la totalidad de Internet.

En un ambiente totalmente interoperable, cualquier dispositivo de la Internet of Things se podría conectar a cualquier otro dispositivo o sistema e intercambiar información si así lo quisieran. En la práctica, la interoperabilidad es mucho más compleja. La interoperabilidad entre los dispositivos y sistemas de Internet of Things ocurre en diferentes grados en diferentes capas dentro de la pila de protocolos de comunicación entre los dispositivos. Además, no siempre es posible, necesario o deseable lograr la interoperabilidad plena en todos los aspectos de un producto y, de ser impuesta artificialmente (por ejemplo, a través de un mandato gubernamental o legislación), podría desincentivar la inversión y la innovación. La estandarización y la adopción de protocolos que especifican estos detalles de la comunicación, en particular cuando resulta óptimo tener estándares, están en el centro de la discusión sobre la interoperabilidad para la IoT.[115]

---

[110] "Internet interoperability". Richard Feasey. https://innovation-regulation.telecom-paristech.fr/wp-content/uploads/2017/10/Internet-Interoperability.pdf

[111] "A History of the Internet" . http://inthistory4u.blogspot.com/2010/08/1988.html

[112] "A Mission Statement for the IETF. H. Alvestrand. https://www.rfc-editor.org/rfc/rfc3935.txt

[113] "Open Internet: What is it, and how to avoid mistaking it for something else". Internet Society https://www.internetsociety.org/wp-content/uploads/2017/08/The20Open20Internet20What20it20is2C20and20how20to20avoid20mistaking20it20for20something20else20.pdf

[114] "What is a Walled Garden? And why it is the strategy of Google, Facebook and Amazon Ads platform?". Pierre de Poulpiquet. https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1

[115] "Why interoperability holds the keys to the smart home". Jessica Groopman. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-interoperability-holds-the-keys-to-the-smart-home

Más allá de las cuestiones técnicas, la interoperabilidad tiene una marcada influencia sobre el potencial impacto económico de Internet of Things. La interoperabilidad eficaz y bien definida de los dispositivos puede fomentar la innovación y estandarización para quienes fabrican dispositivos inteligentes, aumentando así el valor económico total del mercado. Por otra parte, la implementación de los estándares existentes y el desarrollo de nuevos estándares abiertos cuando estos son necesarios ayudan a reducir las barreras de entrada, facilitan nuevos modelos de negocio y construyen economías de escala[116].

Un artículo del McKinsey Global Institute publicado en 2015 sostiene que "en promedio, la interoperabilidad es necesaria para crear un 40 por ciento del potencial valor que puede generar la IoT en diversos entornos."[117] El informe continúa diciendo que "La interoperabilidad es necesaria para desbloquear más de 4 billones de dólares al año de potencial impacto económico por el uso de la IoT en 2025, de un impacto total de $11.1 billones en los nueve entornos analizados por McKinsey". Aunque para algunas empresas el hecho de construir sistemas propietarios pareciera tener ventajas competitivas e incentivos económicos, en un mercado de silos las oportunidades económicas pueden ser limitadas[118].

Además, la interoperabilidad tiene un gran valor tanto desde el punto de vista del usuario individual como de las organizaciones que utilizan estos dispositivos. Facilita la capacidad de escoger los dispositivos con las mejores características y al mejor precio e integrarlos de manera que funcionen juntos. Los consumidores podrían dudar a la hora de adquirir productos y servicios de Internet of Things si no existe flexibilidad en cuanto a su integración, si su propiedad es compleja, si existe preocupación con respecto a una potencial dependencia del proveedor o en caso de temor a su obsolescencia debido al cambio de estándares.[119]

Algunos fabricantes de dispositivos ven una ventaja competitiva en la creación de un universo de productos propietarios compatibles; los mencionados previamente "jardines vallados". Generalmente, las características que tienen estos productos es que limitan interoperabilidad a los dispositivos y componentes de una misma marca. Estos fabricantes pueden generar dependencia (lock-in) en el

[116] "Rolling plan for ICT standardisation. European Commission". Sección 3.5.6, https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation
[117] "The Internet of Things: Mapping the Value beyond the Hype". McKinsey Global Institute. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
[118] "Freedom and Walled Gardens". Bryon Moyer. http://www.insidetheiot.com/freedom-walled-garden/
[119] "Why interoperability is key to building confidence in IoT". Dr. Omar Elloumi. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-interoperability-is-key-to-building-confidence-in-IoT

ecosistema de sus dispositivos, aumentando los costos en que deben incurrir los consumidores para cambiar a otra marca o utilizar componentes de otros fabricantes. Por ejemplo, los focos de luz de un fabricante podrían no ser interoperables con un sistema de interruptores de otro. Un claro ejemplo de esto son los dispositivos de iluminación fabricados por Philips: HUE.[120]

Existen varios puntos de vista con respecto a si la interoperabilidad es beneficiosa o no para los usuarios. Los partidarios de la interoperabilidad consideran que estas prácticas impiden la elección del usuario, dado que evitan que estos se cambien a productos alternativos. También consideran que estas prácticas representan una barrera para la innovación y la competencia, ya que limitan la capacidad de los competidores de crear nuevos productos basados en la infraestructura en la cual se sustenta el ecosistema. Sin embargo, algunos fabricantes de dispositivos consideran que el enfoque del ecosistema cerrado beneficia a los usuarios porque les proporciona un protocolo que se puede adaptar con mayor rapidez y facilidad cada vez que las exigencias técnicas o de mercado requieran un cambio.[121]

Las consideraciones con respecto a interoperabilidad también se extienden a los datos que recogen y procesan los servicios de Internet of Things. Uno de los principales atractivos de los dispositivos conectados es su capacidad de transmitir y recibir datos de los servicios "en la nube", que a su vez proporcionan valiosos servicios o información sobre la base de esos datos. Si bien esto es muy útil, también puede presentar desafíos en caso que un usuario desee pasar a un servicio de otro fabricante. Incluso si el acceso a los datos generados por los dispositivos se pone a disposición de los usuarios, obtener los datos no servirá de nada si están en un formato propietario. Un usuario solo podrá cambiarse a otro proveedor de servicios o analizar los datos por su cuenta si los datos fuente están libremente disponibles para los usuarios que los originan y en un formato abierto estándar.[122]

A medida que los fabricantes crean dispositivos de Internet de las Cosas van surgiendo limitaciones técnicas, de tiempo al mercado y de costos que hay que tener en cuenta a la hora de decidir sobre su interoperabilidad y su diseño. Algunos dispositivos se ven limitados por factores técnicos como los recursos de procesamiento disponibles, la memoria o las demandas de energía. Del mismo modo, los fabricantes se ven presionados para reducir el costo unitario de los dispositivos, reduciendo al mínimo los costos de diseño de los productos y las piezas utilizadas. Los fabricantes realizan análisis de costo-

[120] "Philips Lighting: Standardization and Interoperability are Keys to Success". Weili Lin. https://mysmahome.com/company/5907/philips-lighting-standardization-and-interoperability-are-keys-to-success-2/
[121] "Interoperability: A key barrier to connected home adoption". Harry Wang. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Interoperability-A-key-barrier-to-connected-home-adoption
[122] "Fitbit leverages Google Cloud to accelerate healthcare innovation". Ryan Daws. https://www.iottechnews.com/news/2018/apr/30/fitbit-google-cloud-digital-healthcare/

beneficio para decidir si los mayores costos y las potenciales reducciones del rendimiento de los productos justifican los beneficios adicionales que tendría la implementación de los estándares. A corto plazo, puede ser más costoso diseñar e incluir características de interoperabilidad en un producto y probar su conformidad con la especificación de una norma. En ciertos contextos, el camino más económico al mercado podría ser el uso de protocolos y sistemas propietarios. Sin embargo, esto se debe comparar con las ganancias que se obtendrán durante el ciclo de vida a largo plazo gracias a la interoperabilidad del producto.[123]

En un mercado competitivo y globalizado, quien saca un producto y fija un precio de mercado más rápidamente suele tener una ventaja. Esto también se aplica a los fabricantes de dispositivos de Internet de las Cosas. El problema surge cuando el cronograma de diseño del fabricante se adelanta a la disponibilidad de los estándares de interoperabilidad. Un fabricante de dispositivos ansioso por sacar un producto al mercado puede considerar que la falta de certeza en cuanto a los tiempos y los procesos de desarrollo de los estándares constituye un riesgo comercial que se debe minimizar o evitar. Esto puede hacer que las alternativas de diseño que no contemplan estándares de interoperabilidad abiertos sean más atractivas, especialmente a corto plazo.[124]

Como parte del proceso de desarrollo, quien fabrica o utiliza dispositivos para IoT debe evaluar los riesgos técnicos de diseño de los protocolos. Incorporar estándares existentes y comprobados en el diseño de sistemas y productos puede implicar un riesgo técnico menor que desarrollar y utilizar protocolos propietarios. El uso de estándares genéricos, abiertos y ampliamente disponibles (como la familia de protocolos de Internet) como componentes de los dispositivos y servicios puede aportar otros beneficios, como el acceso a una mayor cantidad de talento técnico y software, que implican una reducción en los costos de desarrollo. Estos factores se discuten en la RFC 7452, "Architectural Considerations in Smart Object Networking"[125].

El impacto de la falta de estándares y mejores prácticas va más allá de la limitación del potencial de los dispositivos de Internet of Things. De una manera pasiva, la ausencia de estas normas puede permitir el mal comportamiento de los dispositivos. En otras palabras, sin estándares que sirvan de guía para los fabricantes, quienes desarrollan estos dispositivos suelen diseñar productos cuyo funcionamiento perjudica a Internet sin prestar demasiada atención al impacto que pueden llegar a

[123] Architectural Considerations in Smart Object Networking". Hannes Tschofenig. https://tools.ietf.org/html/rfc7452
[124] Ibid.
[125] Ibid.

tener. Estos dispositivos son más dañinos que aquellos que simplemente no son interoperables. Si están mal diseñados y configurados, pueden afectar incluso a la propia Internet.[126]

En un artículo, Geoff Huston, especialista en Internet, describe la proliferación de este tipo de dispositivos como la "Internet de las cosas estúpidas"[127]. Huston describe el ejemplo de un módem Netgear que venía configurado con una dirección IP fija de la universidad de Wisconsin. Tal como lo explica en el artículo, "Cuantas más unidades se vendían, mayor era el volumen total de tráfico que se enviaba al servidor de la universidad." Estos dispositivos no solo se comportaban indebidamente (canalizaban todas las solicitudes a un único servidor), sino que el mal diseño del proveedor agravó la situación por no haber provisto un mecanismo de actualización eficaz para solucionar el problema.

Con el tiempo, la implementación de estándares y mejores prácticas para la Internet de las Cosas ofrece la oportunidad de disminuir significativamente estos problemas.

En base a lo expuesto previamente, se puede llegar a la conclusión de que la estandarización de la interoperabilidad representa un desafío para los nuevos dispositivos de Internet of Things que deben interactuar con los sistemas que ya están productivos y en funcionamiento. Esto es relevante para muchos entornos específicos de ciertas industrias y aplicaciones que ya cuentan con redes de dispositivos establecidas. Los fabricantes e ingenieros que trabajan en Internet of Things deben llegar a un compromiso entre un diseño que mantenga la compatibilidad con los sistemas heredados y su intención de lograr una mayor interoperabilidad con otros dispositivos mediante la utilización de estándares.

Los usuarios deberán enfrentar cada vez más desafíos a medida que la cantidad de dispositivos que deban manejar aumente. Uno de estos desafíos es la necesidad de modificar rápida y fácilmente la configuración de múltiples dispositivos en una red. A la hora de enfrentar la configuración de cientos de dispositivos individuales, será fundamental que las herramientas, métodos e interfaces a utilizar hayan sido cuidadosamente diseñadas y estandarizadas.

Además de los tradicionales organismos de normalización, han surgido múltiples coaliciones de la industria cuyo objetivo es ayudar a evaluar, desarrollar, modificar o armonizar los estándares y los protocolos relacionados con IoT. Esto incluye, por ejemplo, organismos de normalización de larga data como el IETF[128], la ITU[129] y el IEEE[130], además de iniciativas comparativamente nuevas como el

[126] Ibid.
[127] "The Internet of Stupid Things". Geoff Huston. https://labs.apnic.net/?p=620
[128] IETF. https://www.ietf.org/about/mission/
[129] ITU. https://www.itu.int/es/about/Pages/default.aspx

Industrial Internet Consortium[131], el Open Interconnection Consortium[132] y ZigBee Alliance[133], entre muchas otras.

Es probable que la industria y las demás partes interesadas deban invertir mucho tiempo y recursos para participar en esta amplia gama de esfuerzos de normalización. Además, es probable que se produzcan solapamientos e incluso conflictos entre algunas de estas iniciativas[134]. Además de aumentar los costos de desarrollo de los estándares, la falta de coordinación entre los diferentes esfuerzos de normalización podría producir protocolos incompatibles, demorar el desarrollo de los productos y generar fragmentación entre los diferentes dispositivos, servicios y mercados verticales de la industria de Internet of Things.

[130] IEEE. https://www.ieee.org/about/vision-mission.html
[131] Industrial Internet Consortium. http://www.iiconsortium.org/about-us.htm
[132] Open Interconnection Consortium. https://openconnectivity.org/
[133] ZigBee Alliance. http://www.zigbee.org/zigbeealliance/developing-standards/
[134] "Why Internet of Things 'standards' got more confusing". Stephen Lawson. https://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

Derechos y cuestiones legales

La utilización de dispositivos de Internet of Things plantea una variedad de desafíos y preguntas sobre aspectos regulatorios y legales que deben ser considerados cuidadosamente. En algunos casos, los dispositivos de Internet of Things dan lugar a nuevas situaciones legales y regulatorias, generando preocupaciones con respecto a los derechos civiles que antes no existían. En otros casos, estos dispositivos magnifican cuestiones legales que ya existían[135]. Además, la tecnología está avanzando a una velocidad mucho mayor que la legislación relacionada a estos temas[136]. A continuación, se mencionan algunos potenciales problemas regulatorios y legales que afectan a todo el espectro de aplicaciones de la IoT.

Protección de datos

No se puede evitar que los datos que procesan los dispositivos de Internet of Things se envíen a través de los límites jurisdiccionales. Estos dispositivos utilizan Internet para comunicarse e Internet atraviesa fronteras físicas y virtuales. Los dispositivos de Internet of Things pueden procesar información sobre las personas en una jurisdicción y transmitirlos a otra para su almacenamiento o procesamiento, muchas veces sin mayores obstáculos técnicos[137]. Esto puede convertirse rápidamente en un problema legal, por ejemplo, si los datos recogidos se consideran datos personales o datos sensibles y están sujetos a las leyes de protección de datos de múltiples jurisdicciones. Para complicar aún más las cosas, las leyes de protección de datos en la jurisdicción donde residen el dispositivo y el titular de los datos podría ser inconsistente o incompatible con las leyes de la jurisdicción donde los datos se almacenan y procesan[138].

[135] "Recent IoT Device Cases". Clifford J. Zatz, Joe Meadows, Laura Aradi and Paul Mathis.
https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/
[136] "Laws and Ethics Can't Keep Pace with Technology". Vivek Wadhwa.
https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/
[137] "Take a tour of Google's secretive data centers where all your photos and emails are stored". Eugene Kim.
http://www.businessinsider.com/google-data-centers-store-all-your-photos-and-emails-2015-6
[138] "Data Protection Law and International Jurisdiction on the Internet
(Part 2)". Christopher Kuner.
https://poseidon01.ssrn.com/delivery.php?ID=278100090106071002110088030110091076096012041014091091022030017078001125122088091064039025063115053046114003078088105113113083122074062093047126015000075094118077096070059039067087118074119115072071010065099125000100030031097124105092107014099116100017&EXT=pdf

Estas situaciones se describen como flujos de datos transfronterizos y plantean preguntas con respecto al alcance jurídico de las normas que podrían ser aplicables. En otras palabras, ¿Qué régimen legal regula el dispositivo que recoge los datos y cuál regula el almacenamiento y el uso de los datos recogidos? Este escenario también plantea preguntas normativas. ¿Se pueden modificar estas leyes para reducir el grado de fragmentación de Internet que provocan y, a la vez, proteger los derechos de los usuarios? Si una jurisdicción tiene leyes de protección de datos más restrictivas en cuanto al manejo y la transmisión de determinados datos provenientes de la IoT, ¿estos requisitos legales se deberían poder proyectar a otras jurisdicciones?[139]

Si bien muchas de estas preguntas sobre los flujos de datos transfronterizos ya se han planteado y abordado en el marco del tráfico de datos de la Internet tradicional, los dispositivos de la IoT plantean un nuevo desafío en este sentido. Cada vez más, estos dispositivos podrán conectarse automáticamente a otros dispositivos y sistemas y transmitir información a través de las fronteras sin el conocimiento del usuario. Estos son temas complejos y lo serán cada vez más, ya que la tecnología sigue avanzando más rápido que la legislación.

Los datos recogidos por los dispositivos de Internet of Things permiten formar una imagen detallada de las personas con que interactúan y estos datos pueden ser utilizados tanto para fines beneficiosos como para fines discriminatorios. Consideremos el caso de los dispositivos que se utilizan para llevar registro de la actividad física. Muchas veces una persona lleva uno de estos dispositivos de forma permanente durante un período de días o semanas; durante todo este tiempo, el dispositivo recoge información muy detallada sobre los movimientos de la persona y otros datos biométricos. Una aplicación analiza estos datos para determinar el estado físico de la persona, estimar las calorías que quema, llevar un registro de las horas de sueño y caracterizar la calidad del sueño. Este análisis es claramente beneficioso para el usuario, ya que le ofrece una manera de cuantificar su actividad física mientras intenta alcanzar un objetivo de pérdida de peso o aptitud física.

Pero estos mismos datos se pueden utilizar en formas potencialmente discriminatorias. En Estados Unidos, algunos planes de seguro médico están incentivando a los participantes para que permitan que el asegurador acceda a los datos del dispositivo a cambio de primas de seguro más bajas[140]. Esta práctica puede ser vista como positiva: ofrecer precios preferenciales a quienes estén dispuestos a entregar sus datos biométricos a cambio de un descuento. Por otra parte, potencialmente podría ser discriminatoria, en especial las personas mas pobres ya que debido a su situación económica sus

[139] Ibid.
[140] "Big Doctor Is Watching". Hamza Shaban. http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html

hábitos alimenticios no son los más saludables. También puede ser aplicable para personas con problemas de sobrepeso.

Los escenarios como este son cada vez más frecuentes. Los vehículos más nuevos están equipados con GPS y enlaces de datos que comunican información de geolocalización y hábitos de conducción (por ejemplo, excesos de velocidad y características del frenado) a sistemas remotos, o que se utilizan para proporcionar asistencia o servicios de viaje al conductor[141]. Si bien estas características le proporcionan ventajas al usuario, los datos podrían llegar a ser utilizados en formas potencialmente discriminatorias. Por ejemplo, los operadores de flotas pueden utilizar estos datos para monitorear el desempeño de sus conductores sin que estos puedan optar por no ser observados. Otro caso similar de este tipo de comportamiento se puede observar en Estados Unidos, donde conductores de camiones se ven obligados a instalar dispositivos IoT para monitorear el comportamiento del vehículo. Si se niegan a esto, la compañía aseguradora puede elegir no renovarles la póliza con la que tienen asegurado el vehículo[142]. Estos son ejemplos bastante concretos de cómo se pueden utilizar los datos de Internet of Things de forma discriminatoria, aunque todavía quedan por describir un sin fin de combinaciones similares para discriminar en el futuro.

Además, la calidad, la particularidad y el volumen de los datos producidos por Internet of Things podría magnificar el potencial de que se generen prácticas de precios discriminatorias y servicios ilegítimos. Con frecuencia los datos de IoT se pueden etiquetar con metadatos (marcas de fecha y de tiempo, etiquetas de geolocalización) que aumentan drásticamente la calidad de los datos desde el punto de vista de su análisis[143]. También, los sensores de IoT suelen realizar muy pocas funciones. Esto significa que los datos de los sensores suelen asociarse con una situación operativa específica, que permite un alto grado de especificidad a la hora de correlacionar los datos con una persona o con un grupo de personas. De hecho, el dispositivo se podría llegar a asociar con la persona en la que está implantado, como en el caso de un marcapasos o una bomba de insulina conectados a Internet. En otros casos, este nivel de especificidad no es deseable y accidentalmente puede provocar resultados discriminatorios. Los sensores de la IoT pertenecientes o gestionados por terceros pueden recoger

[141] "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles". Andrew Meola. http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10
[142] "America's Truckers Embrace Big Brother After Costing Insurers Millions". Leslie Scism. https://www.wsj.com/articles/americas-truckers-embrace-big-brother-after-costing-insurers-millions-1496577601
[143] "Personalization Comes to Retail with Big Data, IoT and Augmented Reality". Michael Wu. https://www.cmswire.com/digital-experience/personalization-comes-to-retail-with-big-data-iot-and-augmented-reality/

datos identificables sobre las personas sin su conocimiento o consentimiento. Estos datos se podrían utilizar de formas que perjudicarían a la persona monitoreada.[144]

Por último, estos dispositivos crean importantes flujos de datos continuos sin intervención humana. La combinación de estas cualidades hace que los análisis de los datos de Internet of Things sean muy descriptivos y útiles para la investigación, el desarrollo de productos y también en otras áreas. Los algoritmos de Big Data pueden examinar cantidades enormes de datos y buscar correlaciones estadísticas y semánticas para así determinar grupos de usuarios con características afines. A su vez, estos algoritmos podrían categorizar injustamente a los usuarios y explotar sus características.[145]

Este tipo de usos de los datos de Internet of Things plantea cuestiones prácticas, legales y reglamentarias. En primer lugar, ¿Cómo podemos detectar las prácticas discriminatorias o injustas contra los usuarios? ¿Existen prácticas discriminatorias
virtualmente imposibles de detectar? ¿Existe alguna diferencia legal en caso que la decisión de discriminar sea tomada por una persona o por una máquina? El desarrollo de herramientas para detectar prácticas algorítmicas injustas es un desafío para la investigación académica, sobre todo porque la mayoría de los algoritmos de análisis de datos son secretos empresariales y no son del dominio público. ¿Cómo podemos equilibrar los enormes beneficios comerciales y sociales del análisis de datos de la IoT con la probabilidad de que se generen prácticas discriminatorias contra los usuarios? ¿Cómo podemos fomentar la adopción de los principios de la innovación sin pedir permiso (permissionless innovation[146]) en el ámbito de Internet of Things y a la vez proteger a los usuarios contra las prácticas ilegítimas? ¿Cómo podemos mejorar la transparencia? ¿Las leyes de privacidad y de protección del consumidor existentes alcanzan para hacer frente a este escenario? ¿Qué recursos deberían estar disponibles en caso de discriminación? ¿Los dispositivos de la IoT se deberían categorizar y regular en función de la naturaleza de los datos que producen, especialmente cuando los datos son propensos a ser mal utilizados?

[144] Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age. Charlotte A Tschider http://www.academia.edu/36014158/Regulating_the_IoT_Discrimination_Privacy_and_Cybersecurity_in_the_Artificial_Intelligence_Age

[145] "Big Data on Internet of Things: Applications, Architecture, Technologies, Techniques, and Future Directions". Heba Aly, Mohammed Elmogy, Shereif Barakat. http://www.ijcse.net/docs/IJCSE15-04-06-040.pdf

[146] "What is Permissionless Innovation?". http://permissionlessinnovation.org/what-is-permissionless-innovation/

Utilización de dispositivos para aplicación de la ley y la seguridad pública.

Los dispositivos de Internet of Things podrían servir como ayuda para las instituciones legales y la seguridad pública, pero en este caso es necesario considerar cuidadosamente las ramificaciones legales y sociales. Sin lugar a dudas, los dispositivos de Internet of Things y los datos que generan pueden ser utilizados como herramientas eficaces para luchar contra el delito. Muchos pequeños negocios han instalado cámaras de seguridad para grabar video y realizar un seguimiento de la actividad de los clientes, algo que ha resultado de gran valor como prueba en los procesos penales y como elemento de disuasión de la delincuencia[147]. Más recientemente, On-Star Corporation, una subsidiaria de General Motors, puede proporcionar datos de los sensores que se encuentran en automóviles que fueron identificados como robados a la policía, facilitando la tarea de recuperación de estos vehículos. También puede desactivar de forma remota un vehículo robado[148]. El Departamento de Policía del Condado de Nassau (Nueva York) utiliza una red de sensores de sonido llamada ShotSpotter que permite detectar y localizar la fuente exacta de un disparo en los barrios donde han sido realizados[149]. Todos estos son ejemplos de los beneficios que la tecnología de la Internet de las Cosas puede ofrecer a la policía para combatir la delincuencia y mejorar la seguridad pública.

Sin embargo, el desarrollo y uso de este tipo de tecnologías provocan preocupación entre algunos defensores de los derechos civiles y otras personas. Entre las posibles causas de preocupación se incluyen la omnipresencia de las actividades de monitoreo de los datos, las políticas sobre su conservación y destrucción, los usos secundarios que los gobiernos pueden darles, así como la potencial exposición accidental de los datos a actores maliciosos. Además, se deben considerar cuidadosamente los efectos potencialmente negativos sobre las actividades beneficiosas de las comunidades y sociedades monitoreadas[150].

Otras situaciones relacionadas a la seguridad pública pueden resultar más complejas. Por ejemplo, al lanzar el iPhone 6 y su sistema operativo iOS 8, Apple eliminó un método de acceso tipo “backdoor” que existía en versiones anteriores de su teléfono. La función de "backdoor" permitía a la policía acceder a los datos que se encontraban en el teléfono de un usuario. Apple eliminó esta característica

[147] "5 Ways Tech Is Stopping Theft". Jennifer Goforth Gregory. https://www.entrepreneur.com/article/229674
[148] "Lawyers reaching for in-car data". Vince Bond Jr. http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data
[149] "Cool cop tech: 5 new technologies helping police fight crime". Todd Weiss. https://www.computerworld.com/article/2501178/government-it/cool-cop-tech--5-new-technologies-helping-police-fight-crime.html?page=2
[150] "Secure all the things! How to protect human rights on the Internet of Things". Lucie Krahulcova. https://www.accessnow.org/secure-things-protect-human-rights-internet-things/

en el nuevo iPhone y ahora encripta el contenido interno del teléfono de una manera difícil de vulnerar y para la cual Apple no tiene las claves, por lo cual no tiene forma de permitir el acceso[151]. Esto hace que solo el propietario del teléfono pueda acceder a su contenido. Las agencias federales de seguridad sostienen que esto hace que sea más difícil procesar los comportamientos criminales, mientras que los partidarios de los derechos civiles ven en esto una victoria para la protección de la privacidad de los datos de los usuarios[152]. Esta controversia con respecto al cifrado de los dispositivos también se aplica a otros dispositivos de Internet of Things. ¿Qué papel debe desempeñar el cifrado de los dispositivos en la protección de los dispositivos de IoT contra los ataques criminales? ¿Cómo se puede equilibrar esto con el legítimo acceso a los datos del usuario en interés de la aplicación de la ley y la seguridad pública?

Los dispositivos de Internet of Things plantean dudas y preguntas con respecto a la responsabilidad desde el punto legal que invitan a la reflexión. Una de las preguntas fundamentales en lo que respecta a los dispositivos de IoT es la siguiente: Si alguien se ve perjudicado como consecuencia de la acción u omisión de un dispositivo de la IoT, ¿quién es el responsable? En muchos casos la respuesta es compleja y todavía no existe demasiada jurisprudencia para sustentar una posición determinada. Los dispositivos de IoT funcionan de forma más compleja que un producto independiente y esto sugiere que será necesario considerar escenarios de responsabilidad más complejos[153].

Ejemplos:

- Puede que los dispositivos de IoT sean utilizados en formas nunca previstas por su fabricante. No es razonable suponer que un fabricante de dispositivos pueda realizar pruebas de control de calidad para todos los potenciales casos de uso de los dispositivos de IoT[154].

- Quizás los dispositivos de IoT se conecten e interactúen con otros de formas no anticipadas y para las cuales no se realizaron pruebas. A medida que aumente la interoperabilidad, estos dispositivos podrán formar entre sí conexiones de red automáticamente. Por lo tanto, antes de

[151] "Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe?". Trevor Timm. https://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default
[152]"Apple will no longer unlock most iPhones, iPads for police, even with search warrants". Craig Timberg. https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.5f654a66048a
[153] "Who Is Responsible for IoT Security?". Rick M Robinson. https://securityintelligence.com/who-is-responsible-for-iot-security/
[154] "Hacker Exploits a Baby Monitor to Spy on and Insult a Toddler". Fox Van Allen. https://www.techlicious.com/blog/hacker-exploits-a-baby-monitor-to-spy-on-and-insult-a-toddler/

desplegar estos dispositivos, es difícil para un fabricante o usuario tener en cuenta todos los escenarios potencialmente perjudiciales que podrían llegar a surgir en el futuro[155].

- Una vez instalados, estos dispositivos pueden tener una larga vida útil y serán susceptibles a futuras amenazas a la seguridad que hoy en día son desconocidas. Esto significa que estos dispositivos podrían verse comprometidos y ser reprogramados maliciosamente para dañarse a sí mismos o a otros dispositivos, o bien para revelar información sensible en forma no intencionada e inadvertida[156].

- Los dispositivos de Internet of Things se integrarán en sistemas autónomos (por ejemplo, automóviles sin conductor) que incorporan algoritmos de aprendizaje adaptativo para controlar su comportamiento sobre la información aportada por los sensores de tales dispositivos. Si bien estos sistemas son probados antes de disponibilizarlos, es imposible asegurar que no vaya a ocurrir un accidente por el momento[157].

Estos y otros escenarios plantean interrogantes. Si uno de uno de estos escenarios genera daños, ¿las leyes de responsabilidad existentes abordan adecuadamente la culpabilidad legal y aclaran la responsabilidad de las partes involucradas? ¿Es necesario repensar las leyes de responsabilidad para los dispositivos inteligentes de IoT que aprenden de su entorno y se modifican a sí mismos a medida que pasa el tiempo? Si un sistema autónomo recibe instrucciones del usuario y no de sus algoritmos internos, ¿qué pasa en caso de error del usuario? ¿En qué medida se pueden ampliar las leyes de responsabilidad que existen para los productos convencionales de manera que abarquen los productos que se van conectando a Internet? Como comunidad, ¿qué podemos hacer para informar mejor a los legisladores y a los formuladores de políticas de modo que no sean tan susceptibles frente a la enorme cantidad de información errónea y consejos sesgados que reciben? ¿Qué podemos hacer para informar mejor a los usuarios y compradores de estos dispositivos de modo que entiendan todos los factores que afectan su uso?

[155] "Hackers hijack Philips Hue lights with a drone". Timothy J. Seppala. https://www.engadget.com/2016/11/03/hackers-hijack-a-philips-hue-lights-with-a-drone/
[156] "IoT attacks are getting worse -- and no one's listening". Alfred Ng. https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/
[157] "Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian". Sam Levin, Julia Carrie Wong. https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe

Dispositivos IoT utilizados en acciones legales

Los datos que recogen los dispositivos de Internet of Things muchas veces pueden servir como evidencia en una variedad de procedimientos legales. A medida que estos datos se vuelvan más frecuentes, es probable que se utilicen cada vez más en este tipo de procedimientos. Por ejemplo, algunos abogados en Estados Unidos han utilizado durante un juicio de divorcio los datos de hora y localización obtenidos de los dispositivos de peaje electrónico instalados en los automóviles para demostrar una infelidad en la pareja[158]. En 2014, una mujer canadiense utilizó los datos de su propio dispositivo de actividad física como evidencia de su reclamo en una demanda por lesiones[159].

En los automóviles se pueden instalar dispositivos conectados a Internet de manera que actúen como garantía en caso de incumplimiento de las obligaciones de pago. Si un conductor no paga el leasing o el crédito de su automóvil, el arrendatario o prestamista puede inactivar el vehículo de forma remota usando el dispositivo instalado hasta que se realice el pago[160]. Estos dispositivos ya se han instalado en más de dos millones de automóviles en Estados Unidos[161].

Este tipo de escenarios plantean nuevas preguntas legales y reglamentarias con respecto a los dispositivos de IoT. ¿Deberían los fabricantes de dispositivos incluir en estos dispositivos tecnologías como el cifrado para restringir el acceso a los flujos de datos como lo ha hecho Apple en el iPhone? A la inversa, ¿deberían los fabricantes estar diseñando dispositivos de IoT que faciliten el uso de los datos en un procedimiento judicial? ¿Es necesario desarrollar estándares que especifiquen requisitos de diseño para que los datos de la IoT soporten la cadena de custodia de los datos en los procesos judiciales? ¿Se deberían establecer regulaciones que protejan al consumidor de ciertos dispositivos de IoT?

La diversidad de temas legales, reglamentarios y de derechos relacionados con Internet of Things es amplia y variada. Los dispositivos de IoT crean nuevos desafíos legales y de políticas que no existían anteriormente y que amplifican muchos de los desafíos ya existentes. Por otra parte, la enorme

---

[158] "E-ZPass records out cheaters divorce court". Chris Newmarker. http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/%20-%20.Vbp9KnjfbFI#.We0FsRNSxTY

[159] "Fitbit data is now being used in COURT: Wearable technology is set to revolutionise personal injury and accident claims". Sarah Griffiths. http://www.dailymail.co.uk/sciencetech/article-2838025/Fitbit-data-used-COURT-Wearable-technology-set-revolutionise-personal-injury-claims.html

[160] "Why the repo man can remotely shut off your car engine". Aimee Picchi. https://www.cbsnews.com/news/why-the-repo-man-can-remotely-shut-off-your-car-engine/

[161] "Miss a Payment? Good Luck Moving That Car". Michael Corkery and Jessica Silver-Greenberg. https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/

cantidad de dispositivos inalámbricos de IoT y el ruido de radiofrecuencia (RF) y las interferencias que producen son ejemplos de cómo los dispositivos de IoT amplifican la dificultad que existe para regular el uso del espectro de RF[162]. Otros desafíos emergentes para los dispositivos de IoT son las preocupaciones legales y reglamentarias con respecto a la propiedad intelectual, las cuestiones ambientales (por ejemplo, cómo desechar los dispositivos) y la propiedad legal de dispositivos (por ejemplo, ¿los dispositivos serán propiedad del usuario o serán alquilados?).

A las complejidades de decidir las estrategias apropiadas de regulación o de políticas para los problemas de Internet of Things se suma el problema de decidir qué lugar de la arquitectura de un sistema de IoT es el mejor para conseguir los resultados deseados. ¿Dónde se deben colocar los controles regulatorios? ¿En el dispositivo, en el flujo de datos, en la puerta de enlace, en el usuario o en la nube donde se almacenan los datos? Las respuestas a estas y otras preguntas dependen de la perspectiva desde la cual se analice la situación. Cada vez más, los análisis regulatorios de los dispositivos de la IoT se realizan desde una perspectiva legal general y tecnológicamente neutra, como por ejemplo las leyes y reglamentos de protección al consumidor[163]. Entre otras cosas, evaluar las implicancias legales de los dispositivos de IoT desde la perspectiva de la prevención de prácticas desleales o engañosas contra los consumidores puede ayudar a informar las decisiones sobre privacidad y seguridad.

[162] "Electronic Noise Is Drowning Out the Internet of Things". Mark A. McHenry, Dennis Roberson and Robert J.Matheson. https://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things
[163] "Policy Paper on IoT Future Technologies". Maarten Botterman. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf

Economía y desarrollo social

La expansión y el impacto de Internet tienen un alcance global: ofrecen oportunidades y beneficios a las regiones desarrolladas y las regiones en desarrollo por igual. Al mismo tiempo, muchas veces en las regiones en desarrollo se plantean desafíos únicos relacionados con el desarrollo, el crecimiento, la implementación y el uso de la tecnología, incluso de Internet[164]. Es razonable esperar que esto también sea aplicable para los potenciales beneficios y desafíos asociados con Internet of Things. Desde la perspectiva de los principios de la Internet Society[165], se piensa que Internet debe ser una fuente de empoderamiento a nivel global, sin importar la ubicación, la región o el estado de desarrollo económico del usuario, y que toda la gama de habilidades y principios que impulsan nuestro trabajo y el éxito de Internet se aplican a nivel global. Desde los comienzos de Internet, la comunidad técnica, la sociedad civil, las organizaciones gubernamentales y la industria privada, entre otros actores, se han centrado en las oportunidades y los desafíos relacionados con Internet en las economías emergentes. De modo que esto también debería aplicar a las oportunidades y desafíos relacionados con Internet of Things.

Oportunidades económicas y de desarrollo

Con respecto a las oportunidades, el McKinsey Global Institute señala que la industria de Internet of Things tiene gran potencial en las economías en desarrollo. Se proyecta que en 2025 hasta un 38% del impacto económico anual de las aplicaciones de IoT provendrá de las regiones menos desarrolladas[166]. Desde una perspectiva económica, se anticipa que las tendencias tanto demográficas como de mercado impulsarán las oportunidades. Por ejemplo, los países en desarrollo tienen un elevado número de potenciales usuarios de IoT (especialmente China[167]), el crecimiento económico mundial se está desplazando hacia las economías en desarrollo y se espera que las aplicaciones industriales de IoT (por ejemplo, en las fábricas, los lugares de trabajo y el transporte) impulsarán la creación de valor económico.

[164] "Developing Countries Will Drive The Growth Of The Internet Of Things". David Bolton. https://www.applause.com/blog/internet-of-things-growth-developing-countries/
[165] "Internet Society - Principles". Internet Society. https://isoc-ny.org/misc/isoc-ny_side2.pdf
[166] "Unlocking the potential of the Internet of Things". James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
[167] "Internet of Things sees explosive growth in China". Li Yan. http://en.people.cn/n3/2017/0914/c90000-9269103.html

Si se concretan las expectativas con respecto a la innovación y la aplicación de la tecnología, las implementaciones de Internet of Things podrían tener un papel muy importante como facilitadoras del desarrollo social, incluyendo el logro de los Objetivos de las Naciones Unidas para el Desarrollo Sostenible[168]. Los Objetivos de la ONU para el Desarrollo Sostenible son un conjunto de diecisiete objetivos que abarcan más de cien metas y que apuntan a guiar los esfuerzos para lograr dignidad, bienestar e igualdad para todas las personas del mundo. Abarcan una amplia gama de desafíos de desarrollo fundamentales, entre ellos la agricultura sostenible, la energía, la disponibilidad de agua, la industrialización y la gestión de los recursos terrestres y marítimos.

Al considerar el potencial de que la tecnología de los dispositivos inteligentes e Internet of Things aborde los desafíos del desarrollo de manera significativa, las oportunidades parecen ser prometedoras. Por ejemplo, la aplicación de redes de sensores a diferentes desafíos ambientales como la calidad y el uso del agua, el saneamiento, la salud y las enfermedades, el cambio climático y el monitoreo de los recursos naturales podría tener un fuerte impacto más allá de la gestión de los recursos. Los datos obtenidos de este tipo de aplicaciones también se podrían utilizar en contextos de investigación y ayudar a los científicos y a las universidades a realizar contribuciones únicas al cuerpo de conocimiento científico global[169].

La creciente población mundial[170] nos dice que los desafíos relacionados con el acceso a alimentos de calidad, servicios y salud aumentarán con el tiempo. El potencial uso de Internet of Things para combatir el hambre y promover una agricultura sostenible ha recibido especial atención, quizás más que cualquier otro problema relacionado con el desarrollo[171]. Desde la gestión de los ciclos de producción agrícola, las amenazas de enfermedades y el aumento de las materias primas gracias a la automatización de las cosechas, la logística aplicada a la distribución y el control de la calidad, se anticipa que las técnicas de "agricultura inteligente" basadas en IoT se incorporarán a toda la cadena de valor para mejorar la sostenibilidad y la productividad de la oferta de alimentos. [172], [173]

[168] "Sustainable Development Topics". ONU. https://sustainabledevelopment.un.org/topics
[169] "Water quality monitoring and waste management using IoT". M. V. Ramesh. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8239311&isnumber=8239217
[170] "World Population Growth". Max Roser, Esteban Ortiz-Ospina. https://ourworldindata.org/world-population-growth
[171] "Internet of food". http://internet-of-food.org/
[172] "Policy Paper on IoT Future Technologies". Maarten Botterman. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf
[173] "Digital farm set for internet's next wave". The Guardian. https://www.theguardian.com/connecting-the-future/2015/sep/21/digital-farm-set-for-internets-next-wave

Casos de exito

Amazon Echo y Alexa

Los asistentes de voz llevan un tiempo en el mercado tratando de conquistar nuestra forma de utilizar nuestros dispositivos inteligentes. Esto implica nuevas formas de interactuar con los dispositivos, ya que hace que "toquemos" menos y hablemos más. Amazon Echo fue sacado al mercado en 2014, básicamente como un reproductor de música que podía ser controlado por voz y algunas funciones más, como hacerle preguntas sobre cuál es la capital de determinado país o cuando nació un actor famoso[174].

Hoy en día es capaz de controlar más de doce mil dispositivos relacionados a casas inteligentes[175]:

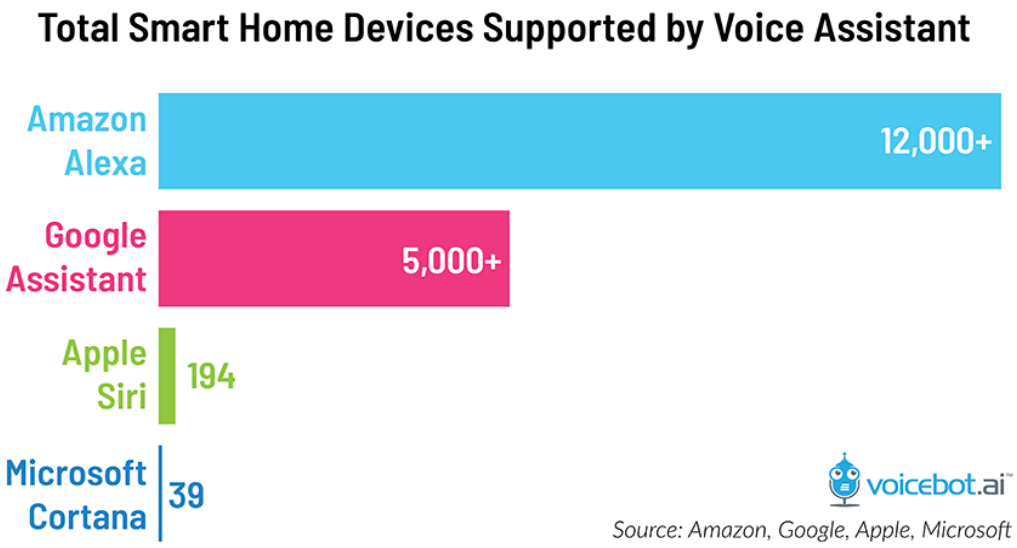

Ilustración 12 - Cantidad de dispositivos Smart Home discriminados por asistente de voz[176].

El Echo utiliza el asistente de voz Alexa, similar a los que utilizan Microsoft y Apple, con Cortana y Siri respectivamente. Hoy en día, es el asistente más utilizado del mercado norteamericano[177]:

[174] "How Amazon's Echo went from a smart speaker to the center of your home". Matt Weinberger. http://www.businessinsider.com/amazon-echo-and-alexa-history-from-speaker-to-smart-home-hub-2017-5
[175] "Alexa and Google Assistant Battle for Smart Home Leadership, Apple and Cortana Barely Register". Bret Kinsella. https://www.voicebot.ai/2018/05/07/alexa-and-google-assistant-battle-for-smart-home-leadership-apple-and-cortana-barely-register/
[176] Ibid.

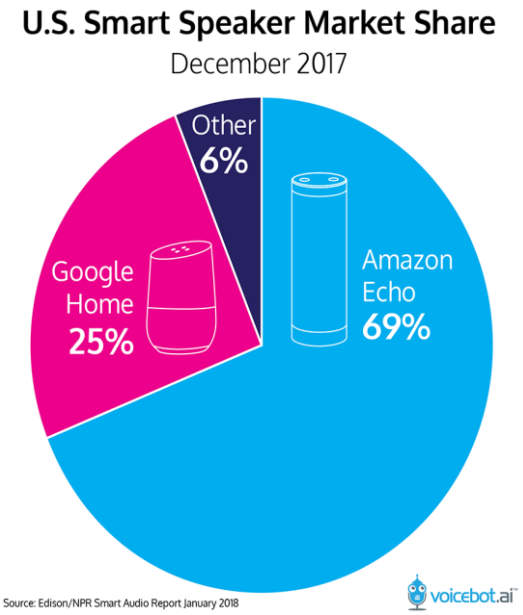

Ilustración 13 - División de mercado de asistentes de voz en Estados Unidos[178]

Si bien el dispositivo Google Home estuvo ganando una parte de mercado en los últimos meses, todavía la posición del dispositivo de Amazon es dominante.

Para entender cómo se llegó a esto, hay que tener en cuenta varios factores. El éxito del Echo no está relacionado al hardware, sino al software dentro de él. Una de las primeras decisiones que tomo la compañía fue crear un marco de trabajo que permitía exprimir la originalidad y el potencial de la plataforma. Amazon fue abriendo su plataforma, disponibilizando una serie de APIs y herramientas para facilitar a terceros poder desarrollar aplicaciones y dispositivos que interactuaran con el Echo.

No solo eso, sino que también que crearon un fondo de cien millones de dólares para invertir en el apoyo de desarrolladores y startups que crearán nuevas experiencias diseñadas en torno a la voz humana[179].

[177] "Amazon Alexa Smart Speaker Market Share Dips Below 70% In U.S., Google Rises to 25%". Brett Kinsella. https://www.voicebot.ai/2018/01/10/amazon-alexa-smart-speaker-market-share-dips-70-u-s-google-rises-25/
[178] Ibid.
[179] "Amazon Introduces the Alexa Fund: $100 Million in Investments to Fuel Voice Technology Innovation". Amazon. http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=2062558

Esto hizo que le sacara una gran ventaja a dispositivos como el HomePod, de Apple. El HomePod es un buen ejemplo del término antes mencionado "Jardín Vallado", ya que por el momento no tiene una plataforma abierta para desarrollar aplicaciones que se conecten con este[180].

También hay casos donde fabricantes decidieron entrar al mercado de los asistentes virtuales aprovechando el éxito del dispositivo, como por ejemplo el Lenovo Smart Assistant[181]. Este dispositivo utiliza el asistente de voz Alexa y tiene las mismas funcionalidades que el Echo; la única diferencia radica en el hardware, que es propiedad de Lenovo.

Los próximos pasos del dispositivo incluyen mejorar la interacción con los seres humanos a través de inteligencia artificial. Cada vez que interactuamos con el dispositivo, las grabaciones son utilizadas para mejorar la comprensión del lenguaje natural de Alexa y la capacidad de reconocer la voz. Por ejemplo, la compañía Affectiva es capaz de detectar estados de ánimo en las personas, como felicidad, enojo y excitación desde el sonido que produce la voz de una persona. Según su fundadora, el seguimiento de los estados de ánimos de los usuarios va a cambiar la manera en que los robots y los asistentes de inteligencia artificial como Alexa, interactuara con los usuarios: "La inteligencia emocional es la llave para permitirle a los dispositivos con interfaz de voz reaccionar a respuestas y tener conversaciones significativas. Hoy, por ejemplo Alexa puede contarte un chiste, pero no puede reaccionar en base a la respuesta del usuario."[182]

La personalización de la inteligencia artificial es actualmente el corazón de muchos servicios tecnológicos como los listados de que nos aparecen en Airbnb o los productos que vemos ofrecidos en las publicidades de Google[183].

Desde principios del 2018, Amazon le habilitó a los desarrolladores la posibilidad de desarrollar funcionalidades que reconozcan voces[184].

[180] "APPLE HOMEPOD REVIEW: LOCKED IN". Nilay Patel.
https://www.theverge.com/2018/2/6/16976906/apple-homepod-review-smart-speaker
[181] "Alexa with better audio? CES introduces the Lenovo Smart Assistant". Dan Ackerman.
https://www.cnet.com/products/lenovo-smart-assistant-with-amazon-alexa/preview/
[182] "Affectiva CEO: AI needs emotional intelligence to facilitate human-robot interaction". Khari Johnson.
https://venturebeat.com/2017/12/09/affectiva-ceo-ai-needs-emotional-intelligence-to-facilitate-human-robot-interaction/
[183] "Amazon's Alexa wants to learn more about your feelings". Khari Johnson.
https://venturebeat.com/2017/12/22/amazons-alexa-wants-to-learn-more-about-your-feelings/
[184] "Amazon will let developers build Alexa skills that recognize unique voices in 2018". Khari Johnson.
https://venturebeat.com/2017/11/28/amazon-will-let-developers-build-alexa-skills-that-recognize-unique-voices-in-2018/

2016 fue el año más caluroso desde que se empezaron a registrar las temperaturas en 1880. Si uno ve el promedio a lo largo de los años, se puede afirmar que esta tendencia de aumento de temperatura a nivel mundial se está incrementando con el transcurso de los años[185]:

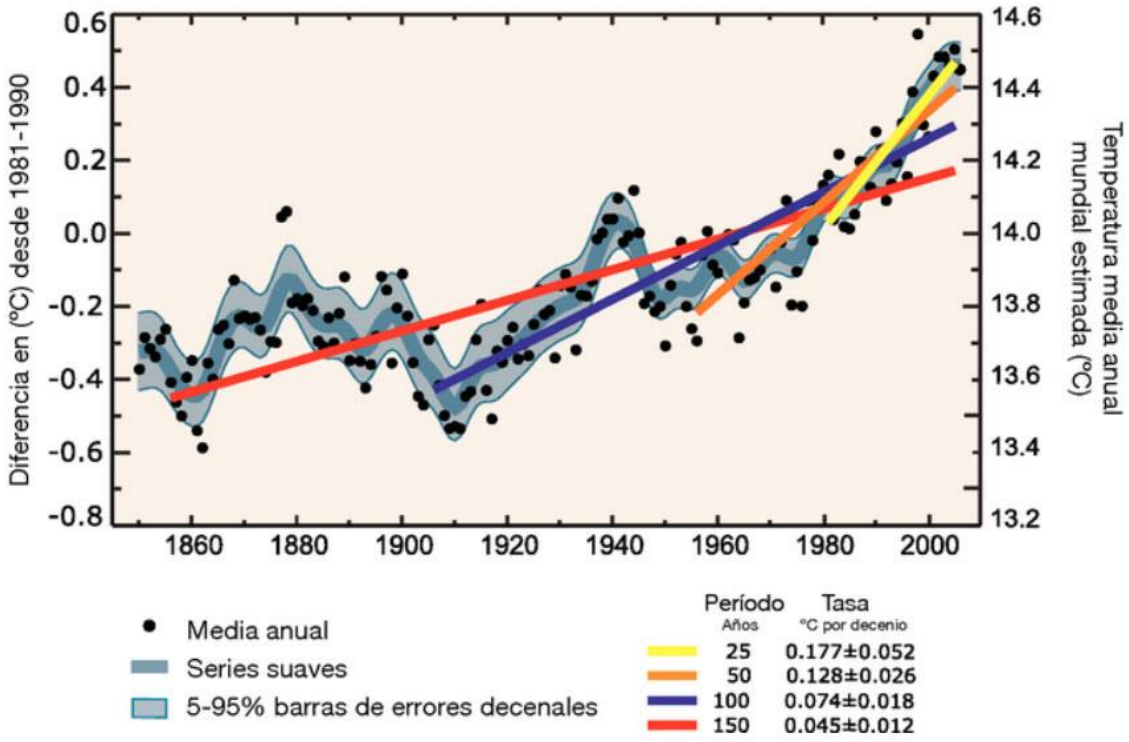

Ilustración 14 - Temperatura media anual mundial (puntos negros) con ajustes lineales de información. El eje izquierdo muestra anomalías en las temperaturas promedio en el período de 1961 a 1990 y el eje derecho muestra el cálculo de las temperaturas actuales, ambas expresadas en °C. Las tendencias lineales se muestran durante los últimos 25 años (amarillo), 50 años (anaranjado), 100 años (morado) y 150 años (rojo). La curva suave azul muestra variaciones por decenio, con un margen de error de 90% por decenio mostrado como una banda azul clara sobre esa línea. El aumento total de la temperatura desde el período de 1850 a 1899 al período de 2001 a 2005 es 0,76°C ± 0,19 °C.[186]

[185] "The 10 Hottest Global Years on Record". Climate Central.
http://www.climatecentral.org/gallery/graphics/the-10-hottest-global-years-on-record
[186] "Temperaturas promedio mundiales". Intergovernmental Panel on Climate Change.
https://www.ipcc.ch/publications_and_data/ar4/wg1/es/tssts-3-1-1.html

Con la polución como el principal sospechoso del aumento de las temperaturas[187], hay un interés creciente en automatización de edificios para que estos sean más eficientes al momento de consumos energéticos[188].

Como resultado, los edificios con consumo de energía eficiente son tendencia y se espera que que para el 2021 sea un negocio que alcance los cuarenta y cinco billones de dólares según un estudio realizado por ABI Research[189].

La automatización de edificios no es algo nuevo. El primer control automático de temperatura fue creado en 1895 por Warren Johnson, iniciando un nuevo tipo de industria dedicada a la automatización[190]. Con la creación de este dispositivo, Warren también fundó la compañía Johnson Controls.

En la actualidad, Jonhson Controls lidera la industria de edificios inteligentes y sustentables. En 2007, fue una de las cuatro compañías que logró cumplir los requisitos de eficiencia energética para edificios definidos por la iniciativa de Clinton Foundation[191].

Las grandes cantidades de datos que producen actualmente los sensores y termostatos en las fábricas o edificios dificultan las tareas que tienen que realizar los supervisores de mantenimiento. Johnson Controls busca facilitar y automatizar todas estas tareas de recolección y procesamiento de información, para poder brindarle al usuario un análisis más detallado de lo que está sucediendo, ya sea en el mismo lugar físico o en cualquier otro lugar del mundo. Según dice Jim Schwartz, director de Jonhson Controls "Nuestros clientes nos comentan que en muchos casos tienen una gran cantidad de información en vez de poca. En vez del modelo tradicional de recolectar y administrar datos manualmente, nosotros buscamos entregar herramientas que agreguen información y entreguen ideas accionables"[192].

---

[187] "Air Polution". National Geographic. https://www.nationalgeographic.com/environment/global-warming/pollution/

[188] "The rise of co-working space and the need for smart buildings". Rinse Bruggeman, Desie Driever and Wilfrid Donkers. https://www2.deloitte.com/global/en/pages/real-estate/articles/rise-co-working-space-need-smart-buildings.html

[189] "Global Commercial Building Automation Market Revenues will Reach $45 Billion by 2021". ABI Research. https://www.abiresearch.com/press/global-commercial-building-automation-market-reven/

[190] "Multi-Zone Automatic Temperature Control System". ASME. https://www.asme.org/about-asme/who-we-are/engineering-history/landmarks/244-multi-zone-automatic-temperature-control

[191] "Press Release: President Clinton Announces Landmark Program to Reduce Energy Use in Buildings Worldwide". Clinton Foundation. https://www.clintonfoundation.org/main/news-and-media/press-releases-and-statements/press-release-president-clinton-announces-landmark-program-to-reduce-energy-use.html

[192] "Connecting Buildings to the Cloud for a Greener Planet". Microsoft. https://customers.microsoft.com/en-US/story/connecting-buildings-to-the-cloud-for-a-greener-planet

Otra de las soluciones creadas por Johnson Controls es una plataforma extensible y conectada, capaz de integrarse con virtualmente con cualquier dispositivo del edificio; ya sea sensores, termostatos o sistemas de refrigeración. Por ejemplo, los sistemas de refrigeración pueden disminuir hasta un cincuenta por ciento el consumo de energía si se los utilizan y configuran correctamente[193].

Otra de las variables a tener en cuenta, es la performance de estos equipos. Los sistemas de refrigeración se encuentran entre los componentes más costosos y críticos de un edificio. Por ejemplo, un sistema de refrigeración de un hospital o laboratorio que no está funcionando correctamente puede tener impactos casi catastróficos. Administrar edificios más eficientemente es la llave para controlar los gastos del mismo, asegurando la seguridad de las personas que se encuentran en él y reduciendo el impacto que tiene en nuestro planeta[194].

Johnson Controls ya tiene más de 30 años trabajando con equipamiento y sensores de automatización de edificios, por lo que incorporar soluciones de Internet of Things no les resultó un gran desafío. Sin embargo, si necesitaban una plataforma para poder administrar los grandes flujos de información eficientemente.

La compañía tomó la decisión construir esta solución en la nube con Microsoft Azure Internet of Things Suite. Según explica Sudhi Sinha, Vicepresidente de Desarrollo de Producto; "Vimos que estábamos utilizando alrededor de siete datacenters diferentes. Cuando vimos como podíamos reducir estos costos, mejorar la performance y seguridad, e incrementar la confiabilidad de nuestra infraestructura central de datos, Azure fue la elección debido a la buena asociación e historia que tenemos con Microsoft. Elegir Azure fué una experiencia muy satisfactoria"[195].

Actualmente la compañía está recolectando más de catorce millones de registros por día, almacenando más de tres terabytes de información en Azure. Este volumen de información continua creciendo exponencialmente[196].

Por el momento, Johnson Controls tiene miles de sistemas de refrigeración y aproximadamente cuarenta mil edificios alrededor del mundo conectados a Azure. Los clientes ven los resultados en

[193] "Chiller Best Practices VSD". Johnson Controls. http://www.johnsoncontrols.com/buildings/hvac-equipment/chillers/variable-speed-drives/chiller-best-practices-vsd
[194] "Cost control strategies for zero energy buildings". National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy14osti/62752.pdf
[195] "Connecting Buildings to the Cloud for a Greener Planet". Microsoft. https://customers.microsoft.com/en-US/story/connecting-buildings-to-the-cloud-for-a-greener-planet
[196] Ibid.

reportes mensuales personalizados, alertas y análisis accesibles virtualmente desde cualquier dispositivo, incluyendo computadoras, tablets y smartphones. Pueden visualizar datos en tiempo real, como así también sugerencias para mantenimiento predictivo. En términos prácticos, esto significa que el cliente puede advertir futuros problemas y todo lo que esto implica[197].

[197] Ibid.

Conclusiones

Aunque la idea de combinar computadoras, sensores y redes para monitorear y administrar diferentes dispositivos no es nueva, la reciente confluencia de tecnologías clave y tendencias de mercado está marcando el comienzo de un nuevo paradigma. Internet of Things promete abrir la puerta a un mundo totalmente nuevo, un mundo “inteligente" completamente interconectado en el cual las relaciones entre los dispositivos, su entorno y las personas estarán completamente integrados. La visualización de Internet of Things como una matriz omnipresente de dispositivos conectados a Internet podría cambiar radicalmente la definición de lo que significa estar “online”.

Teniendo en cuenta que su su potencialidad es significativa, hay una serie de problemas que podrían surgir en el camino de esta transformación, especialmente en las áreas de la seguridad; la privacidad; la interoperabilidad y los estándares; temas legales, reglamentarios y de derechos; y económicos. Internet of Things implica un complejo conjunto de consideraciones tecnológicas, sociales y políticas en constante evolución que atraviesa un conjunto variado de actores. Internet of Things está pasando ahora mismo, por lo que es necesario hacer frente a sus desafíos, maximizar sus beneficios y simultáneamente reducir sus riesgos.

El mundo está pendiente del avance de Internet of Things, ya que su participación en la vida cotidiana aumenta constantemente. Hace ya unos años que la legislación ha sido sobrepasada exponencialmente por la cantidad de escenarios y nuevas situaciones que genera la tecnología, por lo que hoy más que nunca es necesario hacerse las preguntas correctas. Para maximizar los beneficios que ofrece esta tecnología y minimizar sus riesgos, es necesario que todas las partes interesadas se comprometan a dialogar y colaborar.

Internet of Things se encuentra en una etapa en la que diferentes redes y una multitud de sensores deben unirse e interoperar según un conjunto común de estándares. Para esto, es necesario que las empresas, los gobiernos, los organismos de normalización y las universidades trabajen en forma conjunta para conseguir un objetivo común.

Para que Internet of Things gane aceptación entre el público general, los proveedores de servicios y otros organismos deberán ofrecer aplicaciones que aporten un valor tangible a la vida de las personas. Internet of Things no debe representar el avance de la tecnología porque si; el sector tiene que demostrar que existe un valor en el plano humano.

Las tecnologías emergentes normalmente se ven limitadas por la legislación y las regulaciones vigentes, ya que al ser disruptivas suelen desafiar los límites previamente establecidos. Internet of Things no es la excepción a esa brecha legislativa que varía además de país a país y de industria a industria.

La legislación sin duda deberá tratar antes o después situaciones nuevas que aborden los desafíos que van surgiendo para la privacidad, seguridad o propiedad de los datos y la responsabilidad legal que esto conlleva. Cada tecnología del mundo IoT presenta diferentes desafíos.

La revisión legislativa necesaria puede ir desde cambios normativos hasta redactar nuevas leyes, por lo que la manera de abordar estos temas varía completamente. Volvo[198], por ejemplo, tiene una marcada tradición de usar tecnología para crear valor. Sus vehículos utilizan tecnología IoT para compartir información sobre condiciones de tráfico y de meteorología. Esto puede suponer un impacto muy relevante y positivo en las estadísticas de accidentes. La tecnología disruptiva siempre supone un desafío a la legislación vigente, ya que debe adaptarse para aclarar aspectos tales como si el usuario tiene derecho a revelar su localización o si prevalece un bien colectivo superior.

La cantidad de temas que se abren a debate no tiene fin. Debe poder denunciarte tu auto si vas a una velocidad no permitida? Pueden los fabricantes monitorear sus productos una vez vendidos para ofrecerte un mejor servicio posventa? Pueden fabricantes compartir tus datos personales para ofrecerte un mejor servicio? Puede un auto conducir por uno? Y en el caso de que haya un siniestro, quien es el responsable? Que pasa si chocan un auto manejado por un conductor humano y uno autónomo? De quién es la responsabilidad? Las preguntas que nos podemos hacer son infinitas.
Por otro lado, el éxito de IoT también depende del despliegue de estándares abiertos para todo tipo de industrias y sectores. A pesar de que se trata de un mercado con muchísimo potencial, el espacio IoT sufre actualmente de cierta fragmentación. Un sin fin de estándares bloquea la colaboración intersectorial e impide establecer un legado unificado y común. Los millones de teléfonos, computadoras, sensores y otros dispositivos conectados con los que viviremos en los próximos años deberían poder comunicarse entre sí independientemente de cual sea el fabricante, el sistema operativo o el chipset. Aunque ya hay organizaciones trabajando en el tema, todavía queda mucho camino por recorrer hacia la convergencia de protocolos y soluciones, ya que todos los años se incrementa su número.

[198] "Daimler and Volvo Take Lead in Implementation of V2V Communication Systems in Europe." Katja Feick. http://www.frost.com/prod/servlet/press-release.pag?docid=289374477

Bibliografía

- "The Diffusion of Innovation – What it is and where it began." Kevin McGourty. https://inpdcenter.com/blog/the-diffusion-of-innovation-what-it-is-and-where-it-began/
- "Intelligence without representation". Rodney A. Brooks. https://people.csail.mit.edu/brooks/papers/representation.pdf
- "Take a look at Apple by the numbers". Michelle Gorman. http://www.newsweek.com/apple-statistics-370137
- "Astonishing Number: Ericsson Predicts 5.9 Billion Smartphone Users Within 5 Years." Tim Worstsall. https://www.forbes.com/sites/timworstall/2014/05/18/astonishing-number-ericsson-predicts-5-9-billion-smarpthone-users-within-5-years/#92e98f4211da
- "Exponential Growth of Software Patents". League for Programming Freedom. https://groups.csail.mit.edu/mac/projects/lpf/Patents/counts.html
- "Swarming Robots: Nanobot Miniature Drones Could Advance". Ashik Siddique. Micromedicinehttps://www.medicaldaily.com/swarming-robots-nanobot-miniature-drones-could-advance-micromedicine-video-244820
- Amazon Prime Air. https://www.amazon.com/b?node=8037720011&ref_=aa_art_btn&pf_rd_r=N92PR7H0T2SAB1Q9K7WF&pf_rd_p=ec147290-16e4-4069-a486-b236c63d9f95
- "How Big Data is Powering the Internet of Things (IoT) Revolution". Avantika Monnappa. https://www.simplilearn.com/how-big-data-powering-internet-of-things-iot-revolution-article
- "The Art of Connecting Man and Machine: The Internet of Things". Ashish Gupta. https://www.infosys.com/insights/digital-future/Pages/art-connecting-man-machine.aspx
- "The Internet of Things: The Next Technological Revolution". M. A. Feki ; F. Kawsar ; M. Boussard ; L. Trappeniers. http://ieeexplore.ieee.org/document/6457383/?reload=true
- "The Internet of Things: Evolution or Revolution?". Shawn DuBravac, Carlo Ratti. https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-white-paper-iot-english-digital-brochure.pdf
- "Our lives in 2025: What the world will be like in 10 years". Rohit Talwar. https://www.mirror.co.uk/news/uk-news/lives-2025-what-world-like-4878804
- "That 'Internet of Things' Thing". Kevin Ashton. http://www.rfidjournal.com/articles/view?4986
- "Sensor monitoring device". Theodore G. Paraskevakos. https://patents.google.com/patent/US3842208
- "Know the Difference Between IoT and M2M." Polsonetti, Chantal. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m
- "The Internet Toaster." Living Internet. http://www.livinginternet.com/i/ia_myths_toast.htm
- "The "Only" Coke Machine on the Internet." Carnegie Mellon University Computer Science Department. https://www.cs.cmu.edu/~coke/history_long.txt
- "The Trojan Room Coffee Pot." Stafford-Fraser, Quentin. http://www.cl.cam.ac.uk/cof
- "The IoT will be as fundamental as the Internet itself." Conant, Susan. http://radar.oreilly.com/2015/06/the-iot-will-be-as-fundamental-as-the-internet-itself.html

- "Moore's Law." Gordon E. Moore. http://www.umsl.edu/~siegelj/information_theory/projects/Bajramovic/www.umsl.edu/_abdcf/Cs4890/link1.html
- "Miniaturized Electronics". Harry K. Charles Jr. http://www.jhuapl.edu/techdigest/TD/td2604/Charles.pdf
- "Who needs faster computers?". John Naughton. https://www.theguardian.com/commentisfree/2016/feb/14/moores-law-no-more-computer-industry-processing-power-semiconductors
- "The Rise of Cloud Computing". David Byrnea, Carol Corradob, Daniel Sichelc. https://bea.gov/about/pdf/acm/2017/the-rise-of-cloud-computing-minding-your-ps-and-qs.pdf
- "IoT market research: Which industries are leading the curve?". Juan Jose Bello. http://www.ioti.com/strategy/iot-market-research-which-industries-are-leading-curve
- "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute, Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
- "What's Missing from the Industrial Internet of Things Conversation? Software." Cicciari, Matt http://www.wired.com/insights/2014/11/industrial-internet-of-things-software/
- "Internet of Things: Wearables." Paper realizado por Application Developers Alliance. http://www.appdevelopersalliance.org/internet-of-things/wearables/
- "Appliance Science: The Internet of Toasters (and Other Things)." Baguley, Richard, and Colin McDonald. http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/
- "What Is A Smart Home?". Dann Albright. https://www.makeuseof.com/tag/smart-home/
- "What Is a Smart City?". CISCO. https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html
- "Cisco Visual Networking Index: Forecast and Methodology, 2016–2021." Cisco. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf
- "History of the Internet of Things- Postscapes." Postscapes http://postscapes.com/internet-of-things-history
- "Internet Invariants: What Really Matters." Internet Society. https://www.internetsociety.org/wp-content/uploads/2017/08/Internet20Invariants-20What20Really20Matters.pdf
- "Architectural Considerations in Smart Object Networking." H. Tschofenig, J. Arkko, D. Thaler, D. McPherson. https://tools.ietf.org/html/rfc7452
- "Architectural Considerations in Smart Object Networking." H. Tschofenig, J. Arkko, D. Thaler, D. McPherson. https://www.ietf.org/proceedings/92/slides/slides-92-iab-techplenary-2.pdf
- "Overview of the Internet of Things." ITU. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

- "IEEE Communications Magazine - March 2018". IEEE http://digital.comsoc.org/system/files/magazines/ci/2018/march/index.html
- "Internet of Things." Oxford Dictionaries. http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things
- "One law professor's overview of the confusing net neutrality debate". Orin Kerr. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/11/28/one-law-professors-overview-of-the-confusing-net-neutrality-debate/?noredirect=on&utm_term=.c08a3ef76d57
- "Clueless CIO cloud confusion continues". Steven J. Vaughan-Nichols. https://www.computerworld.com/article/3132950/cloud-computing/clueless-cio-cloud-confusion-continues.html
- "What IP Means and How It Works". Nadeem Unuth. https://www.lifewire.com/internet-protocol-explained-3426713
- "Internet Protocol." DARPA. https://tools.ietf.org/html/rfc791
- "About DARPA". DARPA. https://www.darpa.mil/about-us/about-darpa
- "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460
- "Importance and Benefits of IPV6 over IPV4: A Study". Palukuru Venkata Praneeth Reddy, Kavali Mohammed Imran Ali, B. Sandeep, T.Ravi http://www.ijsrp.org/research-paper-1212/ijsrp-p1288.pdf
- "IPv6 Transition/Coexistence Security Considerations". IETF. https://tools.ietf.org/html/rfc4942
- Google IPv6. https://www.google.com/intl/es/ipv6/statistics.html
- "Internet Protocol, Version 6 (IPv6)". IETF. https://tools.ietf.org/html/rfc2460
- "What is White Space?". The Centre for White Space Communications, University of Strathclyde. https://www.wirelesswhitespace.org/more/what-is-white-space/
- ZigBee. http://www.zigbee.org/zigbee-for-developers/zigbee-3-0/
- Philips hue. https://www2.meethue.com/en-us/about-hue
- "What Are "ZigBee" and "Z-Wave" Smarthome Products?". Craig Lloyd. https://www.howtogeek.com/250614/what-are-zigbee-and-z-wave-smarthome-products/
- "Bluetooth Low Energy: It's Not Bluetooth. It's Better – Much Better". Craig Mathias. https://www.networkworld.com/article/2224506/smartphones/bluetooth-low-energy--it-s-not-bluetooth--it-s-better---much-better.html
- "ECSM2015-Proceedings of the 2nd European Conference on Social Media 2015". https://books.google.com.ar/books?id=VDU7CgAAQBAJ&lpg=PA398&ots=D-PIAxyjlL&dq=Bluetooth Special Interest Group (SIG) 2018 90%25&hl=es&pg=PP1 -v=onepage&q&f=false
- "IPv6 over BLUETOOTH(R) Low Energy". IETF. https://tools.ietf.org/html/rfc7668
- "Edge-centric Computing: Vision and Challenges". ACM SIGCOMM Computer Communication Review. https://dl.acm.org/citation.cfm?id=2831347.2831354
- WHAT IS THREAD?. Thread. https://www.threadgroup.org/What-is-Thread/Overview
- Nest. https://developers.nest.com/
- Sigfox. https://www.sigfox.com/en

- "M2M communications: A Systems Approach". What is M2M? p.2. David Boswarthick,Omar Elloumi,Olivier Hersent. https://books.google.com.ar/books?id=bVaqAFpH6EgC&printsec=frontcover&redir_esc=y#v=onepage&q&f=falsehttps://books.google.com.ar/books?id=bVaqAFpH6EgC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false
- Neul. http://neul.com/
- "Iceni – Product Brief". http://www.neul.com/neul/wp-content/uploads/2013/06/NL-000874-PB-5-Iceni-Product-Brief.pdf
- "What is Weightless?". http://www.weightless.org/about/what-is-weightless
- "Ofcom gives green light for 'TV white space' wireless technology". Ofcom. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2015/tvws-statement
- "6LoWPAN: An Open IoT Networking Protocol". Stefan Schmidt. https://events.static.linuxfound.org/sites/events/files/slides/6lowpan-openiot-2016.pdf
- "What is LoRaWAN?". https://www.lora-alliance.org/technology
- "Z-Wave". http://www.z-wave.com/about
- "What is NFC? Everything you need to know". Cameron Faulkner. https://www.techradar.com/news/what-is-nfc
- "Architectural Considerations in Smart Object Networking". Tech. no. RFC 7452. Internet Architecture Board. https://www.rfc-editor.org/rfc/rfc7452.txt
- "IAB Releases Guidelines for Internet-of-Things Developers." Duffy Marsan, Carolyn. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf
- "¿Qué es la informática en la nube?". Amazon. https://aws.amazon.com/es/what-is-cloud-computing/
- "Meet the Nest Thermostat." Nest Labs. https://nest.com/thermostat/meet-nest-thermostat/
- "Samsung Privacy Policy--SmartTV Supplement." Samsung Corp. http://www.samsung.com/sg/info/privacy/smarttv.html
- "Why Move To The Cloud? 10 Benefits Of Cloud Computing". Salesforce UK. https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html
- "The concept of vendor lock-in and how it relates to cloud computing." CA Community. https://www.ca.com/en/blog-highlight/the-concept-of-vendor-lock-in-and-how-it-relates-to-cloud-computing.html
- FitBit. https://www.fitbit.com/whyfitbit
- "How do I set up my Fitbit device?". FitBit Help. http://help.fitbit.com/articles/en_US/Help_article/1873
- "How It Works." SmartThings. http://www.smartthings.com/how-it-works
- "IAB Releases Guidelines for Internet-of-Things Developers." Duffy Marsan, Carolyn. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf
- "IETF Journal July of 2015". Carolyn Duffy Marsan, p.6.-p.8. https://wp.internetsociety.org/ietfjournal/wp-content/uploads/sites/22/2015/07/201507-ietf-journal-vol11-1-en.pdf

- "Security in the Internet of Things". Harald Bauer, Ondrej Burkacky, and Christian Knochenhauer. https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things
- "Fridge Caught Sending Spam Emails in Botnet Attack - CNET." Starr, Michelle. http://www.cnet.com/news/fridge-caught-sending-spamemails-in-botnet-attack/
- "The rise of IoT hacking: New dangers, new solutions". Conner Forrest. https://www.zdnet.com/article/the-rise-of-iot-hacking-new-dangers-new-solutions/
- "Why IoT Security Is So Critical". Ben Dickson. https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/
- "Securing the Internet of Things: A Proposed Framework". CISCO. https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
- "Hackers and defenders continue cybersecurity game of cat and mouse". Colin Barker.
- https://www.zdnet.com/article/hackers-and-defenders-continue-cyber-security-game-of-cat-and-mouse/
- Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST). http://www.nist.gov/customcf/ get_pdf.cfm?pub_id=912091
- Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) norma ISO/IEC 31010:2009 "Gestión de riesgos – Técnicas de evaluación de riesgos". http://www.iso.org/ iso/catalogue_detail?csnumber=51073
- "Hacking critical infrastructure via a vending machine? The IOT reality". Myles Bray. https://www.scmagazineuk.com/hacking-critical-infrastructure-via-a-vending-machine-the-iot-reality/article/740222/
- "The internet of things: convenience at a price". Nicole Kobie. https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security
- "EXTERNALIDADES Y MEDIOAMBIENTE". Víctor Manuel Vázquez Manzanares. http://www.eumed.net/rev/ibemark/02/medioambiente.html
- "Information Security and Externalities". Bruce Schneier
- https://www.schneier.com/essays/archives/2007/01/information_security_1.html
- "Will utilities drive IoT security market growth?". Donal Power. https://www.ibm.com/blogs/internet-of-things/will-utilities-drive-iot-security-market-growth/
- "Should I worry about my Philips Hue? Smart lights hacked by fly-by drone attack". Thomas Newton. http://uk.pcmag.com/philips-hue-connected-bulb/85962/news/should-i-worry-about-my-philips-hue-smart-lights-hacked-by-f
- "Why Do IoT Devices Die?". Leor Grebler. https://medium.com/iotforall/why-do-iot-devices-die-e4df0c7a075d
- "Fiat Chrysler recalls 1.4m vehicles in wake of Jeep hacking revelation".
- https://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking
- "IoT security: the majority of IoT devices is not monitored in real time". I-SCOOP. https://www.i-scoop.eu/iot-security-majority-iot-devices-not-monitored-real-time/

- "IoT in Physical Security: Understanding Threats and Concerns". Bernhard Mehl. https://www.getkisi.com/blog/secure-iot-physical-security-whitepaper-free-pdf-download
- "The silent, lethal rise of the 'shadow Internet of Things'". John E Dunn. https://www.techworld.com/security/silent-lethal-rise-of-shadow-internet-of-things-3614910/
- http://www.arduino.cc y la Fundación Raspberry Pi http://www.raspberrypi.org/
- "Four Ethical Issues in Online Trust." Wilton, Robin. https://www.internetsociety.org/sites/default/files/Ethical Data-handling - v2.0.pdf
- "60% of IoT devices falling short on privacy and data protection". Sarah Wray. https://inform.tmforum.org/news/2016/09/60-iot-devices-falling-short-privacy-data-protection/
- "Your New Fridge Is Spying on You". Harrison Cramer
- https://tcf.org/content/commentary/new-fridge-spying/
- "Is Alexa Really Eavesdropping on You?". Brad Stone. https://www.bloomberg.com/news/articles/2017-12-11/is-alexa-really-eavesdropping-on-you-jb25c6vc
- "Why the fight over IoT data is just getting started". Gary Eastwood. https://www.networkworld.com/article/3234367/internet-of-things/why-the-fight-over-iot-data-is-just-getting-started.html
- "People are really worried about IoT data privacy and security—and they should be". Fredric Paul. https://www.networkworld.com/article/3267065/internet-of-things/people-are-really-worried-about-iot-data-privacy-and-securityand-they-should-be.html
- "IoT silliness: 'Headless' devices without UI". Galem Gruman.
- https://www.infoworld.com/article/2867356/internet-of-things/beware-this-iot-fallacy-the-headless-device.html
- "The psychology of privacy in the era of the Internet of Things". Susan Scutti. https://edition.cnn.com/2017/03/22/health/psychology-privacy-wikileaks-internet-of-things/index.html
- "Insurance industry lags behind in using IoT data to boost business value". Alison DeNisco Rayome. https://www.techrepublic.com/article/insurance-industry-lags-behind-in-using-iot-data-to-boost-business-value/
- "Putting Privacy Concerns about the Internet of Things in Perspective". Adam Thierer. https://iapp.org/news/a/putting-privacy-concerns-about-the-internet-of-things-in-perspective/
- "Internet interoperability". Richard Feasey. https://innovation-regulation.telecom-paristech.fr/wp-content/uploads/2017/10/Internet-Interoperability.pdf
- "A History of the Internet" . http://inthistory4u.blogspot.com/2010/08/1988.html
- "A Mission Statement for the IETF. H. Alvestrand. https://www.rfc-editor.org/rfc/rfc3935.txt
- "Open Internet: What is it, and how to avoid mistaking it for something else". Internet Society https://www.internetsociety.org/wp-content/uploads/2017/08/The20Open20Internet20What20it20is2C20and20how20to20avoid20mistaking20it20for20something20else20.pdf
- "What is a Walled Garden? And why it is the strategy of Google, Facebook and Amazon Ads platform?". Pierre de Poulpiquet. https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1

- "Why interoperability holds the keys to the smart home". Jessica Groopman. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-interoperability-holds-the-keys-to-the-smart-home
- "Rolling plan for ICT standardisation. European Commission". Sección 3.5.6, https://ec.europa.eu/digital-agenda/en/rolling-plan-ict-standardisation
- "The Internet of Things: Mapping the Value beyond the Hype". McKinsey Global Institute. http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
- "Freedom and Walled Gardens". Bryon Moyer. http://www.insidetheiot.com/freedom-walled-garden/
- "Why interoperability is key to building confidence in IoT". Dr. Omar Elloumi. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Why-interoperability-is-key-to-building-confidence-in-IoT
- "Philips Lighting: Standardization and Interoperability are Keys to Success". Weili Lin. https://mysmahome.com/company/5907/philips-lighting-standardization-and-interoperability-are-keys-to-success-2/
- "Interoperability: A key barrier to connected home adoption". Harry Wang. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Interoperability-A-key-barrier-to-connected-home-adoption
- "Fitbit leverages Google Cloud to accelerate healthcare innovation". Ryan Daws. https://www.iottechnews.com/news/2018/apr/30/fitbit-google-cloud-digital-healthcare/
- "The Internet of Stupid Things". Geoff Huston. https://labs.apnic.net/?p=620
- IETF. https://www.ietf.org/about/mission/
- ITU. https://www.itu.int/es/about/Pages/default.aspx
- IEEE. https://www.ieee.org/about/vision-mission.html
- Industrial Internet Consortium. http://www.iiconsortium.org/about-us.htm
- Open Interconnection Consortium. https://openconnectivity.org/
- ZigBee Alliance. http://www.zigbee.org/zigbeealliance/developing-standards/
- "Why Internet of Things 'standards' got more confusing". Stephen Lawson. https://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html
- "Recent IoT Device Cases". Clifford J. Zatz, Joe Meadows, Laura Aradi and Paul Mathis. https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/
- "Laws and Ethics Can't Keep Pace with Technology". Vivek Wadhwa. https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/
- "Take a tour of Google's secretive data centers where all your photos and emails are stored". Eugene Kim. http://www.businessinsider.com/google-data-centers-store-all-your-photos-and-emails-2015-6
- "Data Protection Law and International Jurisdiction on the Internet (Part 2)". Christopher Kuner. https://poseidon01.ssrn.com/delivery.php?ID=278100090106071002110088030110091076096012041014091091022030017078001125122088091064039025063115053046114003078088105113113083 1

220740620930471260150000750941180770960700590390670871180741191150720710100650991250001000300310971241050921070140991161000 17&EXT=pdf

- "Big Doctor Is Watching". Hamza Shaban. http://www.slate.com/articles/technology/future_tense/2015/02/how_data_from_fitness_trackers_medical_devices_could_affect_health_insurance.html
- "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles". Andrew Meola. http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10
- "America's Truckers Embrace Big Brother After Costing Insurers Millions". Leslie Scism. https://www.wsj.com/articles/americas-truckers-embrace-big-brother-after-costing-insurers-millions-1496577601
- "Personalization Comes to Retail with Big Data, IoT and Augmented Reality." Michael Wu. https://www.cmswire.com/digital-experience/personalization-comes-to-retail-with-big-data-iot-and-augmented-reality/
- Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age. Charlotte A Tschider http://www.academia.edu/36014158/Regulating_the_IoT_Discrimination_Privacy_and_Cybersecurity_in_the_Artificial_Intelligence_Age
- "Big Data on Internet of Things: Applications, Architecture, Technologies, Techniques, and Future Directions". Heba Aly, Mohammed Elmogy, Shereif Barakat. http://www.ijcse.net/docs/IJCSE15-04-06-040.pdf
- "What is Permissionless Innovation?". http://permissionlessinnovation.org/what-is-permissionless-innovation/
- "5 Ways Tech Is Stopping Theft." Jennifer Goforth Gregory. https://www.entrepreneur.com/article/229674
- "Lawyers reaching for in-car data." Vince Bond Jr. http://www.autonews.com/article/20140914/OEM11/309159952/lawyers-reaching-for-in-car-data
- "Cool cop tech: 5 new technologies helping police fight crime". Todd Weiss. https://www.computerworld.com/article/2501178/government-it/cool-cop-tech--5-new-technologies-helping-police-fight-crime.html?page=2
- "Secure all the things! How to protect human rights on the Internet of Things." Lucie Krahulcova. https://www.accessnow.org/secure-things-protect-human-rights-internet-things/
- "Your iPhone is now encrypted. The FBI says it'll help kidnappers. Who do you believe?" Trevor Timm. https://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default
- "Apple will no longer unlock most iPhones, iPads for police, even with search warrants." Craig Timberg. https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.5f654a66048a
- "Who Is Responsible for IoT Security?". Rick M Robinson. https://securityintelligence.com/who-is-responsible-for-iot-security/

- "Hacker Exploits a Baby Monitor to Spy on and Insult a Toddler". Fox Van Allen. https://www.techlicious.com/blog/hacker-exploits-a-baby-monitor-to-spy-on-and-insult-a-toddler/
- "Hackers hijack Philips Hue lights with a drone". Timothy J. Seppala. https://www.engadget.com/2016/11/03/hackers-hijack-a-philips-hue-lights-with-a-drone/
- "IoT attacks are getting worse -- and no one's listening". Alfred Ng. https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/
- "Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian". Sam Levin, Julia Carrie Wong. https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe
- "E-ZPass records out cheaters divorce court". Chris Newmarker. http://www.nbcnews.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/%20-%20.Vbp9KnjfbFI#.We0FsRNSxTY
- "Fitbit data is now being used in COURT: Wearable technology is set to revolutionise personal injury and accident claims". Sarah Griffiths. http://www.dailymail.co.uk/sciencetech/article-2838025/Fitbit-data-used-COURT-Wearable-technology-set-revolutionise-personal-injury-claims.html
- "Why the repo man can remotely shut off your car engine". Aimee Picchi. https://www.cbsnews.com/news/why-the-repo-man-can-remotely-shut-off-your-car-engine/
- "Miss a Payment? Good Luck Moving That Car". Michael Corkery and Jessica Silver-Greenberg. https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/
- "Electronic Noise Is Drowning Out the Internet of Things". Mark A. McHenry, Dennis Roberson and Robert J.Matheson. https://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things
- "Policy Paper on IoT Future Technologies". Maarten Botterman. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf
- "Developing Countries Will Drive The Growth Of The Internet Of Things". David Bolton. https://www.applause.com/blog/internet-of-things-growth-developing-countries/
- "Internet Society - Principles". Internet Society. https://isoc-ny.org/misc/isoc-ny_side2.pdf
- "Unlocking the potential of the Internet of Things". James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
- "Internet of Things sees explosive growth in China". Li Yan. http://en.people.cn/n3/2017/0914/c90000-9269103.html
- "Sustainable Development Topics". ONU. https://sustainabledevelopment.un.org/topics
- "Water quality monitoring and waste management using IoT". M. V. Ramesh. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8239311&isnumber=8239217
- "World Population Growth". Max Roser, Esteban Ortiz-Ospina. https://ourworldindata.org/world-population-growth
- "Internet of food". http://internet-of-food.org/

- "Policy Paper on IoT Future Technologies". Maarten Botterman. http://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf
- "Digital farm set for internet's next wave". The Guardian. https://www.theguardian.com/connecting-the-future/2015/sep/21/digital-farm-set-for-internets-next-wave
- "How Amazon's Echo went from a smart speaker to the center of your home". Matt Weinberger. http://www.businessinsider.com/amazon-echo-and-alexa-history-from-speaker-to-smart-home-hub-2017-5
- "Alexa and Google Assistant Battle for Smart Home Leadership, Apple and Cortana Barely Register". Bret Kinsella. https://www.voicebot.ai/2018/05/07/alexa-and-google-assistant-battle-for-smart-home-leadership-apple-and-cortana-barely-register/
- "Amazon Alexa Smart Speaker Market Share Dips Below 70% In U.S., Google Rises to 25%". Brett Kinsella. https://www.voicebot.ai/2018/01/10/amazon-alexa-smart-speaker-market-share-dips-70-u-s-google-rises-25/
- "Amazon Introduces the Alexa Fund: $100 Million in Investments to Fuel Voice Technology Innovation". Amazon. http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=2062558
- "APPLE HOMEPOD REVIEW: LOCKED IN". Nilay Patel. https://www.theverge.com/2018/2/6/16976906/apple-homepod-review-smart-speaker
- "Alexa with better audio? CES introduces the Lenovo Smart Assistant". Dan Ackerman. https://www.cnet.com/products/lenovo-smart-assistant-with-amazon-alexa/preview/
- "Affectiva CEO: AI needs emotional intelligence to facilitate human-robot interaction". Khari Johnson. https://venturebeat.com/2017/12/09/affectiva-ceo-ai-needs-emotional-intelligence-to-facilitate-human-robot-interaction/
- "Amazon's Alexa wants to learn more about your feelings". Khari Johnson.
- https://venturebeat.com/2017/12/22/amazons-alexa-wants-to-learn-more-about-your-feelings/
- "Amazon will let developers build Alexa skills that recognize unique voices in 2018". Khari Johnson.
- https://venturebeat.com/2017/11/28/amazon-will-let-developers-build-alexa-skills-that-recognize-unique-voices-in-2018/
- "The 10 Hottest Global Years on Record". Climate Central. http://www.climatecentral.org/gallery/graphics/the-10-hottest-global-years-on-record
- "Temperaturas promedio mundiales". Intergovernmental Panel on Climate Change. https://www.ipcc.ch/publications_and_data/ar4/wg1/es/tssts-3-1-1.html
- "Air Polution". National Geographic. https://www.nationalgeographic.com/environment/global-warming/pollution/
- "The rise of co-working space and the need for smart buildings". Rinse Bruggeman, Desie Driever and Wilfrid Donkers. https://www2.deloitte.com/global/en/pages/real-estate/articles/rise-co-working-space-need-smart-buildings.html
- "Global Commercial Building Automation Market Revenues will Reach $45 Billion by 2021". ABI Research.
- https://www.abiresearch.com/press/global-commercial-building-automation-market-reven/

- "Multi-Zone Automatic Temperature Control System". ASME. https://www.asme.org/about-asme/who-we-are/engineering-history/landmarks/244-multi-zone-automatic-temperature-control
- "Press Release: President Clinton Announces Landmark Program to Reduce Energy Use in Buildings Worldwide". Clinton Foundation. https://www.clintonfoundation.org/main/news-and-media/press-releases-and-statements/press-release-president-clinton-announces-landmark-program-to-reduce-energy-use.html
- "Connecting Buildings to the Cloud for a Greener Planet". Microsoft. https://customers.microsoft.com/en-US/story/connecting-buildings-to-the-cloud-for-a-greener-planet
- "Chiller Best Practices VSD". Johnson Controls. http://www.johnsoncontrols.com/buildings/hvac-equipment/chillers/variable-speed-drives/chiller-best-practices-vsd
- "Cost control strategies for zero energy buildings". National Renewable Energy Laboratory.
- https://www.nrel.gov/docs/fy14osti/62752.pdf
- "Daimler and Volvo Take Lead in Implementation of V2V Communication Systems in Europe." Katja Feick. http://www.frost.com/prod/servlet/press-release.pag?docid=289374477
- "¿Qué es la informática en la nube?". Amazon. https://aws.amazon.com/es/what-is-cloud-computing/
- "The Cloud Imperative". Simson Garfinkel. https://www.technologyreview.com/s/425623/the-cloud-imperative/
- "Who Coined 'Cloud Computing'?". Antonio Regalado. https://www.technologyreview.com/s/425970/who-coined-cloud-computing/
- "Conversation with Eric Schmidt hosted by Danny Sullivan". Eric Schmidt. https://www.google.com/press/podium/ses2006.html
- "CEO of $50 billion Salesforce shared his epic founding story to inspire a small business owner". Eugene Kim. http://www.businessinsider.com/salesforce-benioff-shares-founding-story-2015-9
- "The history of AWS: A timeline of 12 defining moments from 2002 to now". Computerworld UK staff. https://www.computerworlduk.com/galleries/cloud-computing/aws-12-defining-moments-for-the-cloud-giant-3636947/
- "Google Apps is out of beta (yes, really)". Matthew Glotzbach. https://googleblog.blogspot.com/2009/07/google-apps-is-out-of-beta-yes-really.html
- "Cloud computing defined: Characteristics & service levels". Edwin Schouten. https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/
- "Precios de Amazon EC2". Amazon. https://aws.amazon.com/es/ec2/pricing/
- "What is scalability in cloud computing?". Phil Zona. https://www.cloudassessments.com/blog/scalability-cloud-computing/
- "Virtualization and Cloud Computing". Intel. https://www.intel.com/content/dam/www/public/us/en/documents/guides/cloud-computing-virtualization-building-private-iaas-guide.pdf
- "Cloud physical security considerations". Turgut Aslan. https://www.ibm.com/blogs/cloud-computing/2012/02/22/cloud-physical-security-considerations/

- "Operation and Maintenance Management Strategy of Cloud Computing Data Center." Wei Bai, Wenli Geng. http://onlinepresent.org/proceedings/vol78_2014/2.pdf
- "WHAT IS INFRASTRUCTURE AS A SERVICE (IAAS)?". Redcentric. http://www.redcentricplc.com/resources/articles/what-is-iaas/
- "¿Qué es SaaS?". Microsoft. https://azure.microsoft.com/es-es/overview/what-is-saas/
- "¿Qué es PaaS?". Microsoft. https://azure.microsoft.com/es-es/overview/what-is-paas/
- "What is IaaS?". Microsoft. https://azure.microsoft.com/en-us/overview/what-is-iaas/
- "Cisco UCS and EMC® VNX™ 5300 with Microsoft Private Cloud Fast Track 2.0". CISCO. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-711496.pdf
- "What are public, private, and hybrid clouds?". Microsoft. https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/
- "¿Cuántos tipos de 'cloud computing' existen y en qué se diferencian?". Alberto Iglesias Fraga. http://www.ticbeat.com/tecnologias/cuantos-tipos-de-cloud-computing-existen-y-en-que-se-diferencian/
- "How Virtualization Enhances Cloud Computing". Vittorio Viarengo. https://www.forbes.com/2010/08/24/enterprise-cloud-computing-technology-cio-network-virtualization.html#1f59c12c4b9f
- "5 Benefits of Virtualization in a Cloud Environment". Muzzammil Hanif. https://www.quickstart.com/blog/post/5-benefits-of-virtualization-in-a-cloud-environment/
- "The Economic Benefit of Cloud Computing". Kevin Jackson. https://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/#118e88a4225c
- "What high availability for cloud services means in the real world". Thoran Rodrigues. https://www.techrepublic.com/blog/the-enterprise-cloud/what-high-availability-for-cloud-services-means-in-the-real-world/
- "Cloud Computing, Server Utilization, & the Environment". Jeff Barr. https://aws.amazon.com/es/blogs/aws/cloud-computing-server-utilization-the-environment/
- "12 Benefits of Cloud Computing". Salesforce. https://www.salesforce.com/hub/technology/benefits-of-cloud/
- "Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward". Joe McKendrick. https://www.forbes.com/sites/joemckendrick/2011/11/20/cloud-computings-vendor-lock-in-problem-why-the-industry-is-taking-a-step-backwards/#1137961f7267
- "Cambridge Analytica: Facebook data-harvest firm to shut". BBC. https://www.bbc.com/news/business-43983958
- "Cloud computing is a trap, warns GNU founder Richard Stallman". Bobbie Johnson. https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman