CELE
Centro de Estudios en Libertad de Expresión y Acceso a la Información

EL 'INTERNET DE LAS COSAS':

MÁS INTERNET QUE OTRA COSA[1]

[1] *Este documento fue elaborado por Carlos Cortés, investigador del iLei en el CELE. La investigación contó con el apoyo de Juan Diego Castañeda y aportes de Eduardo Bertoni, director del CELE.*

Resumen

El objetivo de este documento es ofrecer un panorama sobre el tema conocido públicamente como el 'internet de las cosas' (IoT). Primero, plantea el antecedente histórico de la computación ubicua; segundo, describe los retos técnicos que implica hablar de un internet de las cosas; tercero, habla sobre los riesgos de un entorno de objetos interconectados.

La idea subyacente de este texto es que el internet de las cosas reúne una amalgama de conceptos e ideas sobre productos y servicios presentes y futuros. Es decir, gira alrededor de hechos, ideas y meras especulaciones. Esto implica, en parte, que cualquier aproximación al internet de las cosas pasa por debates conocidos sobre internet, privacidad y seguridad en línea, entre otros.

Al final, el documento plantea las siguientes conclusiones y recomendaciones:

- Los riesgos en materia de privacidad, seguridad y autonomía que surgen en el IoT no son distintos a los que encontramos asociados hoy al entorno digital en general.

- Entre todos los problemas identificados, el de privacidad parece el más grave. Pensada desde el diseño y la ingeniería, el IoT no incorpora un análisis sobre este punto, a pesar de que la 'privacidad por diseño' no es un tema nuevo en el debate de tecnología y regulación.

- En un contexto como el latinoamericano, la idea del IoT puede desembocar fácilmente en formas de discriminación y profundización de la brecha digital.

- La decisión sobre estándares técnicos para conectar objetos a la red está relacionada con la gobernanza de internet. En particular, con la gestión de los recursos críticos.

- Cualquier discusión sobre IoT debe tener en cuenta los retos que aún subsisten en materia de infraestructura y acceso a internet en América Latina.

- Donde la sociedad está organizada alrededor de la tecnología, el poder tecnológico es la principal forma de poder. Esto implica aproximarse críticamente al proyecto comercial del IoT, sin desconocer sus virtudes y sin desestimar sus problemas.

- Para la sociedad civil resulta fundamental abrir espacios de interlocución para participar en este tipo de discusiones. Las organizaciones, centros de pensamiento, universidades y grupos ciudadanos, pueden ofrecer una perspectiva distinta al tema del IoT.

1. Introducción

De un tiempo para acá venimos oyendo hablar de un nuevo amanecer en la tecnología: el internet de las cosas. Un mundo de objetos interconectados, de ciudades y hogares inteligentes, de aplicaciones y servicios automáticos. Los ejemplos de este futuro digital son tan inagotables como la imaginación de sus exponentes. Los más convencionales se relacionan con el hogar: cortinas que interpretan la luz del día para abrirse o cerrarse, lavadoras que pueden interactuar con la ropa para reportar el estado de desgaste de ésta, y neveras que reportan directamente los alimentos que están por caducar o que hacen falta.

También hay ejemplos más complejos, que involucran un mayor grado de interacción entre la persona y la máquina, y entre éstos y los entornos sociales: un profesor se encuentra enfermo y avisa a la universidad donde trabaja que no se presentará a clase. La universidad envía esa información a los estudiantes y, a través de un sistema que integra dispositivos conectados a la red, cambia la agenda de los estudiantes, cambia la hora de sus despertadores e incluso programa la cafetera para una hora más tarde.[1]

En esencia, el internet de las cosas promete escenarios donde los objetos facilitarán nuestra vida cotidiana. Pero, ¿es realmente algo distinto a lo que ya tenemos? ¿Es el internet de las cosas una idea, un proyecto, una estrategia comercial? ¿Conlleva riesgos?

Parece prematuro adentrarse en esta discusión cuando todavía internet es una tecnología joven y su desarrollo y regulación enfrentan tantas incertidumbres. Más aún en América Latina, donde la penetración ni siquiera alcanza el 50% y los computadores portátiles y los teléfonos móviles siguen siendo artículos costosos.[2] Sin embargo, la atención que los medios de comunicación vienen prestándole al tema y la inclinación de la gente por consumir innovación tecnológica –ya sea a manera de noticias o de productos como tal–, amerita hacer una revisión más desapasionada.

El objetivo de este documento es entonces ofrecer un panorama sobre el tema conocido públicamente como el 'internet de las cosas'. Para hacerlo, primero planteamos el antecedente histórico de la computación ubicua, lo cual permite ubicarse de mejor manera en la coyuntura actual; en seguida, describimos los retos técnicos que implica hablar de un internet de las cosas; en tercer lugar, describimos los riesgos de un entorno de objetos interconectados –haciendo énfasis en el acopio de información y los problemas de seguridad–, y, finalmente, planteamos unas conclusiones y recomendaciones.

La idea subyacente de este texto es que el internet de las cosas reúne una amalgama de conceptos e ideas sobre productos y servicios presentes y futuros. Es decir, gira alrededor de hechos, ideas y meras especulaciones. Esto implica, en parte, que cualquier aproximación al internet de las cosas pasa

[1] Ejemplo tomado de Internet of Things Europe - Teaser N° 1: Student por Digital Agenda EU. Disponible en: https://www.youtube.com/watch?v=kq8wcjQYW90 (consultado el 30 de noviembre de 2014).
[2] Ver, Internet Usage Statistics for all the Americas. En Internet World Stats. Disponible en: http://www.internetworldstats.com/stats2.htm (consultado el 30 de noviembre de 2014).w

por debates conocidos sobre internet, privacidad y seguridad en línea, entre otros. Para efectos de discusiones sobre regulación y políticas públicas de internet, esta claridad puede servir para evitar distraer la atención o, más bien, para centrar la atención en los aspectos relevantes de este tema.

2. La sala de trabajo del futuro

En septiembre de 1991, Mark Weiser escribió para *Scientific American* un artículo titulado 'El computador para el siglo XXI'. En una de las fotos que acompañan el texto aparecen Weiser y tres personas más en una especie de sala de trabajo del futuro. La primera está parada explicando algo en una pantalla o televisor gigante, similar en tamaño a un tablero de un salón de clases. Las demás están cómodamente sentadas alrededor de una mesa redonda: dos de ellas trabajan en tabletas monocromáticas –en verde y negro– con lápices o bolígrafos en la mano, mientras que la última –Weiser– observa un monitor individual.[3]

Se trataba, en realidad, de un futuro próximo. Para entonces este grupo de científicos del centro de investigación de Xerox en Palo Alto (conocido como PARC, por su nombre en inglés) ya había diseñado tres dispositivos –dos de los cuales aparecen en la foto–: los *tabs*, pequeños aparatos que hacían las veces de notas post-it; los *pads,* que se asemejaban a una libreta u hoja de papel, y los tableros, homónimos de sus pares analógicos. Weiser proponía que la oficina del futuro tuviera centenares de éstos en una habitación. Y, contrario a lo que vemos hoy, no se trataba de dispositivos personales. De la misma forma como una persona usa una hoja de borrador en una reunión, la idea era que pudiera usar un *tab* o *pad* cualquiera que estuviera disponible, para después transmitir la información sin llevárselo.

Aunque en 1991 se trataba de una escena que maravillaría a una persona común y corriente, el PARC veía todos estos aparatos como una escala para llegar a algo más grande. Para Weiser, la noción del computador personal era en sí misma equivocada: *"Tales máquinas no pueden lograr que la computación sea una parte integral e invisible en la forma como la gente vive sus vidas. Por lo tanto, estamos tratando de concebir una nueva forma de pensar acerca de los computadores en el mundo, una que tome en cuenta el medio ambiente natural del ser humano y permita que los computadores como tales desaparezcan en un segundo plano"*.[4] Dicho en otras palabras, Weiser abogaba porque el poder de la computación se liberara de la esclavitud de la pantalla. Solo así podría mezclarse en nuestras vidas cotidianas.

Weiser –que moriría en 1999 sin llegar a ver la revolución que vaticinó– bautizó esta compenetración entre la máquina y el entorno humano como 'computación ubicua', que para él no podía entenderse ni como realidad virtual ni inteligencia artificial. Esta última se enfoca en simular el mundo real, y no en aumentar y mejorar el que ya existe. Tampoco se trataba de lo primero. El reto, concluía, era incrustar la computación en el día a día de las personas. Para la época del artículo de *Scientific American* los 'switches' de luz, termostatos, hornos y equipos de sonido ya tenía algún nivel de computación interna. El propósito era, entonces, que esos y otros objetos entraran a hacer parte de una red omnipresente e invisible.

[3] La foto puede verse en: http://www.watershed.co.uk/pmstudio/events/fri-14052010-100pm (consultado el 30 de noviembre de 2014).
[4] Weiser, M. 'The Computer of the 21st Century'. En: Scientific American, septiembre de 1991, p. 94 (traducción informal).

Esta proposición se adentra en los terrenos del diseño, donde quizá el exponente más relevante para los partidarios de la computación ubicua es el diseñador japonés Naoto Fukusawa. Fukusawa considera que los productos deben ser sensibles a la naturaleza humana; deben poder usarse 'sin pensar'. Cuando los objetos se amoldan de manera natural a ciertos ambientes y ciertos patrones de uso, se disuelven en la acción del individuo –'diseño que se disuelve en conducta'–.[5] Un ethos similar guiaba a Steve Jobs, el fundador de Apple, para quien los objetos tenían una esencia y una pureza intrínseca.[6] Weiser resumió ese horizonte en una frase que a la postre se convirtió en el prólogo de la computación ubicua, el antecedente obligatorio –y técnicamente más ajustado– de lo que hoy conocemos como internet de las cosas (*Internet of Things* o *IoT*): *"Las tecnologías más profundas son aquellas que desaparecen. Se tejen a sí mismas en la tela de la vida diaria hasta que son imposibles de distinguirse de ésta".*[7]

Distintos autores han propuesto nuevas aproximaciones que abarquen y den un sentido integral a la idea de computación ubicua.[8] Al final, cada aporte da un elemento adicional sin que parezca posible asir algo tan amplio y ambiguo. Adam Greenberg, por ejemplo, considera que definir la computación del futuro como aquella que es móvil, usable, conectada o situada, ofrece una visión muy angosta del fenómeno. En respuesta, él propone el paradigma del *everyware,* un neologismo en inglés que mezcla términos como 'todos los días' (*everyday*) y 'en todas partes' (*everywhere*), con otros como 'ubicado', 'consciente' (*aware*) y 'usable' (*wearable*). *Everyware,* según Greenberg, es una experiencia que involucra *"una ecología diversa de dispositivos y plataformas"* que difiere del entendimiento convencional que tenemos sobre los computadores. Se trata de un fenómeno distribuido: el poder y significado no radica en los nodos sino en la red, que es en efecto invisible y que permea lugares y actividades.[9]

La descentralización y dispersión de dispositivos implica una multiplicación de las fuentes de información. Información que no necesariamente tiene que procesar un computador de uso general, sino que está presente en los mismos objetos, que dan cuenta del lugar en el que se encuentran y la función que cumplen; objetos conscientes de su contexto (*context-aware*). Kevin Ashton, la persona que acuñó el término de 'internet de las cosas', considera que el núcleo es dotar a los objetos con la capacidad de recoger información por ellos mismos y no a través de seres humanos, como hoy se hace.[10]

[5] Cfr. Parsons, T. Thinking Objects: Contemporary Approaches to Product Design, AVA Book, 2009.
[6] Cfr. Morozov, E. 'Steve Jobs's pursuit of perfection—and the consequences'. En: The New Republic, febrero de 2012. Disponible en: http://www.newrepublic.com/article/books-and-arts/magazine/100978/form-fortune-steve-jobs-philosopher (consultado el 30 de noviembre de 2014).
[7] Ibidem.
[8] Cfr. Bell, G.; Dourish, P. 'Yesterday's tomorrows: notes on ubiquitous computing's dominant vision'. Personal and Ubiquitous Computing 11.2, 2007; Abowd, G.,; Mynatt, E. 'Charting past, present, and future research in ubiquitous computing'. ACM Transactions on Computer-Human Interaction (TOCHI) 7.1. 2000.; Hansmann, U. (ed). Pervasive computing: The mobile world. Springer, 2003.; Saha, D.; Mukherjee, A. Pervasive computing: a paradigm for the 21st century. Computer 36.3. 2003.
[9] Cfr. Greenfield, A. Everyware. The dawning age of ubiquitous computing. New Riders, 2006, p. 38-39.
[10] Ashton, K. `The Internet of Things 'Thing'. En RFID Journal, junio de 2009. Disponible en: http://www.rfidjournal.com/articles/view?4986 (consultado el 30 de noviembre de 2014).

Reuniendo de una u otra forma los elementos anteriores, se han propuesto decenas de definiciones del IoT. Para efectos de ilustración, citaremos dos:

- *"Es una infraestructura global interconectada, enlazando objetos físicos y virtuales a través de la explotación de la captura de datos y las capacidades de comunicación. Ofrecerá identificación específica de objetos y capacidades sensoriales y de conectividad como la base para el desarrollo de servicios cooperativos y aplicaciones independientes".*[11]

- *"Un mundo donde los objetos están integrados de manera perfecta y sin sobresaltos en la red de la información, y donde los objetos físicos pueden convertirse en participantes activos de los procesos comerciales. Los servicios pueden interactuar con estos 'objetos inteligentes' a través del internet, hacer una consulta y cambiar su estado y cualquier información asociada con ellos".*[12]

El internet de cosas se plantea también como una fase evolutiva en la relación en línea entre el individuo y el computador. Servicios como el correo electrónico, los mensajes de textos y las llamadas, tenían el propósito de satisfacer una interacción de persona a persona. En efecto, en una primera etapa de internet la mayor parte del tráfico correspondía a datos de voz y texto. Más adelante, apareció la interacción individuo-máquina con servicios de distribución de contenido -como el video por demanda-, que hoy ocupan un lugar protagónico. Ahora, con la computación ubicua en el horizonte, los servicios de automatización plantean una relación máquina-máquina o cosa-cosa (dispositivos que 'hablan' entre sí: sensores de movimiento o de luz que envían una orden a un sistema de sonido o de seguridad, o automóviles que capturan datos de las autopistas).[13]

Más allá de eso, hoy por hoy el énfasis del debate público sobre el IoT parece estar más en el diseño y estética de la cosa, que en la computación que requiere. David Rose se refiere a los 'objetos encantados', que empiezan como algo ordinario –un zapato, una billetera, un bombillo– para convertirse en aparatos extraordinarios gracias a los sensores, conexiones y procesos tecnológicos incrustados. Es ahí donde encontramos las imágenes futuristas, ya no desde la visión remota de Weiser sino desde un mañana que parece cercano. Parece, decimos, porque muchos de los anuncios del internet de las cosas dependen de posibilidades tecnológicas y realidades de mercado. Es decir, el internet de las cosas está y no está entre nosotros.

[11] CASAGRAS, 'RFID and the Inclusive Model for the Internet of Things'. Citado en: 'Internet of Things Definitions. Postscapes (traducción informal). Disponible en: http://postscapes.com/internet-of-things-definition (consultado el 30 de noviembre de 2014).
[12] Haller, S., SAP Research. 'Internet of Things: An Integral Part of the Future Internet', Ibidem.
[13] Cfr. Chaouchi, H. ed. The Internet of Things: Connecting Objects to the Web. Wiley, 2010.

3. Los retos técnicos del IoT

La computación ubicua que imaginaba Weiser implicaba superar varios escollos que él mismo dejó planteados. En primer lugar, el problema del movimiento de dispositivos: *"Los ingenieros tendrán que desarrollar nuevos protocolos de comunicación que reconozcan explícitamente el concepto de máquinas que se mueven en el espacio físico"*.[14] En segundo lugar, la interconexión de las redes y la interoperabilidad de los sistemas. En 1991 ya existían redes cerradas –tanto cableadas como inalámbricas– para la transmisión de datos. Además, la capacidad estaba en incremento, especialmente en distancias cortas. Pero un dispositivo no podía tener simultáneamente conexión inalámbrica de muy corto alcance, inalámbricas de largo alcance, y fijas de alta velocidad. Finalmente, se necesitaría un método que permitiera un verdadero intercambio de datos. Ahí el científico del PARC se aventuró con una predicción: las redes del futuro usualmente no dedicarán su ancho de banda a una sola transmisión; *"en cambio, permitirán que una enorme cantidad de transmisiones de baja velocidad se lleven a cabo de manera simultánea"*.[15]

No hacen falta más pistas. Weiser marcaba un derrotero –en el que por supuesto participaron miles de personas como él– para llegar a lo que hoy tenemos: conexiones de datos celulares, conexiones inalámbricas como *Wifi* y *Bluetooth,* y la conmutación de paquetes.[16] Estos avances técnicos, sumados a los microprocesadores y los sensores para identificar objetos, permiten imaginar el internet de las cosas.[17]

Las etiquetes de Identificación por Radiofrecuencia (RFID, por su nombre en inglés) son un elemento básico en este sistema descentralizado de datos. Pueden ser tan pequeñas como el botón de una camisa o un grano de arroz, y están compuestas por dos partes: un 'transpondedor', que contiene un microchip y una antena, y un lector, que activa y recupera la información que aquel almacena.[18] En otras palabras, las etiquetas RFD guardan datos y los transmiten vía radio, a través de una antena, a un dispositivo con capacidad de leerlos.

Estas etiquetas pueden ser pasivas, semi-pasivas o activas. Como su nombre lo indica, las pasivas no tienen alimentación eléctrica propia, sino que se activan gracias a la energía que produce la señal del lector. Las semi-pasivas, mientras tanto, usan batería para alimentar el microchip y la energía del lector para hacer la transmisión. Finalmente, las etiquetas activas emplean una batería capaz de alimentar tanto el microchip como la transmisión de la señal.[19]

[14] Ibidem, p. 101 (traducción informal).
[15] Ibidem.
[16] Sobre la conmutación de paquetes, ver Cortés, C. 'La neutralidad de la red: la tensión entre la no discriminación y la gestión' y 'Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet'. En: Internet y derechos humanos. Aportes para la discusión en América Latina. CELE, Universidad de Palermo, 2014.
[17] Cfr. Kellmereit, D., Obodovski,D. 'The Silent Intelligence - The Internet of Things'. DnD Ventures. 2013.
[18] Cfr. Finkenzeller, K. RFID Handbook. Fundamentals and applications in contactless smart cards and identification. John Wiley and Sons. Second Edition, 2003, p.7

Usualmente, las etiquetas RFID contienen datos sobre la identidad del objeto, conocida como código electrónico de producto (EPC, por su nombre en inglés). Así, es usual ver estas etiquetas en almacenes de cadena adheridas a ropa, juguetes o electrodomésticos. En ese contexto, cumplen una función similar, pero más sofisticada, que la del código de barras. La tecnología RFID se emplea también en industrias como la automotriz, donde es posible monitorear el progreso del ensamblaje de las partes; en la de alimentos, para monitorear inventarios, y en la farmacéutica, para identificar medicamentos y fechas de caducidad. Igualmente, las etiquetas RFID pueden 'inyectarse' en animales para efectos de identificación –recientemente, Eduardo Bertoni contaba sobre un proyecto en Argentina para monitorear el ganado en el país con propósitos tributarios–,[20] o adherirse a dispositivos médicos, como el marcapasos, para monitorear su funcionamiento y el estado de salud del paciente.

La tecnología RFID, sin embargo, no resulta suficiente para que los escenarios más ambiciosos del IoT sean una realidad. La Agenda Digital de la Unión Europea plantea el siguiente ejemplo del internet de las cosas: una persona ha sufrido un accidente en su automóvil y automáticamente se envía una alerta a un hospital cercano. Esta alerta, además, sirve como notificación para que los otros automóviles informen a sus conductores sobre el hecho y la necesidad de tomar una ruta alterna.[21]

Tal nivel de comunicación entre objetos no se lograría con etiquetas RFID, puesto que involucra acciones más complejas: el automóvil debe tener sensores para determinar su posición (giroscopios) y para darse cuenta de que se detuvo de manera abrupta (acelerómetros). También debe contar con alguna capacidad para conectarse a internet y enviar un mensaje de emergencia. De la misma forma, los automóviles que van en la vía deben poder recibir a través de internet la sugerencia de desvío, todo lo cual debe estar mediado por algún tipo de central de tráfico.

Esta situación plantea un contraste entre las etiquetas RFID y un 'objeto inteligente', que en últimas sería necesario para el IoT –al menos en los términos en que se vende comercialmente–. Para hablar de un internet de las cosas se requiere de objetos que puedan comunicarse entre sí, den cuenta de su entorno y, en ocasiones, actúen sobre él.[22] Un objeto es 'inteligente' dependiendo de sus niveles de (i) 'conciencia' sobre el ambiente, (ii) representación, que es la forma como se comporta, y (ii) capacidad de interacción con el usuario.[23] De allí se colige que un objeto con un sensor RFID adherido puede

---

[19] Cfr. Atzori, L., et al. The internet of things: A survey. Computer networks 54.15, 2010, p.2790.
[20] Bertoni, E. El derecho a la privacidad de las vacas. Agosto de 2014, Disponible en: http://ebertoni.blogspot.com/2014/07/el-derecho-la-privacidad-de-las-vacas.html (consultado el 4 de diciembre de 2014).
[21] Ejemplo tomado de Internet of Things Europe - Teaser N° 3: Traffic. por DigitalAgendaEU. Disponible en: https://www.youtube.com/watch?v=lkIXHzcU5XA (consultado el 30 de noviembre de 2014).
[22] Cfr. Vasseur, J.; Dunkels, A. 'Interconnecting smart objects with ip: The next internet'. Morgan Kaufmann, 2010.p.3-7. En el mismo sentido: Cristea, V., et al. 'Context-aware environments for the Internet of things'. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Springer Berlin Heidelberg, 2013. p. 26.
[23] Kortuem, Gerd, et al. "Smart objects as building blocks for the internet of things." Internet Computing, IEEE 14.1 (2010): p.45.

contener datos de manera descentralizada –siguiendo la idea del *everyware*–, pero no puede hacer parte de un entorno digital ubicuo.

Esto significa que si los 'objetos inteligentes' pretenden ser autónomos y realmente descentralizados, deberán tener la capacidad funcional para cumplir con los protocolos de la red. De lo contrario, serán simplemente apéndices de máquinas más grandes. Dicho de otra forma, el 'internet' en el internet de las cosas es el mismo que conocemos, y si los 'objetos inteligentes' van a hacer parte de esta red, tendrán que ser compatibles.[24] Jean-Phillipe Vasseur y Adam Dunkels consideran que por su flexibilidad, el protocolo TCP/IP es apropiado para una red de 'objetos inteligentes'. Mientras un protocolo semi-cerrado o propietario afectaría la escala de dispositivos conectados, el TCP/IP busca un 'óptimo global', es decir, una mayor compatibilidad e interconexión.

Para que una serie de datos puedan ir de un lugar a otro se requiere que tanto el receptor como el emisor estén identificados, y que esa identificación no se confunda con otras. El protocolo de internet (IP) cumple esa función al asignar direcciones únicas a cada uno de los nodos que se conectan a la red –ya sea un computador, un teléfono o un radio–. La versión 4 del protocolo de internet IP es la más extendida hoy (IPv4). Dado que su tamaño es de 32 bits,[25] permite unas 5.000 millones de direcciones únicas, que no son suficientes para los 50.000 millones de dispositivos que, según empresas como Cisco, estarán conectados a internet para 2020.[26] Por ello, se ha diseñado la versión 6 del protocolo (IPv6), que cuenta con un enorme número de direcciones, ya que su tamaño asciende a 128 bits.[27]

Si en gobernanza de internet se identificaba como un problema la gestión de recursos críticos de internet y, en especial, el agotamiento de direcciones IP –y por tanto la necesidad de hacer la transición de IPv4 a IPv6–, el internet de las cosas hace aún más patente esa necesidad.

Este no es el único escollo técnico que presenta el IoT. Alrededor de los propósitos de conectividad e interoperabilidad y de las capacidades de los dispositivos, se dan toda suerte de discusiones entre ingenieros. Por ejemplo, en una red de 'objetos inteligentes' el tráfico de datos tendrá que determinarse según la capacidad de los nodos, toda vez que las cosas conectadas no tendrán ni la memoria ni la energía de un computador tradicional. Igualmente, es necesario adoptar un protocolo de transporte de datos (TCP o UDP), y adoptar decisiones metodológicas para que los objetos puedan conectarse a la red. Hoy contamos protocolos como SLP, UPnP (*Universal Plug and Play*) y Zeroconf, que permiten que

[24] Cfr. Vasseur, J.; Dunkels, A. Interconnecting smart objects with ip: The next internet. Morgan Kaufmann, 2010.p.28.
Para una explicación sobre la arquitectura de internet, ver: Op. Cit. Cortés, C. 'La neutralidad de la red: la tensión entre la no discriminación y la gestión' y 'Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet'.
[25] Un bit es la unidad básica de información digital. Puede tener sólo uno de dos valores: 0 o 1. Cuando se habla de una dirección de 32 bits se hace referencia a su tamaño pues, en este caso, ella tiene 2^32 combinaciones diferentes posibles.
[26] IETF RFC791. http://tools.ietf.org/html/rfc791
[27] Cfr. Coffeen, Tom. IPv6 Address Planning. Designing and Address Plan for the Future. O'Reilly Media. 2014.

un periférico conectado a una red –una impresora, un control para juegos, un 'mouse'– sea reconocido inmediatamente y quede establecida la comunicación.

Por último, los 'objetos inteligentes' tendrán que cumplir ciertos requisitos de seguridad: confidencialidad de los datos que almacenan y envían, integridad de la información, protección del usuario legítimo y prevención de fraude. Una serie de riesgos que no distan demasiado de los que subsisten hoy en sistemas de información y computadores. A este punto nos referiremos brevemente en el siguiente capítulo.

4. El riesgo de un entorno digital omnipresente

Para no pocos críticos, la idea de tener objetos que registren y reporten todos nuestros movimientos y actividades constituye *"una irrupción tecnológica violenta en la vida cotidiana"*.[28] No hay que ir demasiado lejos para entender la preocupación: en la propia visión de una red omnipresente de objetos y dispositivos subyace un sistema robusto de vigilancia del individuo. No necesariamente uno público o arbitrario, pero aun así inquietante.

Sin tener que adentrarse en el terreno del internet de las cosas, esta pregunta subiste hoy en día en el entorno digital de computadores y teléfonos móviles. Con la tecnología de la que disponemos, es posible monitorear comunicaciones y movimientos en tiempo real. Por supuesto, en un contexto en el que todos los objetos almacenan datos sobre el individuo o que posibilitan su identificación o ubicación, la capacidad de vigilancia solo aumenta. De una parte, será más fácil monitorear y, de la otra, habrá más datos personales para procesar.

En muchos casos, el primer actor interesado en esa información será el Estado. "*Todos esos nuevos objetos en línea son un tesoro de datos si usted es una 'persona de interés' para la comunidad espía",* afirma David Petraeus, exdirector de la Agencia Central de Inteligencia de Estados Unidos. *"Con el surgimiento de la 'casa inteligente', cuando usted use en su 'smartphone' la aplicación para ajustar la luz de su sala, estará enviando datos etiquetados y geolocalizados que una agencia de espionaje podrá interceptar en tiempo real*".[29]

De la misma forma como hoy las conversaciones y los datos son interceptados, los objetos inteligentes de una casa, una ciudad o una fábrica serán usados como fuente de información. Y de la misma forma en que el IoT se acoplará a la vida cotidiana por su ubicuidad e invisibilidad, los esquemas de vigilancia terminarán siendo omnipresentes e imperceptibles. Lawrence Lessig hace un interesante paralelo entre las capacidades de vigilancia de las nuevas tecnologías y el referente paradigmático descrito en '1984', la novela distópica de George Orwell. Mientras que en este último existía la 'telepantalla', un aparato transparente e imperfecto por cuanto era posible saber en dónde y en qué condiciones observaba, los dispositivos conectados a internet ofrecen formas subrepticias de monitoreo y control.[30]

---

[28] Araya, A.A. 'Questioning Ubiquitous Computing'. En: Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science. ACM Press, 1995. Para consultar críticas similares, ver, Bohn, J, et al. 'Social, Economic, and Ethical Implications of Ambient Intelligence
and Ubiquitous Computing'. En: Weber W. Ambient Intelligence, Springer Berlin Heidelberg, 2005.

[29] Ackerman. S. `CIA Chief: We'll Spy on You Through Your Dishwasher´. En Wired, marzo de 2012. (traducción informal). Disponible en http://www.wired.com/2012/03/petraeus-tv-remote/ (consultado el 30 de noviembre de 2014).

La captura masiva de información personal en tiempos del IoT es distinta –y más preocupante– que la actual por varias razones: primero, se capturará información en muchos lugares más; segundo, el acopio será invisible; tercero, los datos serán más íntimos –qué, dónde, cuándo, cómo, con quién, por cuánto tiempo, por qué–, y cuarto, las facilidades de interconexión conllevarán a que nuestros datos sean compartidos en niveles nunca antes vistos.[31] Compárese, por ejemplo, la etiqueta RFID con el código de barras –su antecesor–: mientras el segundo contiene alguna información sobre el producto, la primera puede incluir datos personales e historiales de compra; mientras el segundo debe estar a la vista para capturar la información, la primera solo necesita de un lector a una distancia adecuada, y mientras el segundo requiere de algún nivel de interacción humana, la primera opera entre máquinas.

Asociada a la invasión de la privacidad –entendiéndola en un sentido que va más allá de la protección de un espacio íntimo– el IoT conlleva también un riesgo de normalización del individuo y de coerción de su autodeterminación. Para Greenfield, el éxito del *everyware* –que, recordemos, es esa intersección entre ubicuidad y cotidianidad– depende de que el ecosistema de objetos pueda moldearse a la vida de una persona de manera tal que interprete y distinga entre órdenes o simple ruido, entre acciones relevantes e irrelevantes.[32] En otras palabras, el IoT tiene que ser tan preciso y previsible como el algoritmo de un programa. ¿Qué nivel de autodeterminación y espontaneidad quedaría para el individuo?

Natasha Dow-Schüll, quien estudió la compleja relación entre los apostadores y las máquinas 'tragamonedas' en Las Vegas, plantea que los procesos de automatización en la relación individuo-máquina van desplazando el núcleo de control de la actividad –y por ende, la capacidad de acción–[33] del primero al segundo. La persona comienza a participar en acciones en las que responde automáticamente, perdiendo de alguna forma el sentido de sí misma.[34] Siguiendo esa línea, Bruce Sterling considera que en el IoT el usuario no decide ni entiende ni modifica; son las grandes empresas –cuyas prioridades son comerciales– las que determinan cómo y qué se conecta.[35]

Un ecosistema 'exitoso' de IoT podría desembocar entonces en lo que se conoce como una 'arquitectura de control', una configuración que define o moldea de manera muy detallada el tipo de conductas permitidas. Y aunque es posible que ese no sea el objetivo de muchos de sus proponentes, resulta claro que es útil para ese fin. Los sensores para identificar usuarios, bienes o servicios de

[30] Cfr. Lessig, L. 'On the Internet and the Benign Invasions of Nineteen Eighty-Four'. En: Gleason, A. et al (ed). On Nineteen Eighty-Four. Orwell and our Future. Princeton University Press, 2005.
[31] Cfr. Lahlou, S., et al. 'Privacy and trust issues with invisible computers'. En: Communications of the ACM 48.3, 2005, p.59.
[32] Cfr. Op. Cit. Greenfield.
[33] En inglés se usa el término 'agency'. Acá lo traducimos como capacidad de acción, a pesar de que el significado es un poco más complejo.
[34] Cfr. Dow-Schüll, N. Addiction by Design: Machine Gambling in Las Vegas. Princenton University Press, 2014.
[35] Cfr. Sterling, B. The Epic Struggle of the Internet of Things. Strelka Press, 2014.

ubicación, se prestan fácilmente para fines de control y supervisión.[36] Desde una perspectiva comercial, pueden ser herramientas ventajosas para el individuo; desde una perspectiva policial, se vuelven talanqueras, exclusas y cuellos de botella. Lessig considera que ante el control creciente en el entorno digital –invisible y preestablecido– el ser humano termina siguiendo un 'principio bovino': simplemente se ajusta a las cercas que ve, como las vacas.[37]

A continuación mencionamos más en detalle dos riesgos planteado acá entrelíneas: la acumulación masiva de información (el *big data*) y los riesgos de seguridad, inherentes a cualquier sistema de información y con opciones de escalar en el contexto del IoT.

a. 'Big data'

El *big data* es una herramienta que busca abarcar un conjunto de datos relevantes tan aproximado a la totalidad como sea posible. Es de alguna forma una paradoja: la captura y procesamiento de una infinidad de datos que se acerque al límite disponible. Su esencia se opone a una toma de muestra: el *big data* no analiza el préstamo de materiales de una biblioteca en particular, sino *todos* los préstamos, en todas las categorías y temas; no analiza un mensaje con palabras clave, sino que procesa *todo* el historial de conversaciones. Igualmente, para el *big data* lo relevante no es el porqué sino el qué. Averiguar por qué prolifera la gripa en ciertos lugares de un país es menos importante que detectar posibles casos de gripa a partir de búsquedas en Google.[38]

Para Kevin Ashton, el complemento entre el *big data* y el internet de las cosas es ideal: *"si tuviéramos computadores que supieran todo lo que hay que saber acerca de las cosas –usando datos que ellos mismos hayan recogido sin intervención humana– podríamos monitorear e inventariar todo y reducir significativamente las pérdidas, desperdicios y costos".*[39] Sin embargo, la relación entre los datos masivos y el IoT no es estructural. El primero no es consecuencia de lo segundo. El problema, nuevamente, es que un entorno ubicuo interconectado potenciaría el procesamiento de datos disponibles. Entre más objetos reciban y transmitan información, más profundo será el pozo de datos. Un riesgo que para Ashton es más bien una ventaja.

Las ventajas de analizar vastas cantidades de datos para encontrar patrones y tomar decisiones, son innegables. A través del *big data* las empresas cuentan con una base racional que les permite identificar individuos para categorizarlos en grupos con otros similares.[40] Así, pueden hacer ofertas diferenciadas, productos para nichos específicos o seguimientos a compras previas. Los efectos

[36] Cfr. Cohen, J. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press, 2012.
[37] Cfr. Op. Cit. Lessig.
[38] Cfr. Mayer-Schönberger, V.; Cukier, K. Big data. La revolución de los datos masivos. Ed. Turner. 2013.
[39] Op. Cit. Ashton, K. (traducción informal).
[40] Cfr. Barocas, S.; Selbst, A. 'Big Data's Disparate Impact'. SSRN 2477899, 2014. Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899 (consultado el 30 de noviembre de 2014).

benéficos no se quedarán solo en las empresas. Esta herramienta permitirá observar mejores correlaciones entre hábitos de consumo y efectos ambientales, lo que puede incentivar un consumo más consciente.[41]

En el área de la salud, por ejemplo, se prevé que el *big data* propiciará opciones de vida más saludables; permitirá proveer tratamientos más adecuados; orientará la selección del profesional con mejores capacidades para atender un caso; racionalizará los costos del sistema de salud, y permitirá una mayor innovación en los servicios.[42]

No obstante, esta amplia oferta informativa, sumada a la vulnerabilidad de las bases de datos –piénsese en contexto frágiles como los latinoamericanos– y a decisiones arbitrarias y erróneas, puede desembocar en violaciones a la privacidad y en prácticas discriminatorias.

Uno de los ejemplos más documentados frente a este problema está en los datos masivos y la información financiera. Con datos crediticios, antecedentes personales, ubicación geográfica e información de redes sociales, los bancos han lanzado productos bancarios que terminan por segregar ciertos grupos –afroamericanos, concretamente– o han calificado la calidad de un cliente a partir de inferencias equivocadas (si vive en cierta zona, frecuenta ciertos lugares o usa cierto lenguaje, puede no ser confiable).[43]

Dichas conclusiones son el resultado de una combinación algorítmica, pero su fundamento es una decisión humana, con lo cual el error se sistematiza y el análisis sesgado del *big data* se perpetúa. Por ejemplo, volviendo al tema de salud, en el Saint George's Hospital Medical School de Londres se creó un programa para seleccionar aspirantes laborales basándose en un modelo de análisis de aplicaciones decididas favorablemente en el pasado. Posteriormente, la Comisión de Igualdad Racial encontró que al menos 60 de las 2.000 aplicaciones que se presentaban anualmente se habían rechazado por razones de género. A la postre, el programa simplemente replicaba las decisiones discriminatorias de quienes habían llevado a cabo los procesos de selección en el pasado, cuyos datos definieron los criterios para modelar el programa.[44]

Aunque planteábamos al comienzo que el *big data* no es un efecto atribuible únicamente al internet de las cosas, sí existe una complementariedad que puede potenciar, en particular, el riesgo de discriminación. A medida que la información personal se acumule –financiera, social, económica– y se ate a ubicaciones y

[41] Anderson, J , Rainie, L. `The Future of Big Data' en Pew Research Center's Internet & American Life Project, julio de 2012. Disponible en: http://www.pewinternet.org/2012/07/20/the-future-of-big-data/ (consultado el 30 de noviembre de 2014).
[42] Groves, P. et al. `The `big data' revolution in healthcare: accelerating value and innovation'. McKinsey & Company. 2013.
[43] Cfr. Peña, S. 'The Dangers of High-Tech Profiling Using Big Data'. En: New York Times, 7 de agosto de 2014. Disponible en: http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/the-dangers-of-high-tech-profiling-using-big-data (consultado el 26 de noviembre de 2014).

accesos en una ciudad o lugar, surgirán esquemas de restricciones, como si se tratara de un gigantesco club social donde la gente tiene permiso para moverse a partir de los privilegios que tenga. Estos 'regímenes de autenticación', donde cada acción debe estar previamente validada, no podrán ser cuestionados por el individuo, toda vez que estarán incrustados en los objetos.[45]

b. Seguridad

La seguridad de un sistema depende de su capacidad para, por un lado, responder a ataques externos y, por el otro, evitar daños al ambiente o a las personas.[46] En inglés se ha habla de *secure* y *safe* que, si bien en español sólo encuentran traducción en la palabra 'seguro', hacen alusión a dos formas distintas de seguridad. Para Dunkel y Vasseur, entretanto, la seguridad es confidencialidad, integridad y disponibilidad.[47]

En todos los elementos del internet de las cosas –objetos, sensores, actuadores y conectores– hay puntos de vulnerabilidad, y en cada caso la virtud de automatización es a la vez un talón de Aquiles. Las etiquetas RFID –que son por ahora la tecnología principal de identificación– sirven como ejemplo: teniendo en cuenta que se trata de identificadores únicos que pueden ser leídos sin intervención humana, un dispositivo no autorizado puede 'escanear' los datos allí contenidos. De la misma forma, podría falsificarse una etiqueta RFID o engañar de otra forma al dispositivo-lector para que, por ejemplo, registre equivocadamente la salida o entrada de un producto en un inventario. En pocas palabras, los problemas pueden surgir por etiquetas auténticas que son registradas por lectores clandestinos o por etiquetas falsas que, de una u otra forma, engañan a lectores legítimos[48].

La lista de problemas de estas etiquetas no termina ahí. También es posible bloquear un lector legítimo exponiéndolo a una cantidad tal de etiquetas que no pueda procesar ninguna –similar a un ataque de denegación de servicio *DDoS* en internet–;[49] se puede generar interferencia en el espectro electromagnético de modo que no pueda leerse ninguna etiqueta; se puede obtener información ilegítimamente empleando intermediarios clandestinos, o un lector clandestino puede monitorear la comunicación entre etiquetas y lectores legítimos.[50]

---

[44] Cfr. Lowry, S.; Macpherson, G. 'A blot on the profession'. British medical journal (Clinical research ed.) 296.6623, 1988.
[45] Cfr. Op. Cit. Greenfield, A. Para más información sobre los 'regímenes de autenticación', ver Op. Cit., Cohen, J.
[46] Cfr. Axelrod Warren, C. Engineering Safe and Secure Software Systems. Artech House, 2012.
[47] Cfr. Vasseur, J.; Dunkels, A.
[48] Cfr. Juels, A. RFID security and privacy: A research survey. Selected Areas in Communications, IEEE Journal on, 24(2), 2006, p.384.
[49] El DDoS es un ataque con el propósito de que una máquina o recurso de red quede indisponible para sus usuarios. Los métodos varían, pero en general el ataque consiste en hacer miles de solicitudes simultáneas a un servidor o servicio, desbordando la capacidad de la máquina de atenderlos o procesarlos.
[50] Cfr. Khoo, Benjamin. 'RFID as an enabler of the internet of things: issues of security and privacy'. En: Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011.

Una vez capturados los datos de la etiqueta, se abren todos los problemas de seguridad y privacidad.[51] Una lectura de los objetos que carga una persona pueden dar mucha información sobre ella: entre otros, los objetos que lleva consigo, sus afinidades –libros, música– o su estado de salud –medicinas o fórmulas médicas–. Así mismo, a través de las etiquetas sería posible seguir los movimientos de alguien.[52]

No obstante, como veíamos en el capítulo anterior, el IoT prometido está compuesto por 'objetos inteligentes' conectados entre sí y a internet. En esa línea, la presencia en red de cualquier cosa, en cualquier parte, en cualquier momento, multiplicará los puntos de entrada y salida de información y, por lo tanto, aumentará el riesgo. La heterogeneidad de los objetos conectados también ofrecerá niveles distintos de fragilidad. En otras palabras, no habrá soluciones que se ajusten –literalmente– a todos los tamaños del riesgo.[53]

Muchos de los ejemplos del peligro que representan los objetos conectados a internet suelen ser apocalípticos, tan radicales como los que desde la orilla opuesta se proponen como el idilio del IoT. No obstante, en algunos de ellos es posible entrever el reto que enfrenta la industria, los gobiernos y la sociedad civil en este proyecto.

En 2013, Dick Cheney, exvicepresidente de la administración de George W. Bush, contó a la prensa que sus médicos le habían recomendado desactivar la funcionalidad inalámbrica de su marcapasos después de haber estudiado las posibilidades de que el dispositivo fuera accedido subrepticiamente para tomar control de él y quizás causarle la muerte.[54]

Barnaby Jack, el experto en seguridad que probó la posibilidad de que ese tipo de ataque ocurriera, había logrado también en otra ocasión que un cajero automático expulsara billetes de manera ininterrumpida. Igualmente, había 'hackeado' una bomba de insulina para que hiciera una descarga letal del medicamento.[55] *"Si se puede acceder remotamente al dispositivo siempre habrá posibilidades de abusar de él"*, dijo en una entrevista.[56]

[51] Medaglia, Carlo Maria, and Alexandru Serbanati. "An overview of privacy and security issues in the internet of things." The Internet of Things. Springer New York, 2010. p.391.
[52] Cfr. Weber, Rolf H. "Internet of Things–New security and privacy challenges." Computer Law & Security Review 26.1 (2010). p.24.
[53] Cfr. Roman, R. et al. 'On the features and challenges of security and privacy in distributed internet of things'. Computer Networks 57.10, 2013.
[54] The Washington Post. 'Yes, terrorists could have hacked Dick Cheney's heart'. Octubre de 2013, disponible en: http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ (consultado el 30 de noviembre de 2014).
[55] Cfr. CSO. Lethal medical device hack taken to next level. Disponible en: http://www.cso.com.au/article/404909/lethal_medical_device_hack_taken_next_level/ (consultado el 30 de noviembre de 2014).
[56] Cfr. Alexander, W. 'Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode'. Vice. Disponible en: http://www.vice.com/read/i-worked-out-how-to-remotely-weaponise-a-pacemaker (consultado el 30 de noviembre de 2014).

Otro ejemplo interesante se dio en 2010, cuando se descubrió un virus informático –'Stuxnet'– que por cerca de dos años había pasado desapercibido para las empresas de seguridad. Éste se propagaba a través de memorias externas USB, y tenía el objetivo de infectar los computadores que controlaban ciertas centrífugas utilizadas en el proceso de enriquecimiento de uranio. Como la mayoría de ataques parecían ocurrir en una planta nuclear cerca a la ciudad de Natanz, en Irán, se entendió que el propósito del virus era sabotear el programa de energía nuclear de este país.[57] El caso no solo quedó como antecedente de la guerra digital entre potencias; un virus con tal capacidad de camuflaje y expansión podría fácilmente tomar control de redes completas de objetos y dispositivos. Este tipo de virus está apenas emergiendo. Recientemente, se descubrió 'Regin', tan complejo y sofisticado como 'Stuxnet', aunque orientado al robo de datos y espionaje. Aún es materia de investigación.[58]

En conclusión, cualquier cosa conectada a la red puede ser accedida clandestinamente y obligada a actuar de forma impredecible y dañina. Por supuesto, las consecuencias y dimensiones del daño que provoque la manipulación de cada dispositivo dependerán de sus funciones. Por eso, Adam Greenfield propone que los *"sistemas ubicuos tengan por defecto un modo de configuración que asegure la seguridad física, psíquica y financiera del usuario"*.[59] Enunciada en teoría, la idea parece sensata, pero su aplicación práctica es a todas luces un reto aparte.

[57] Zetter, K. 'Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon'. Crown Publishing Group, 2014.
[58] Cfr. Marquis-Boire et al. Secret malware in European Union attack linked to U.S. and british intelligence. En The Intercept, noviembre de 2014. Disponible en https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/ (consultado el 30 de noviembre de 2014).
[59] Op. Cit. Greenfield, p. 500 (traducción informal).

5. Conclusiones

Buena parte de la bibliografía que encontramos sobre internet de las cosas está relacionada con su futuro, sus posibilidades y el valor en el mercado de uno u otro servicio.[60] Y, como se planteó a lo largo de este documento, no se trata de un área de estudio en tecnología o ingeniería, sino de una sumatoria de cosas con el antecedente común de la computación ubicua y un presente ineludiblemente atado a internet. Esto abre de entrada un camino de trabajo para quienes quieran ahondar en el tema. Partiendo de ese supuesto central, hacemos las siguientes conclusiones y recomendaciones:

- Los riesgos en materia de privacidad, seguridad y autonomía que surgen en el IoT no son distintos a los que encontramos asociados hoy al entorno digital en general. Si hubiera que plantear alguna diferencia, ésta reside en la escala: en un contexto de IoT, estos riesgos parecen acentuarse.

- Entre todos los problemas identificados, el de privacidad –en el sentido planteado en este documento– parece el más grave. Pensada desde el diseño y la ingeniería –y con una veta claramente comercial– el IoT no incorpora un análisis sobre este punto, a pesar de que la 'privacidad por diseño' o, dicho de otra forma, la inclusión de la privacidad en las arquitecturas y los dispositivos, no es un tema nuevo en el debate sobre tecnología y regulación.

- En un contexto como el latinoamericano, donde los esquemas de identificación son generalizados, la idea del IoT puede desembocar fácilmente en formas de discriminación y profundización de la brecha digital. Tal y como se presenta, los dispositivos y servicios asociados al IoT harán parte de ofertas comerciales que solo un sector de la población podrá pagar.[61]

- La decisión sobre estándares técnicos para conectar objetos a la red está relacionada con la gobernanza de internet. En particular, con la gestión de los recursos críticos. En consecuencia, resulta relevante que en esos escenarios se haga seguimiento al proyecto del IoT, aterrizado en su real dimensión, como lo propone este documento.

[60] Cfr. Kellmereit, D., Obodovski,D. 'The Silent Intelligence - The Internet of Things'. DnD Ventures. 2013.; Gartner. 'Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business'. Agosto de 2014. Disponible en http://www.gartner.com/newsroom/id/2819918 (consultado el 30 de noviembre de 2014).; Press, G. 'Internet of Things By The Numbers: Market Estimates And Forecasts' En Forbes, agosto de 2014. Disponible en http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/ (consultado el 30 de noviembre de 2014).; Greenough, J. 'The 'Internet of Things' Will Be The World's Most Massive Device Market And Save Companies Billions Of Dollars'. En Business Insider, noviembre de 2014. Disponible en http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10 (consultado el 30 de noviembre de 2014).

[61] Cfr. Bohn, J. et al. 'Social, economic, and ethical implications of ambient intelligence and ubiquitous computing'. Ambient intelligence. Springer Berlin Heidelberg, 2005.

- Un escenario futuro de millones de dispositivos conectados a la red implicará una explosión exponencial del tráfico. Según el reporte anual de Cisco, en 2018 el 50% de todas las conexiones provendrán de un dispositivo móvil. Además, se multiplicarán 11 veces las conexiones existentes entre máquinas.[62] Es decir, darán cuenta de un 3% del tráfico en internet. Si esta realidad es desafiante para Estados Unidos o Europa, es abrumadora para los países de la región. Así, cualquier discusión sobre IoT debe tener en cuenta los retos que aún subsisten en infraestructura y acceso a internet.

- Donde la sociedad está organizada alrededor de la tecnología, el poder tecnológico es la principal forma de poder.[63] Un entorno digital conectado y omnipresente va más allá de los servicios y funciones que ofrece. La configuración de una arquitectura es el resultado de configuraciones de poder que a su vez lo distribuyen y reproducen. Esto implica aproximarse críticamente al proyecto comercial del IoT, sin desconocer sus virtudes y sin desestimar sus problemas.

- Para la sociedad civil resulta fundamental abrir espacios de interlocución para participar en este tipo de discusiones. Desde la perspectiva de la industria, es difícil tomar en cuenta posibles externalidades, en términos de derechos fundamentales, que traigan tecnologías omnipresentes. En cambio, las organizaciones, centros de pensamiento, universidades y grupos ciudadanos, pueden ofrecer una perspectiva distinta.

[62] Cisco. 'Cisco Virtual Network Index'. Disponible en http://share.cisco.com/vni14/ (consultado el 30 de noviembre de 2014).
[63] Cfr. Feenberg, A. Between Reason and Experience: Essays in Technology and Modernity, p. 80.