Internet de las Cosas

Secretaría de Regulación de Tecnologías de la Información y las Comunicaciones

Introducción

Desde la Secretaría de Regulación de Tecnologías de la Información y las Comunicaciones del Ministerio de Comunicaciones analizamos las nuevas tendencias en las TICs y sus implicancias, con el objetivo último de ser engranajes en su desarrollo, cuando éstas puedan constituirse en beneficiosas para nuestro país y sus ciudadanos.

Consideramos que Internet es la expresión más acabada del nuevo paradigma de la sociedad de la información, así como del desarrollo de nuevos procesos tecnológicos y económicos y de producción de bienes y servicios que han resultado en la denominada Economía Digital.

Creemos que en los casos de tratarse de aspectos innovadores, complejos y dinámicos, es oportuno propiciar un espacio para el diálogo de todas las partes interesadas, promoviendo la participación de la comunidad técnica y académica, el sector privado y las organizaciones de la sociedad civil, en un marco institucional oficial, para que realicen sus aportes con la finalidad de lograr una visión amplia y participativa sobre las cuestiones objeto de estudio.

En este sentido, mediante la Resolución 8/2016, esta Secretaría creó el Grupo de Trabajo de Servicios de Internet, cuyo objeto es analizar y proponer políticas públicas y regulaciones para la promoción y el desarrollo de servicios de Internet. Este grupo lleva adelante reuniones abiertas y consultas públicas para nutrirse de las experiencias, mejores prácticas y opiniones de todos los sectores de la sociedad.

Entendemos que Internet de las Cosas está llamada a transformar las dinámicas de consumo, los procesos productivos, las cadenas de valor en todas las industrias y, en definitiva, la forma de relacionarnos con lo que nos rodea, por tal motivo generamos este documento de entendimiento inicial, que servirá de base para el trabajo posterior del Grupo de Trabajo de Servicios de Internet.

¿Qué entendemos por Internet de las cosas?

Definición

Internet de las cosas, IdC, *Internet of Things* o *IoT* por sus siglas en inglés, es un concepto abstracto. De su nombre se desprende el concepto de cosas cotidianas que se conectan a Internet, pero en realidad se trata de mucho más que eso. IoT potencia objetos que antiguamente se conectaban mediante circuito cerrado, como comunicadores, cámaras, sensores, y demás, y les permite comunicarse globalmente mediante el uso de la red de redes.

Una posible definición de IoT es considerarla una red que interconecta objetos físicos valiéndose de Internet. Tales dispositivos utilizan software embebido, que le permite no solo la conectividad a Internet, sino que además programa eventos específicos en función de las tareas que le sean dictadas remotamente. En resumen, se trata de la interconexión digital de los objetos.

En tal sentido, la recomendación ITU Y.6060 de la Unión Internacional de Telecomunicaciones manifiesta que "...IoT puede ser considerada una infraestructura global para la sociedad de la información, permitiendo servicios avanzados para interconectar (física y virtualmente) cosas, basadas en tecnologías de la información y las comunicaciones interoperables. A través de la identificación, captura de datos, capacidades de comunicaciones y procesamiento, IoT hace un uso integral de las cosas para ofrecer servicios para todo tipo de aplicaciones mientras asegura que los requisitos de seguridad y privacidad sean cumplimentados".

Características

IoT consiste en de chips y circuitos que cuentan con todas las herramientas necesarias para cumplir tareas muy específicas. Cada uno de los objetos conectados a Internet tiene una IP específica y mediante esa IP puede ser accedido para recibir instrucciones. Asimismo, puede contactarse con un servidor externo y enviar los datos que recoja.

En este sentido, las principales características de IoT son:

- **Interconectividad:** Cualquier cosa se puede interconectar con la infraestructura global de TICs.
- **Servicios relacionados con las cosas:** IoT es capaz de proveer servicios relacionados con objetos sin los propios constreñimientos de las cosas, como la consistencia semántica entre las cosas *físicas* y las cosas asociadas a ellas virtualmente.
- **Heterogeneidad:** los dispositivos IoT son heterogéneos al estar basados en hardwares muy variados de plataformas y redes, y a su vez pueden interactuar con otros dispositivos o servicios

en otras plataformas o redes.

- **Cambios dinámicos:** el estado de los dispositivos cambia muy dinámicamente, generalmente de acuerdo al usuario. Por ejemplo, de dormir a despertarse, conectado o desconectado, y también de acuerdo al contexto y velocidad necesarias.

Tendencias de uso

El sector privado es aquel donde IoT se está haciendo cada vez más popular. Entre los sectores empresarios que están haciendo uso de este nuevo fenómeno, se pueden mencionar:

- **La industria de producción en masa:** la maquinaria que se encarga de controlar los procesos de fabricación, robots ensambladores, sensores de temperatura, control de producción, etc.
- **Control de infraestructura urbana:** control de semáforos, puentes, vías de tren, cámaras urbanas.
- **Control ambiental:** sensores atmosféricos, meteorológicos, sísmicos, etc.
- **Sector salud:** monitoreo activo de pacientes de manera ambulatoria y no invasiva.
- **Transporte:** seguimiento satelital, control del estado de los automotores, autos conectados, etc.
- **Industria energética:** Smart Grid, una solución para gestionar la demanda de electricidad e integrar fuentes de energía renovables, mejorar el servicio al cliente y reducir el consumo energético.

El gran pendiente al momento es el mercado de consumo, es decir, los hogares, pero poco a poco surgen dispositivos como lámparas, cerraduras, termostatos, etc.

Desafíos

La interconexión digital de los objetos, representa una gran oportunidad y a la vez una importante amenaza, especialmente para regiones en desarrollo como América Latina, donde persiste una marcada brecha digital (solo el 53% de los latinoamericanos son usuarios de Internet).

El despliegue de sistemas basados en IoT, y su potencial impacto en los usuarios y negocios, tiene implicancias regulatorias, algunas más relacionadas con las funciones de reguladores de telecomunicaciones y otras relativas a protección de datos, seguridad y privacidad.

En relación a esto, pueden distinguirse dos posturas: una que dice que regulación específica de IoT es necesaria para construir confianza pública y asegurar competitividad. Esta postura suele estar apoyada por académicos y la sociedad civil, así como grupos de usuarios. Por el contrario, una segunda posición sostiene que regular de modo específico IoT sería prematuro para un sector tan joven, y que las reglas generales aplicables de regulación de telecomunicaciones y privacidad son aplicables.

En los siguientes párrafos se describen algunos de los desafíos que se plantean para el desarrollo y adopción de sistemas de IoT a los fines de maximizar sus beneficios sociales.

Licencias y espectro

El otorgamiento de licencias y la gestión del espectro son un asunto importante para asegurar la disponibilidad y capacidad de las comunicaciones de IoT. Los dispositivos de IoT se comunican utilizando un rango amplio de protocolos, basados en requerimientos de conectividad y limitaciones de recursos. Estos incluyen protocolos de radio de corto alcance como ZigBee, Bluetooth y Wi-Fi, redes de datos móviles y aplicaciones especializadas como infraestructura de datos y protocolos de radio de largo alcance como Ultra-Narrow Band.

Para comunicarse con redes remotas, los dispositivos de IoT podrán enviar datos por medio de un puerto con una conexión móvil o fija a la red telefónica o de Internet. Para los consumidores, dicho puerto será usualmente un router doméstico o un smartphone, mientras que para las empresas probablemente sea su red corporativa. Los dispositivos que se comunican a grandes distancias necesitan acceso al espectro dentro del rango 300 MHz a 3GHz, mientras que las conexiones cercanas pueden usar comunicaciones en la frecuencia de 13 MHz o bandas EHF. Algunas aplicaciones de IoT también pueden usar bandas AM/FM en el rango VHF.

Para todo ello, los reguladores necesitarán prestar atención continua a la disponibilidad de espectro para comunicaciones de corto alcance, y la capacidad de las redes que conectan puertos de IoT a Internet, así como estimular la puesta en marcha de la tecnología de células pequeñas como el 4G.

La FCC de Estados Unidos también está revisando el uso de espectro por arriba de los 25 GHz

para redes de 5G y, posiblemente, para IoT. Por su parte, el gobierno de Corea del Sur planea asegurar frecuencias adicionales de al menos 1 GHz en 2024 y asegurar que el 5G sea comercializado a partir de 2020 en respuesta al crecimiento exponencial que se espera de tráfico de IoT.

En lo que refiere a licencias, estudios de la UE recomiendan que un modelo de exención de licencias es el más efectivo para el desarrollo de IoT, dado que evita la necesidad de negociaciones contractuales antes de que los dispositivos sean utilizados y manufacturados, permitiendo así la producción de numerosos dispositivos a bajos costos. La mayoría de los sistemas utilizan la exención de licencias para frecuencias en las bandas Industrial, Científica y Médica, incluyendo la sub-kHz para videovigilancia y control de acceso. Por ejemplo, los Servicios de Comunicaciones de Implantes Médicos operan en la banda de 400 MHz y 900 MHz para el estándar RFID. Los estándares de Bluetooth, ZigBee y Wi-Fi operan también en espectro sin licencia.

Conmutación y roaming

Las empresas que operan grandes redes de dispositivos *machine-to-machine* vía redes de telefonía móvil, con una tarjeta SIM fija a cada dispositivo, pueden encontrar no muy sencillo el cambiar de operador al final de un contrato, o si un dispositivo itinera hacia una red local diferente por determinado período puede ser que obtenga un mejor servicio de otro operador. Esta capacidad de itinerar es importante para los dispositivos que se mueven entre países, y también para dispositivos con una localización fija que puedan ser usados en áreas con períodos de no disponibilidad de servicios.

Se han llevado a cabo tareas de estandarización técnica para permitir dichos servicios. Los primeros pasos en esa dirección fueron tomados en los Países Bajos, que en 2014 permitieron que las tarjetas SIMs fueran entregadas por entidades que no fueren operadores de redes móviles, tales como empresas de servicios públicos y de autos. Asimismo GSMA ha desarrollado estándares para la gestión de dispositivos *machine-to-machine*, que están siendo apoyados por operadores móviles tales como China Unicorn y Telefónica.

En tal sentido, mayor flexibilidad y competencia serían posible si grandes operadores de IoT fueren capaces de actuar de modo similar a operadores móviles virtuales, lo cual no es menor ya que entonces podrían tener acceso a las redes móviles al por mayor. En tal sentido, un analista de la OECD estimó que si los fabricadores de autos alemanes tuviesen autorización para comercializar o entregar sus propias tarjetas SIM y rentar capacidad sobrante en redes móviles, podrían ahorrarse unos U$D 2.5 billones por año a través de menores precios y contratos más flexibles. Por otro lado, el regulador belga de comunicaciones también ha empezado a planificar un plan nacional de numeración a tales fines.

Por su lado, la Conferencia Europea de Administraciones Postales y de Telecomunicaciones, por medio de su Comité de Comunicaciones Electrónicas, ha recomendado que los SIMs cuyo IMSI puede ser actualizado remotamente deberían ser implementados lo más pronto posible, mientras que los Estados miembros consideran que hay mayor flexibilidad en la asignación de Códigos de Red

Móvil para proveedores de servicios de IoT. En tal sentido, han solicitado al Sector de Normalización de la ITU que reconsidere actualizar la Recomendación E.212 para que explicitamente autorice esta flexibilidad, así como planificar el futuro uno de Códigos de Red Móvil para apoyar un mayor rango de servicios de IoT. Estos cambios están en este momento bajo consideración del Grupo de Estudio ITU-T 2.

Direcciones y numeración

Los dispositivos de IoT requieren una dirección de comunicaciones única y enrutable (que requiere un protocolo amplio de direcciones, tales como IPv6); y una dirección asignada que permite conexión interredes limitada; o requieren hacer uso de redes locales únicamente, para compartir datos con otros dispositivos y recibir instrucciones de un controlador cercano, como una computadora personal o un smartphone, en cuyo caso una dirección globalmente única no es requerida.

Permitir conexiones P2P entre dispositivos puede aumentar la fiabilidad de las comunicaciones, en relación a las comunicaciones necesarias con una red global grande y compleja, lo cual coincide con el caso de uso común de un descubrimiento individual y la interacción con dispositivos cercanos. Pero cuando los dispositivos deben ser globalmente accesibles -posiblemente, a través de Internet- se requiere espacio de direcciones de gran tamaño para identificar individualmente a cada uno.

El número de direcciones no asignadas para la versión actual del protocolo de Internet (IPv4) es extremadamente limitado, pero la nueva versión (IPv6) que se está desplegando en todo el mundo tiene suficientes direcciones para casi cualquier número concebible de dispositivos. La transición de IPv4 a IPv6 ha tardado más de lo esperado, y son necesario programas para fomentar la transición en el mediano plazo. El gobierno de Estados Unidos, por ejemplo, llevó a cabo una puesta para mover todas las agencias federales de IPv4 a IPv6, con el único objetivo es alentar al sector privado a hacer lo mismo. Muchos otros países han puesto en marcha también Task Force IPv6 para estimular el transiciones nacionales.

Defensa de la competencia

Las tecnologías IoT probablemente tengan una serie de impactos sobre la competitividad de los diferentes mercados. En el corto plazo, las empresas que adopten sistemas de IoT tendrán mejor información sobre sus procesos de negocio, lo que permite un aumento en la eficiencia y las respuestas más flexibles para el suministro, procesamiento y las demandas. Esto podría fortalecer la posición de mercado de las empresas más grandes, las que tienen un mayor acceso al capital (para construir su propia infraestructura de IoT) o lealtad a la marca (para aumentar el volumen de ventas en pos de cubrir el precio de los servicios IoT de terceros). Para los productos con efectos en la red (aquellos cuya compra aumenta su valor para los compradores existentes - por ejemplo, el servicio

telefónico, donde un nuevo cliente puede llamar y ser llamado por todos los existentes clientes), los mayores volúmenes de ventas pueden aumentar la probabilidad de que los consumidores se encuentren “enjaulados” en los proveedores existentes -especialmente si el proveedor utiliza interfaces no-estándar y vende servicios complementarios-.

Con el tiempo, si la tecnología IoT es adoptada de modo que que se requiera un elevado gasto de capital, aumentará el poder de fijación de precios de las empresas, o se reforzarán los efectos de red, entonces esto puede generar la expulsión de los competidores. La estructura del mercado también se verá afectada si las grandes empresas pueden construir sus propios sistemas IoT, ya que las empresas más pequeñas tienen que suscribirse a ellos, o conectarse a las redes de las empresas más grandes. Si el "núcleo" de las grandes empresas adopta IoT, esto podría aumentar la competencia entre ellos, mientras que se reduce la competencia entre las empresas centrales y periféricas. Los consumidores se podrían ver beneficiados si la competencia pasa de basarse en precios a basarse en la calidad. Pero si las empresas adoptan IoT porque los competidores cuentan con la tecnología ¿Puede esto conducir a un exceso de inversión de las empresas ya establecidas y la reducción de la entrada en esos mercados a empresas no aptas para llevar a cabo esa inversión?

Un aspecto importante que afecta a la competitividad de los sistemas IoT en el largo plazo es el grado en el que los usuarios finales pueden acceder a los datos recogidos y almacenados por los componentes. Si bien la tecnología IoT hace que los sistemas sean más fáciles de usar, esto reduce la capacidad de los usuarios de transferir información a diferentes proveedores si un mejor sistema es ofrecido. También es difícil para los usuarios finales combinar los sistemas de diferentes proveedores -lo que podría convertirse en un problema de competencia si el proveedor comienza a ser dominante en un área, y trata de extender el dominio en otras áreas mediante el bloqueo de la interoperabilidad con los sistemas de la competencia-.

Un ejemplo de actividad reguladora para promover la competencia es Corea del Sur, donde existe una Estrategia del Consejo de Telecomunicaciones por medio de la que se le ha otorgado la responsabilidad de adaptar leyes y reglamentos vigentes para asegurar un ambiente competitivo liberal e industrial vinculado a IoT.

En esta etapa relativamente temprana de desarrollo del mercado de IoT, no está claro si se apoyará en "más que un número relativamente pequeño de grandes jugadores", como es el caso con los actuales mercados de Internet vinculados a búsqueda y publicidad. Reguladores de la competencia tendrán que estar atentos a verificar si la revisión *ex-post* de abuso de posición dominante será suficiente para fomentar el mercado competitivo y la rápida innovación, incluyendo la capacidad de empresas nuevas y empresarios individuales para crear nuevos productos y servicios.

Seguridad

Sin seguridad adecuada, los intrusos pueden entrar en los sistemas y redes IoT, acceder a información personal potencialmente sensible acerca de los usuarios, y hacer uso de las

vulnerabilidades de dispositivos para atacar redes y dispositivos locales. Esto es de particular relevancia cuando los dispositivos se utilizan en espacios privados, como los hogares de los individuos, por ejemplo, los monitores de bebés. Los operadores de sistemas de IoT , y otros con acceso autorizado a los datos producidos, están también en condiciones de "recopilar, analizar y actuar sobre grandes cantidades de datos dentro de los espacios privados tradicionales”

Por su parte, ataques electrónicos podrían también conducir a amenazas a la seguridad física, por ejemplo, si se realiza contra dispositivos médicos como marcapasos y bombas de insulina, o motores de automóviles y frenos. Información sobre la ocupación del edificio podría ser utilizado por los ladrones para dirigirse a locales desocupados, mientras que los datos de seguimiento de ubicación podrían permitir ataques físicos contra individuos específicos. Si los dispositivos IoT comprometidos pueden conectarse a los sistemas de otros lugares en Internet, esto proporciona la ruta potencial para nuevos ataques.

Otra cuestión común de seguridad es el uso de contraseñas por defecto en los dispositivos, esto es, el hecho de que los usuarios no están obligados a cambiar la configuración del dispositivo. Una página web anunció haber encontrado 73.000 webcams accesibles a través de Internet utilizando una contraseña por defecto y conocida. En este sentido, dispositivos IoT pueden ser más difíciles de asegurar que las computadoras personales. A menudo los dispositivos IoT son de bajo costo, lo que pone una fuerte presión sobre los costos de seguridad y hardware adicional o software para hacer frente a amenazas. En combinación con la conectividad a Internet limitada de algunos dispositivos, esto puede hacer que sea más difícil de desarrollar y aplicar los parches de seguridad cuando regularmente se descubren vulnerabilidades. La mayoría de los dispositivos IoT contienen equipos polivalentes y pueden ser reprogramados más allá del propósito previsto. Los dispositivos IoT con frecuencia comparten sistemas operativos, chips integrados y drivers, lo que significa que una sola vulnerabilidad puede ser utilizada para atacar una amplia variedad de dispositivos.

En los grandes sistemas de IoT, tales como ciudades inteligentes (*smart cities*), la inseguridad de IoT puede crear vulnerabilidades significativas, y ser extremadamente complejo direccionar interdependencias y vínculos del sistema público y sector privado.

Una evaluación de amenazas en el 2014 encontró 200.000 vulnerabilidades a los sensores de control de tráfico en ciudades como Washington DC, Nueva York, Seattle, San Francisco, Londres, Lyon, y Melbourne. La evaluación también encontró que dichas tecnologías vulnerables están siendo desarrolladas y utilizadas en infraestructura crítica sin un control de seguridad y que puede ser difícil para investigadores terceros conseguir acceso a los dispositivos para llevar adelante su propio control, debido a los costos y límites en ventas para los gobiernos y compañías específicas.

Las empresas que desarrollan y operan sistemas IoT necesitarán llevar a cabo pruebas de seguridad y considerar cómo las vulnerabilidades de seguridad descubiertas después de que los dispositivos son vendidos pueden solucionarse durante la probable vida útil del dispositivo. En caso de que las fallas de seguridad causen daño al consumidor, las agencias de protección del consumidor pueden ser capaces de tomar medidas para requerir remediar estos daños y mejorar los procesos de seguridad para reducir el riesgo en la ocurrencia nuevamente del hecho.

Las reglas de UE requieren que las organizaciones que traten datos personales en los sistemas IoT lleven a cabo evaluaciones de seguridad como así también hacer uso de las certificaciones de seguridad pertinentes y standards. Además, las compañías necesitan garantizarlo cuando utilicen proveedores de servicios externos para gestionar los dispositivos y los datos de IoT, en este sentido, aquellos proveedores también deben tomar razonables precauciones de seguridad.

Para hacer frente a estos retos de seguridad y privacidad, los reguladores han sugerido que las empresas desarrolladoras de dispositivos IoT deberían cumplir con la seguridad y privacidad desde el diseño “by design”, y así generar construir la seguridad y funcionalidad de privacidad en el dispositivo desde el principio del proceso de desarrollo, cuando es mucho más probable que sea efectivo.

Una cantidad significativa de trabajo ya se ha hecho en materia de seguridad y de privacidad por los políticos y los reguladores de la UE y EE.UU.. Bajo el Reglamento General de Protección de Datos discutido en el Parlamento Europeo y el Consejo de Ministros, habrá fuertes incentivos regulatorios para las empresas desarrolladoras de sistemas que procesan datos personales para la protección de la seguridad y privacidad desde el diseño.

La Comisión Federal de Comercio de los Estados Unidos (FTC) también sugiere a compañías que sigan el enfoque de "defensa en profundidad" (*defence in depth*), considerando las medidas de seguridad en varios puntos distintos de sus sistemas, tales como el uso de medidas de control de acceso y la encriptación de los datos incluso cuando los usuarios están haciendo uso de enlaces cifrados en el wi fi router del hogar (lo cual no protegerá los datos entre el router y servidores de la compañía o si el router está mal configurado).

Privacidad

La privacidad es un tema regulatorio particularmente fuerte en los países europeos, en los que se incluye un amplio marco legal que incluye la Convención Europea sobre los Derechos Humanos del Consejo de Europa y el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos personales y la Carta de los Derechos Fundamentales de la UE. Este Marco ha sido influyente en el desarrollo de las leyes de privacidad en más de 100 países de todo el mundo.

El alto volumen de flujos de datos personales podría presentar desafíos para la regulación tradicional de protección de datos - por ejemplo, desde que los individuos no serán conscientes necesariamente cuando se comparten datos o capaces de revisar esa información antes de ser enviada a otras partes, creando un riesgo de auto-exposición y falta de control.

Otra cuestión en privacidad es la cantidad de información personal que se puede derivar de los sensores, especialmente cuando se combina con perfiles de usuario y datos de otras fuentes. Los reguladores de privacidad de Europa señalan que el desarrollo pleno de IoT puede provocar una tensión en las posibilidades actuales del uso anónimo de los servicios y en general, limitar la posibilidad de pasar desapercibido.

Investigadores han encontrado que los datos obtenidos por los sensores de teléfonos

inteligentes pueden utilizarse para inferir información acerca de los usuarios, tal como, tipos de personalidad, la demografía y factores de salud (estados de ánimo, los niveles de estrés, tabaquismo, niveles de ejercicio y actividad física) e incluso la aparición de enfermedades como la enfermedad de Parkinson y desorden bipolar. Este tipo de información tiene aplicaciones obvias, tales como, en cuanto al seguro de salud respecto a la fijación de precios como así también para otras decisiones relacionadas con el empleo, el crédito y la vivienda. Esto podría conducir a la discriminación económica contra los individuos clasificados como pobres o con riesgos de salud, y potencialmente a nuevas formas de discriminación racial, de género, u otra discriminación de las personas en las clases protegidas donde Internet de las Cosas puede utilizar servidores proxy ocultos.

Para la protección de la privacidad individual, la Comisión Federal de Comercio de los Estados Unidos (FTC) ha sugerido el requerimiento de la notificación y consentimiento cuando datos personales son recolectados por aplicaciones IoT por fuera de la expectativa razonable de los consumidores, basado en el contexto de las transacciones y las empresas.

Del mismo modo, las autoridades de protección de datos de la Unión Europea han señalado que los datos recogidos por medio de dispositivos IoT para una determinada finalidad pueden ser analizados y combinados con otros datos, lo que lleva a una serie de efectos secundarios que debería ser compatible con el propósito original de la recolección y conocimiento para el usuario (esto se conoce como la limitación de la finalidad).

La recolección y análisis de datos por dispositivos IoT podría afectar la privacidad cuando se incluyen datos de los espacios privados como casas y automóviles, e incluso hacer que sea difícil para las personas manejarse en su vida diaria en forma anónima.

Cuando las aplicaciones de IoT procesan información personal que a la fecha puede revelar datos "sensibles" con arreglo a la ley de protección de datos - origen étnico racial, las opiniones políticas, creencias religiosas o filosóficas, la pertenencia a sindicatos, salud o la vida sexual - se requiere el consentimiento explícito del individuo.

Bajo la ley de la Unión Europea, los individuos deben ser capaces, en cualquier momento, de retirar su consentimiento a la totalidad o parte de los datos procesados, sin "ningún impedimento o restricción técnico u organizativo", utilizando herramientas que sean "accesibles, visibles y eficaces."

La Comisión Federal de Comercio de EEUU (FTC) prevé una mayor flexibilidad para los servicios IoT en la recolección de datos no requeridos inicialmente para proporcionar el servicio, mientras que bajo la normativa europea más estricta, las autoridades de protección de datos de la UE "no pueden compartir este análisis".

Responsabilidad

El proveedor de dispositivos IoT debe considerar los aspectos vinculados a los riesgos legales que genera esta modalidad de provisión de componentes y a su vez, el usuario debe ser consciente de aquellas contingencias por las que el proveedor debiera responder. En este sentido, es importante

considerar aspectos que están asociados a la responsabilidad por parte del Proveedor, entre las que podemos mencionar responsabilidad en base a:

i. Contenido ilegal provisto por el Usuario

En algunas jurisdicciones, los proveedores de IoT pueden ser responsables de información ilegal provista por el usuario que resulta incorporada a los IoT por lo que es de suma importancia establecer en los acuerdos suscriptos con los usuarios aquellas prohibiciones que el usuario tiene en cuanto al uso que puede hacer de los dispositivos y a su vez, prever el límite de responsabilidad a favor del proveedor en base a las acciones desplegadas por el usuario que son contrarias a los términos y usos pactados.

ii. Software / Internet

Los dispositivos que cuentan con las características de IdC están integrados por software embebido, el que está configurado para llevar a cabo ciertas funciones. En cuanto al uso del software en particular, resulta conveniente para el proveedor prever en los acuerdos con el usuario cláusulas que establezcan que el software podrá contener errores, cuya cantidad y magnitud no excederán de ninguna manera el promedio de errores que puede tener cualquier obra de software, pero que es posible que tales errores existan, por tal motivo es usual que las partes contratantes reconozcan que los factores que pueden influir para el correcto funcionamiento del sistema sobre el cual está montado el software, son insusceptibles de ser mesurados en su totalidad al momento de la instalación del software.

Por su parte y en relación a la necesidad de contar con acceso a internet para hacer uso de IoT, es usual que el proveedor prevea en las condiciones de contratación que no responderá por la pérdida o daño total o parcial de los datos e información objeto de los servicios de referencia, producido por fallas en equipos, redes, instalaciones eléctricas y otras instalaciones en general, red de energía eléctrica, proveedor de Internet u otras aplicaciones, siempre que excedan las medidas de seguridad provistas por el proveedor comprometidas en los mismos términos.

iii. Suspensión o terminación del servicio

Por lo general los dispositivos IoT pueden resultar críticos para el negocio o vida diaria y en este sentido, la continuidad y el uso del servicio resulta de suma importancia, por lo que la terminación o suspensión por parte del proveedor podría generar una responsabilidad derivada de los daños en asociación con tales acontecimientos.

iv. Garantías

Las garantías provistas por el proveedor son compromisos asumidos, una promesa vinculada a sucesos que pueden producirse en el futuro. Entre las previsiones que comprende una garantía, están aquellas vinculadas a garantizar que no existen reclamos pendientes ni amenazas vinculadas a derechos de propiedad intelectual y aquellas garantías vinculadas a cuestiones de seguridad de la

información y privacidad. La violación de las garantías otorgadas generará responsabilidad a cargo del proveedor del servicio, por lo que este último tiende a limitarla. Atento ello, pesa en el usuario el análisis sobre los riesgos asociados al servicio provisto y la cobertura que la garantía proporciona.

v. Indemnidad

Se trata del compromiso vinculado a compensar a la otra parte en supuestos de pérdidas derivadas de reclamos de terceros. De este modo, la previsión de una cláusula de indemnidad compensará al usuario de los dispositivos IoT por aquel reclamo derivado del uso de los servicios en violación a derecho de terceros vinculados a propiedad intelectual, esto es, derecho de autor, marcas y patentes. Esto mismo podrá contemplarse respecto al contenido proporcionado por el usuario.

vi. Confidencialidad

El usuario de IoT deberá asegurarse de obtener compromisos por parte del proveedor respecto a la confidencialidad de la información a la que este tenga acceso en vinculación a los productos y/o servicios provistos y en este sentido, el reconocimiento por parte del proveedor de aquellos daños que podría generar la divulgación de la información propiedad del usuario y en consecuencia, la responsabilidad asociada.

Tratamiento de datos

La captura masiva de información personal en tiempos de IoT tendrá diferencias a lo que actualmente se realiza. En este sentido, se puede mencionar: se capturará información en muchos lugares más; el acopio será invisible; los datos serán más íntimos –qué, dónde, cuándo, cómo, con quién, por cuánto tiempo, por qué– y por último, las facilidades de interconexión conllevarán a que nuestros datos sean compartidos en niveles nunca antes vistos. Asociada a la invasión de la privacidad –entendiéndose 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.

Un ecosistema 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 conducta permitida. 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 ubicación, se prestan fácilmente para fines de control y supervisión.

Una de las cuestiones vinculadas con el tratamiento de datos resulta la acumulación masiva de información, lo que es más conocido como B*ig Data.* 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".[1]

A su vez, se ha indicado que a través del Big Data las empresas cuentan con una base racional que les permite identificar individuos para categorizarlos en grupos con otros similares.[2] Así, pueden hacer ofertas diferenciadas, productos para nichos específicos o seguimientos a compras previas. Los efectos 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.[3]

No obstante, las ventajas que a primera vista se vislumbra respecto a la implementación y uso del concepto IoT, podrá generar violaciones a la privacidad y prácticas discriminatorias como así también profundización de la brecha digital, ya que dispositivos y servicios asociados al IoT harán parte de ofertas comerciales que solo un sector de la población podrá pagar.

Sin perjuicio de diferenciar *Big Data* de IoT, tales conceptos resultan complementarios al punto que potencian tanto las oportunidades que presentan a efectos de prevenir y planificar en base a datos certeros como así también mayores riesgos en cuanto a cuestiones vinculadas a privacidad y tratamiento de datos.

A medida que la información personal se acumule –financiera, social, económica– y se ate a ubicaciones y 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.[4] [5]

Iniciativas en el mundo

Mientras algunas cuestiones regulatorias son las usuales para los reguladores de comunicaciones (gestión de espectro radioeléctrico, licencias, estándares, competencia, certificación de equipos), otras suelen ser competencia de otros organismos (protección de datos, privacidad, ciberseguridad). Sea cual sea el rol que adopten, los reguladores deben promover la innovación y

[1] 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) Citado por Cortes, Carlos. Ob. citado. Págs. 15 y 16.
[2] 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). Citado por Cortés, Carlos. Ob. citado.Pág. 16.
[3] 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). Cortés, Carlos. Ob. citado. Pág. 16.
[4] Cfr. Op. Cit. Greenfield, A. Para más información sobre los 'regímenes de autenticación', ver Op. Cit., Cohen, J. Citado por Cortés, Carlos. Ob. Citado. Pag. 17.
[5] Cfr. Ob. citado. Cortés, Carlos.Pág. 14 a 17.

facilitar el avance tecnológico.

La Unión Europea

La Comisión Europea, el órgano ejecutivo de la UE, ha creado la "Alianza para la Innovación de IoT". La Comisión Europea ha sugerido que las futuras regulaciones deben enfocarse en la seguridad, la privacidad, la protección al consumidor, el margen para la competitividad y elección de los usuarios.

La Comisión Europea realizó un informe, basado en consultas públicas sobre IoT. La consulta pública concluyó, entre otras cosas, lo siguiente:

- **Privacidad:** Los representantes de la industria no querían ver cambios en las actuales normas de privacidad, a los fines de promover la innovación, mientras que la mayoría de las organizaciones de usuarios y consumidores consideraron a las actuales regulaciones de privacidad inadecuadas, y quieren que se elaboren guías de Evaluación de Impacto en Protección de Datos específicas para IoT.
- **Seguridad y protección:** Representantes de la industria no quieren ver cambios en los actuales requerimientos de seguridad y no quieren que haya una "sobre-regulación". Los usuarios, en cambio, quieren ver que se creen estándares de seguridad para proteger la confidencialidad de los datos, su integridad y disponibilidad en un ecosistema de IoT.
- **Competencia:** Los representantes de la industria respondieron que los dispositivos de IoT deberían ser interoperables para promover la competencia y la innovación de servicios. Sin embargo, señalaron que sistemas no interoperables que estén integrados verticalmente no deben ser obstaculizados por la legislación, principalmente en productos que no son destinados a usuarios finales.

Estados Unidos

En enero de 2015, la Federal Trade Commission (FTC) publicó un Informe sobre IoT. El informe fue preparado en conjunto con sobresalientes tecnólogos, académicos, representantes de la industria y de asociaciones de usuarios. El Informe se enfocó en asuntos de privacidad, seguridad y sobre si la legislación requería que se regule o no IoT. Las conclusiones a las que llegaron fueron las siguientes:

- **Privacidad:** El informe sugirió que las empresas incurran en una práctica de "minimización de datos", que implica que la recolección de los datos y el tiempo en que se lo retiene sea por el menor tiempo posible, teniendo en cuenta la necesidad para su uso.
- **Seguridad y Protección:** El informe reconoció que la seguridad en un contexto de IoT ganó más importancia. Principalmente, el Informe señaló las múltiples maneras en que las violaciones a la seguridad pueden llevar hacia preocupaciones en la vida real. El Informe sugiere que las empresas prioricen embeber a los dispositivos de seguridad desde el inicio, entrenando adecuadamente a sus empleados, asegurando que los contratistas puedan mantener la seguridad, y que monitoreen los dispositivos e informen a los consumidores cuando se detecten violaciones a la seguridad.

El informe también sugiere que una legislación específica de IoT sería prematura. En cambio, recomienda que legislación amplia en temas de seguridad y privacidad deben ser aplicadas a estos asuntos, manteniendo una flexibilidad suficiente para adaptarse a las innovaciones tecnológicas.

Modelo de negocios de IoT

Actualmente el IoT se está acelerando a medida que los costos disminuyen y las aplicaciones innovadoras emergen. A partir de 2020, el despliegue comercial de las redes de la tecnología 5G proporcionarán capacidades adicionales que serán indispensables para el IoT, tales como las segmentaciones de redes y la capacidad de conectar de manera exponencial más dispositivos de lo que es posible en la actualidad". Se prevé que 16 mil millones (de los 28 mil millones) de dispositivos conectados se unan a Internet de las Cosas para finales de 2021.

La cadena de valor es probablemente la parte más importante del modelo de negocio, dado que define cómo el servicio es proporcionado. IoT tiene una cadena de valor muy compleja debido a que impacta en un gran número de procesos. Esto implica una gran oportunidad para múltiples partes interesadas que necesitan trabajar en conjunto para proveer servicios sobre la base de IoT.

Claramente la formación de alianzas no es fácil cuando cada entidad se considera a sí misma más importante que las demás. En tal escenario, la cuestión más importante para cualquier empresa interesada en IoT es encontrar una posición en la cadena de valor. La posición en la cadena de valor definirá su relevancia, estrategia y oportunidades. La gran pregunta es qué jugador captará la mayor porción dentro de la cadena de valor, el cual idealmente estará constituyendo alianzas verticales y horizontales.

Módulos Inteligentes	Objetos Inteligentes	Conectividad	Plataformas	Customización de Software	Aplicaciones	Clientes
Tarjetas SIM Sensores Chips embebidos Agregadores	Expendedoras Autos Cámaras Termostatos	Redes Conectividad Disponibilidad Calidad	Capacidades de IoT CObranzas Integración con otras aplicaciones Analítica	Interfases Hardware Manejo de Datos	Soluciones verticales CRM y Cobranzas Customer care	Compra servicios Vende servicios

Otra clasificación agrupa a los actores en cinco grupos claves, cada uno tiene fortalezas únicas que aportar a IoT, pero no todos con la misma fuerza ni en pie de igualdad:

- **Proveedores de dispositivos:** sin un modelo de servicios, se beneficiarán de la moda generada alrededor de IoT pero se mantendrán como un simple vendedor de aparatos. Su mejor apuesta es ingresar a alianzas no exclusivas con jugadores líderes de otras partes de la cadena de valor.
- **Operadores:** los operadores son críticos dado que proveen conectividad y han tenido un buen comienzo en IoT. Es natural para este grupo considerarse como líderes en la cadena de valor. Sin embargo, los operadores de red pueden conectar con la mayoría de los dispositivos, ganando no sólo valor en la red sino también estando mejor posicionados para capturar valor. En consecuencia, el riesgo de los operadores es el de convertirse en la simple tubería hacia la

computación en la nube.

- **Proveedores de plataformas:** Las plataformas son el corazón de IoT y son los que unen el hardware, la conectividad, a los operadores y a las aplicaciones verticales, para proveer soluciones específicas de IoT en la industria. La mayoría de los jugadores con intenciones fuertes dentro del mercado de IoT buscan convertirse en proveedores de plataformas de IoT, pero el éxito depende de su habilidad para forjar alianzas hacia un mismo fin. Hay distintos tipos de plataformas:
  - de conectividad o *machine-to-machine*, principalmente enfocadas en conectar dispositivos vía redes de telecomunicaciones y/o tarjetas SIM, sin demasiado foco en *analytics* o procesamiento de datos;
  - plataformas de hardware específico, que suelen ser las plataformas propietarias, diseñadas exclusivamente para ciertos dispositivos;
  - plataformas puras de IoT, que han sido específicamente desarrolladas por IoT para mantener la escala, estándares y requerimientos en mente.

  No todos los tipos de plataformas tendrán la habilidad de liderar el esfuerzo de IoT. Algunos afirman que la combinación ganadora será una plataforma que ofrezca gestión de dispositivos, almacenamiento en la nube, *analytics*, visualización de datos y la posibilidad de integrarse con sistemas de terceros vía API o SDK para poder tomar ventaja de la gran variedad de software y hardware de IoT.
- **Integradores de Sistema:** Tienen un rol muy importante en las IoT industriales. Los integradores de sistemas hacen que los componentes individuales de IoT trabajen juntos de la manera más óptima para el cliente. La mejor opción para los integradores de sistemas es identificar su nicho de mercado y asociarse con grandes jugadores proveedores de plataformas.
- **Proveedores de Aplicaciones:** Son un jugador muy pequeño en general, y hay muy pocos grandes proveedores de aplicaciones específicos de IoT que puedan operar independientemente.

A continuación, los posibles modelos de negocios que pueden adoptar las empresas de tecnología, para maximizar los flujos de ganancias, detallando de qué fuente proviene el retorno de inversión:

Modelo de Negocios	Centrado en Dispositivos	Venta de datos	Dispositivos y/o suscripción	Centrado en el volumen	Ganancias colaborativas
Descripción	El foco del negocio es la venta de dispositivos El servicio provisto posteriormente es gratuito o mínimo En ocasiones	Se comercializan los *insights* generados por el uso de plataformas de *analytics* Los datos cedidos son anónimos y agregados	Pago por adelantado por el hardware Suscripción mensual para acceder a contenidos, o en relación al uso o un software que es provisto como servicio	Apalancamiento de IoT para adquirir nuevos clientes Busca maximizar el número de unidades vendidas o aumentar la base de clientes	Uno de los mayores conductores en la presentación de nuevos modelos de negocios Ligado a la idea de “economía colaborativa” que crea y trae más salarios a gente que participa del

	los usuarios pagan una tarifa por una única vez para obtener características o servicios más complejos	Los *data-sets* cedidos suelen ser relativos a un segmento específico de usuarios a los fines de ser utilizados para estrategias de marketing	Suele ser popular en las empresas que cuentan con una flota de vehículos	Apunta al mercado masivo para aumentar la cuota de mercado y aprovechar las economías de escala	negocio pero desde afuera de la industria Contribuye más eficientemente a bajar la estructura de costos en relación al modelo tradicional

Proyecciones estimadas de los efectos de la implementación de IoT

Un pronóstico de Business Insider establece algunas claves sobre las tendencias que se vienen en base a la implementación de IoT. En este sentido, surgen las siguientes ítems:

- Habrá 34 mil millones de dispositivos estarán conectados a internet para el 2020;
- Cerca de 6 trillones serán gastados en soluciones IoT en los próximos 5 años.
- Las empresas serán quienes más adoptarán las soluciones IoT. Ellos ven tres formas en que IoT puede mejorar resultados mediante:
    - la reducción de los costos de operación;
    - el aumento de la productividad; y
    - la expansión a nuevos mercados o el desarrollo de nuevas ofertas de productos;
- Los Gobiernos están enfocados en incrementar la productividad, reducir costos y mejorar la calidad de vida de los ciudadanos, por lo que se estima que serán los segundos en adoptar el ecosistema IoT;
- Los consumidores son los terceros en adoptar IoT. Aún así, ellos compraran dispositivos en números masivos e invertirán cantidades significativas de dinero en el ecosistema IoT.[6]

[6] Greenough, John. *"How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond."* Consultado el 26.08.26 en: http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

Estándares de IoT

La discusión relativa a los estándares de IoT tomó importancia a principios de 2013. La industria tecnológica, sin embargo, avanzaba en el desarrollo de IoT mucho más rápido de lo que lo hacía el desarrollo de estándares. Desde 2014, algunas organizaciones incluso empezaron a certificar sus productos, aunque de modo limitado. Sin perjuicio de ello, el estado actual de situación es muy lejano al establecimiento de un único estándar universal de IoT, y hay incluso quienes afirman que el establecimiento de un único estándar -tal como sucedió con el DVD o el Wi-Fi- es imposible.

La otra cuestión relativa al establecimiento de los estándares de IoT es si en verdad son necesarios o no. Algunos miembros de la industria siguen señalandolos como centrales, principalmente aquellas entidades que se dedican a desarrollarlos.

Si resultara como las anteriores guerras de estándares, plataformas y formatos, los pesos pesados se alinearán detrás de las distintas opciones, hasta que uno gane la delantera y de a poco la mayoría de los actores empiecen a alinearse detrás de aquél. Eventualmente, tal vez, los dispositivos de IoT puedan conectarse y hablar entre sí.

En tal sentido, es necesario tener en cuenta que IoT requiere diversa tecnología para funcionar: desde comunicaciones móviles, a seguridad de la información, a intercomunicaciones e interoperabilidad con otros dispositivos. Un único estándar muy probablemente no podrá cubrir esto, del mismo modo que el funcionamiento de una computadora portátil no es alcanzado por un único estándar.

Como consecuencia de lo anterior, se pueden considerar cuatro capas en las que se está trabajando en desarrollo de estándares de IoT: La primera es la capa de *aplicación*, en la que se mira los protocolos para desarrollar aplicaciones de IoT. Estas están siendo desarrolladas por organismos de estándares, tales como el IETF, OASIS, OMA y W3C. La segunda capa es la de *servicios*, donde se desarrollan marcos que permitan servicios de IoT. Estos marcos están siendo desarrollados por oneM2M, OIC y AllSeen. La capa siguiente es la de *redes*, donde se presta atención a las optimizaciones que apoyan a IoT. Finalmente, la última capa es la de *tecnologías de acceso*, que busca optimizar las capas de aplicación y de servicios para el uso de servicios de IoT y optimizaciones específicas de acceso a redes. Estas optimizaciones de acceso están siendo desarrolladas por 3GPP, IEEE, Bluetooth SIG, Weightless SIG, entre otros.

A continuación se describen algunas de las entidades más relevantes que han desarrollado estándares de IoT de diverso tipo en el último año.