IOT o Internet de las Cosas

1. ¿Qué es?
2. Regulacion
3. Regulaciones extranjeras
   a- Estados Unidos
   b- Union Europea
   c- Brasil
4. Argentina

1- ¿QUÉ ES?

El Internet of Things (IoT) o Internet de las Cosas, describe la red de objetos físicos (cosas) que llevan sensores integrados, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de Internet. Estos dispositivos abarcan desde objetos domésticos cotidianos hasta sofisticadas herramientas industriales.

En los últimos años, IoT se ha convertido en una de las tecnologías más importantes del siglo XXI. El 52 por ciento de las compañías alrededor del mundo ve a IoT como un elemento transformacional de sus industrias, de acuerdo con el Mobile Economy GSMA.

En combinación con herramientas de inteligencia y Big Data, las compañías pueden aprovecharse de la información generada por los dispositivos conectados para tomar mejores decisiones, incrementar la productividad y, en última instancia, lograr una mejor experiencia de usuario. Posibilita la comunicación fluida entre personas, procesos y cosas

Sin embargo, no solo los consumidores están automatizando y adoptando la tecnología según su conveniencia; las ciudades en las que vivimos también están recurriendo a la tecnología para ofrecer servicios, estaciones de alquiler de bicicletas, quioscos automatizados y cosas similares.

El acceso a tecnología de sensores de bajo coste y baja potencia. Los sensores asequibles y fiables hacen que la tecnología de IoT sea posible para más fabricantes.

Conectividad: Un conjunto de protocolos de red para Internet ha hecho que sea fácil conectar sensores a la nube y a otras “cosas” para conseguir una transmisión de datos eficiente.

Plataformas de Cloud Computing: El aumento de la disponibilidad de las plataformas en la nube permite que tanto las empresas como los consumidores accedan a la infraestructura que necesitan para ampliar la capacidad sin tener que gestionarlo todo.

Machine learning y analítica: Con los avances logrados en machine learning y en analítica, junto con el acceso a enormes cantidades de datos de una gran variedad almacenados en la nube, las empresas pueden reunir información más rápido y de forma más sencilla. El surgimiento de estas tecnologías relacionadas sigue ampliando los límites de IoT, y los datos producidos por IoT también retroalimentan estas tecnologías.

Inteligencia artificial (IA) conversacional: Los avances en redes neuronales han llevado el procesamiento de las lenguas naturales (NLP) a los dispositivos de IoT (por ejemplo, los asistentes personales Alexa, Cortana y Siri) y los han convertido en dispositivos atractivos, asequibles y viables para el uso doméstico.

La capacidad de IoT da impulso a un amplio conjunto de aplicaciones. Lo que permiten, por ejemplo:

- Crear nuevas eficiencias en fabricación a través de la supervisión de las máquinas y la supervisión de la calidad de los productos.
- Mejorar el seguimiento para que las empresas determinen la ubicación de los activos, y la “delimitación” de activos físicos para asegurarse de que los activos de alto valor están protegidos del robo y la extracción.
- Usar wearables para supervisar el análisis de la salud humana y las condiciones ambientales. Los wereables de IoT hacen que las personas entiendan mejor su propia salud y permiten a los médicos supervisar de forma remota a los pacientes. Esta tecnología también hace posible que las empresas puedan hacer un seguimiento de la salud y la seguridad de sus empleados, lo que es especialmente útil para los empleados que trabajan en condiciones peligrosas.
- Impulsar eficiencias y nuevas posibilidades en los procesos existentes.
- Facilitar los cambios de procesos empresariales.

Las organizaciones que mejor se adaptan a IoT son aquellas que se beneficiarían del uso de dispositivos con sensores en sus procesos empresariales.

Fabricación:

Los fabricantes pueden conseguir una ventaja competitiva mediante la supervisión de la línea de producción para habilitar el mantenimiento proactivo en los equipos cuando los sensores detectan un fallo inminente. Los sensores pueden medir los momentos en que la capacidad de producción se ve afectada. Con la ayuda de las alertas de los sensores, los fabricantes pueden revisar rápidamente los equipos para comprobar su corrección o retirarlos de la producción hasta que estén reparados. Esto permite a las empresas reducir los costes operativos, obtener mejor tiempo de actividad y mejorar la gestión del rendimiento de los activos.

Industria automovilística:

Además de los beneficios de aplicar IoT a las líneas de producción, los sensores pueden detectar fallos inminentes de los equipos en vehículos que ya están en la carretera y avisar al conductor enviándole información detallada y recomendaciones. Gracias a la información agregada reunida por las aplicaciones basadas en IoT, los fabricantes y proveedores de automóviles pueden obtener más información sobre cómo están funcionando los vehículos e informar de ello a sus propietarios.

Transporte y logística:

Las flotas de coches, camiones, barcos y trenes que requieren llevar un inventario pueden ser redirigidos según las condiciones atmosféricas, la disponibilidad de vehículos o la disponibilidad de conductores, gracias a los datos de los sensores de IoT. El propio inventario podría estar equipado también con sensores para el seguimiento y localización y para supervisar el control de la temperatura. Las industrias de alimentos y bebidas, flores y productos farmacéuticos a menudo llevan un inventario sensible a la temperatura que se beneficiaría enormemente de las aplicaciones de supervisión de IoT que envían alertas cuando las temperaturas suben o bajan hasta un nivel que supone una amenaza para el producto.

Sector minorista:

Las aplicaciones de IoT permiten a las empresas del sector minorista gestionar el inventario, mejorar la experiencia del cliente, optimizar la cadena de suministro y reducir los costes operativos.

Sector público:

Los beneficios de IoT en el sector público y otros entornos relacionados con los servicios son asimismo de una amplia variedad. Por ejemplo, los servicios públicos del gobierno pueden utilizar aplicaciones basadas en IoT para notificar a los usuarios de cortes masivos o incluso de interrupciones más pequeñas en los servicios de agua, electricidad o alcantarillado. Las aplicaciones de IoT pueden recopilar datos sobre el alcance de un corte y desplegar recursos para ayudar a que los servicios públicos se recuperen de los cortes con más rapidez.

Atención sanitaria:

La supervisión de activos de IoT ofrece varias ventajas a la industria de la atención sanitaria. Los doctores, enfermeros y asistentes a menudo necesitan saber la ubicación exacta de recursos de ayuda al paciente, como las sillas ruedas. Si las sillas de ruedas de un hospital están equipadas con sensores de IoT, se puede hacer un seguimiento de ellas desde la aplicación de supervisión de activos de IoT, de modo que cualquiera que la busque pueda encontrar la silla de ruedas disponible más próxima. Muchos recursos de hospital pueden rastrearse de esta forma para garantizar su uso apropiado, así como para llevar la contabilidad financiera de los activos físicos en cada departamento.

Seguridad general en todas las industrias:

Además de rastrear los activos físicos, IoT se puede usar para mejorar la seguridad de los trabajadores. Los empleados de entornos peligrosos, como minas, yacimientos petroleros y de gas, plantas químicas y centrales eléctricas, por ejemplo, tienen que saber si se ha producido una incidencia peligrosa que podría afectarles. Cuando están conectados a aplicaciones basadas en sensores de IoT, se les puede informar de accidentes o rescatarlos lo más rápido posible. Las aplicaciones de IoT también se utilizan en wearables que pueden supervisar la salud humana y las condiciones medioambientales. Estos tipos de aplicaciones no solo ayudan a las personas a entender mejor su propia salud, sino que también permiten a los médicos supervisar de forma remota a los pacientes.

Sin duda, el desarrollo de IoT también está sufriendo el impacto de la pandemia de la COVID-19. En este nuevo escenario en el que el contacto social es más limitado, el contacto entre dispositivos y las distintas herramientas disponibles puede resultar de gran ayuda para permanecer conectados.

Según publica Forbes, IoT será una de las grandes megatendencias de 2021 y desempeñará un papel clave en la forma en la que vivimos, trabajamos y nos relacionamos. Esto llevará a, por ejemplo, asistir a un fuerte impulso de la inversión en IoT dentro del ámbito sanitario, desde para la telemedicina hasta para la ayuda domiciliaria automatizada para personas mayores y discapacitadas, pasando por dispositivos portátiles inteligentes, sensores y dispositivos conectados que seguirán cambiando la forma en la que se brinda la atención médica.

Junto a las aplicaciones en el ámbito sanitario, IoT también experimentará un rol fundamental en el impulso de la productividad. En un momento en el que el trabajo remoto está en auge y los negocios se enfrentan a una crisis económica con grandes incertidumbres, IoT se convertirá en un gran aliado para acelerar la productividad.

El uso de asistentes personales con tecnología de Inteligencia Artificial, como Alexa, en muchos hogares contribuirá a optimizar la productividad de muchos empleados remotos con herramientas y aplicaciones para una gestión más eficiente del tiempo y de las tareas, así como para la mejor calidad de las videoconferencias y reuniones virtuales.

2- REGULACION

No todas las características de IoT son positivas. Este abrumador uso de la tecnología en todas las industrias y todos los rincones de la vida crea una gran oportunidad para que los ciberdelincuentes se aprovechen, como lo demostró en 2016 la botnet Mirai que utilizó cientos de miles de dispositivos IoT para lanzar un ataque de DDoS a los servidores DNS, paralizando gran parte de Internet. A medida que crece el número de dispositivos conectados, la oportunidad de abuso, lamentablemente, también crece.

Si un dispositivo está conectado, probable esté recopilando datos. En el caso de los consumidores, estos podrían ser datos personales sensibles sobre hábitos de sueño, salud o alimentación, por lo que la necesidad de asegurar la gran cantidad de datos que recopilan todos los dispositivos debería estar entre los principales pensamientos de los usuarios al comprar estos dispositivos y de los proveedores al desarrollarlos.

¿Cómo se relacionan las cosas, objeto de los derechos reales, susceptibles de generarse sobre ellos derechos y obligaciones con la animación artificial inteligente mediada por internet? ¿Qué consecuencias jurídicas se pueden producir por el accionar de objetos controlados por programas mediados por internet?

Jean Luis Gassée en 2014, en una nota que se le ha realizado, ha mostrado preocupación por las consecuencias jurídicas que se podría desprender de la utilización de objetos cotidianos, como televisores, licuadoras etc. que se programarán en forma automática mediados por wi-fi o bluetooht, pues estos no cuentan con dispositivos que proporcionen auto descripción o comunicación bidireccional confiable y que finalizarán en una cesta de remotos. Sin embargo el marketing de promociones de ventas, ofrecen estos objetos como herramientas seguras y que ofrecen al consumidor mayor confort y facilidad en la utilización de ellos mediantes programaciones remota.

Dentro de la vida cotidiana de las personas conviven teléfonos inteligentes, televisores inteligentes, heladeras inteligentes, por solo nombrar algunos artículos que pueden recibir órdenes por internet a través de espacios virtuales en la comunicación entre computadores conectados o emparejados ya sea por una red que los aglutina o por bluethooth, y traducir esas órdenes en acciones concretas que se llevan a cabo sin la intervención específica de la mano del hombre. En conclusión, se puede hackear cualquiera de esos objetos, manifestando una pérdida de la seguridad que afecta tanto a las cosas como a las personas.

Entre las diferentes formas de ciber ataque, encontramos el ciber espionaje. Normalmente los ataques a que son sometidas estas cosas, se asocian a la extorción en dinero para “liberarlas”.

Para profundizar más aún, el mundo del internet de las cosas, se complementa con la domótica.

Las normas sobre derecho informático deberían ser integradas a las normas civiles y comerciales unificadas. Adherimos a la teoría que la internet de las cosas, no deja de reunir las características propias de las cosas objeto de los derechos reales, aunque en forma accesoria

funcionen con componentes no materiales que le permitan actuar en forma remota. Por lo tanto son un tipo de objeto, cosa mueble, probablemente registrable en función de su complejidad, que se acompaña de códigos informáticos que le permiten actuar conectados por internet en forma remota sin la necesidad de intervención humana. Sin embargo por su complejidad deberán estar estas normas articuladas con normas informáticas, normas constitucionales, normas penales, normas de consumo y normas comerciales.

En tal sentido, la recomendación ITU Y.6060 de la Unión Internacional de Telecomunicaciones (UIT) establece 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".

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 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.

3- REGULACIONES EXTRANJERAS

La necesidad de que las condiciones de seguridad estén presentes es algo que está fuera de discusión. Y la realidad indica que varios fabricantes de dispositivos IoT han fallado al momento de tomar las medidas razonables para hacer que sus dispositivos sean seguros.

Los legisladores y los gobiernos están tomando medidas para ayudar a garantizar la privacidad y la seguridad. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Privacidad del Consumidor de California (CCPA) son ejemplos que requieren que los proveedores soliciten permiso para recopilar datos y brinden la seguridad adecuada para protegerlos.

También está comenzando a aparecer una regulación que requiere algunos estándares mínimos de seguridad para los dispositivos de IoT. California, por ejemplo, requiere que cada dispositivo tenga una contraseña única lista para usar y que solo recopile los datos necesarios para completar su función anunciada. El gobierno del Reino Unido también anunció una propuesta de ley para proteger los dispositivos de IoT, que incluye exigir que los fabricantes indiquen claramente durante cuánto tiempo estarán disponibles las actualizaciones de seguridad.

a- Estados Unidos

El diario jurídico Gavel Capital en el año 2017 había publicado un artículo mediante el cual analizaba la postura de Estados Unidos frente a la legislación del internet de las cosas. El país del norte ha tomado seriamente legislar sobre la seguridad de estos aparatos en lo que refiere al resguardo de datos y la intromisión de terceros.

En el mes de agosto de 2017, senadores de los dos grandes partidos en forma conjunta han presentado el proyecto destinado a establecer estándares que regulen la seguridad para todos aquellos objetos y aparatos que se encuentre conectados dentro de las redes de las agencias federales (Internet of Things Cibersecurity Improbement Act 2017).

Establecieron que cada agencia incluya las siguientes cláusulas claves en sus futuros contratos para la adquisición de dispositivos conectados a Internet:

I. Certificación escrita del contratista de que sus dispositivos. No contienen componentes con vulnerabilidades o defectos de seguridad conocidos incluidos en la Base de Datos Nacional de Vulnerabilidad del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) o en una base de datos similar identificada por el Director de la Oficina presupuestaria federal**.** Incluyen componentes capaces de recibir parches autenticados y de confianza de los proveedores.
   Utilizan tecnología y componentes estándar para la comunicación, encriptación e interconexión con dispositivos periféricos; y no incluyen “contraseñas fijas o codificadas” para recibir actualizaciones o habilitar el acceso remoto.
II. Compromiso del contratista de notificar a la agencia adquirente cualquier “vulnerabilidad o defecto de seguridad descubierto por el propio contratista o revelado con posterioridad al vendedor por un investigador de seguridad, durante la vida del contrato.
III. Compromiso del contratista de actualizar, reemplazar o eliminar oportunamente, las vulnerabilidades identificadas de los componentes de software y firmware del dispositivo de una manera debidamente autenticada y segura. Esto incluye la obligación de proporcionar información a la agencia adquirente con respecto a la forma de tales actualizaciones, así como un cronograma y un aviso formal al finalizar el soporte de seguridad.

Entre lo más destacado del proyecto se ha encontrado que las normas que se postulan prohíben que los proveedores incluyan nombres de usuario y contraseñas codificados.

El 1 de enero de 2020 entró en vigor la nueva Ley de California que regula el Internet de las cosas (IoT). El texto, aprobado por el Gobernador el 28 de septiembre de 2018, fue una de las primeras regulaciones sobre esta materia.

La normativa de California establece los requisitos de seguridad para los dispositivos conectados que se vendan en California. Así, la norma define "Dispositivo conectado" como "cualquier dispositivo u otro objeto físico que sea capaz de conectarse a Internet, directa o indirectamente, y que tenga asignada una dirección de Protocolo de Internet o una dirección Bluetooth".

La Ley modifica el Código Civil para introducir la obligación de que los dispositivos conectados presenten características de seguridad "razonables" o "apropiadas para la naturaleza y la función del dispositivo". Y obliga a los fabricantes a establecer una contraseña predeterminada diferente para cada gadget que venden o que soliciten a los usuarios que cambien la contraseña predeterminada común antes de empezar a usar el dispositivo por primera vez. De esta forma, los controles de seguridad estándar que resultan de fácil acceso para los hackers deberían ser eliminados.

Lo que caracteriza principalmente a la ley californiana es que, a diferencia de otras normas, se centra en la seguridad de los productos y, por ende, de los usuarios.

La ley no tiene unos requerimientos muy exhaustivos, dando cierta flexibilidad a los fabricantes y al mismo tiempo, a la propia tecnología cuya evolución es constante y cambiante. Algunos medios americanos la consideran que se usa una definición incompleta y superficial de seguridad al no recomendar otras medidas de seguridad, "como la certificación del dispositivo, la firma del código y una auditoría de seguridad para el firmware en componentes de bajo nivel que los proveedores de dispositivos de IoT compran a proveedores extranjeros".

La norma descarta a los particulares la acción para reclamar, dejando esta en manos del Fiscal General, un abogado de la ciudad, un abogado del condado o un fiscal de distrito. Tampoco especifica sanciones a las infracciones que se puedan cometer, por lo que habrá que esperar al resultado de su aplicación en el tiempo.

b- Union Europea

Europa ofrece grandes oportunidades para la adopción de nuevas tecnologías y servicios como solución a los retos de la sociedad. La Unión Europea comenzó a prepararse para la era del IoT hace diez años con el lanzamiento en 2005 del plan i2010: Una sociedad de la información europea para el crecimiento y el empleo. Éste establecía políticas clave para el desarrollo del Espacio Único Europeo de Información, la innovación e inversión en investigación y la inclusión, y la mejora de los servicios hacia los ciudadanos. Posteriormente, se han ido incrementando los campos de regulación mediante diferentes Directivas, destacando aquellos relativos a estandarización, privacidad y protección de los datos, ciberseguridad y cibercriminalidad, infraestructura e I+D+i.

La regulación del IoT requiere la toma de decisiones tanto sobre los dispositivos que se conectan como sobre las redes y su seguridad, y sobre los datos asociados a los dispositivos. Algunas de las Directivas más recientes a destacar en estos campos son:

- En materia de estandarización, la Directiva 2014/53/UE sobre la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos es fundamental para el desarrollo conjunto y armonizado de la tecnología.

- En cuanto a privacidad, protección de datos y propiedad de los mismos, el nuevo Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) armonizará, a partir de 2018, el marco de la UE para el tratamiento de datos personales. Hasta esa fecha, se mantiene en vigor la Directiva sobre Protección de Datos de 1995.

- La cibercriminalidad se aborda en la Directiva 2013/40/UE, que es relativa a los ataques contra los sistemas de información y por la que se establecen normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. Por su parte, la ciberseguridad se trata en la recientemente adoptada Directiva de Seguridad en Redes y Sistemas de Información (NIS por sus siglas en inglés). El objetivo básico de esta Directiva es establecer un nivel común de ciberseguridad en toda la UE y mejorar la coordinación de los Estados Miembros ante posibles ataques cibernéticos.

• La infraestructura necesaria para la el desarrollo del Internet de las Cosas se ha impulsado con diversas medidas, destacando la Iniciativa de Comunidades Conectadas donde se da cabida a diferentes sistemas concebidos para poner en comunicación a diferentes localidades entre sí, y a su vez, a diferentes agentes locales de banda ancha y operadores, con asesores que puedan aconsejarles sobre el mejor modo de acceder a financiación o desarrollar modelos de empresa creados a medida para llevar la banda ancha rápida a su colectividad.

• Finalmente, la medida de fomento de la I+D más emblemática es la iniciativa "Unión por la innovación de Europa 2020", así como las diferentes formas de financiación de la innovación a través de los Programas Marco y, concretamente el último de ellos, también conocido como Horizonte 2020.

Para noviembre de 2017, la comisión había articulado la modernización de legislación respecto a propiedad intelectual, derechos contractuales y adjudicación de espacios radioeléctricos. Estos debates han quedado plasmados en normas que regulan:

- En construir una infraestructura y una red de comunicaciones de primer orden.
- Adoptar un planteamiento común de la ciber seguridad.
- Intensificar los esfuerzos para luchar contra el terrorismo y la delincuencia en línea.
- Conseguir un sistema tributario eficaz y justo que se adapte a la era digital.

Estos pasos dados se refuerzan con nuevas medidas para proteger a los consumidores.
Para profundizar más aún, el mundo del internet de las cosas, es decir objetos cotidianos que pueden interactuar entre ellos y crear acciones sin la intervención humana, se complementa con la domótica.

La legislación propuesta, lanzada por la ministra Digital Margot James, también introduciría un nuevo sistema de etiquetado para informar a los clientes qué tan seguro es un producto IOT.

A los minoristas se les prohibiría eventualmente vender productos sin las etiquetas, aunque inicialmente el esquema sería voluntario.

Para obtener una etiqueta y entrar en el mercado, los dispositivos IOT tendrían que:

- Tener con contraseñas únicas por defecto
- Indicar claramente durante cuánto tiempo estarán disponibles las actualizaciones de seguridad
- Ofrecer un punto de contacto público al que se pueda revelar cualquier vulnerabilidad de seguridad cibernética.

Como contralor y veedor se crea la figura del Delegado de Protección de Datos, quién deberá velar y entender en cuestiones como:

1. La regulación del denominado «derecho al olvido» o derecho de supresión de los datos personales.
2. Derecho a la portabilidad de los datos.
3. Responsabilidad del responsable del tratamiento de datos. El responsable debe tener domicilio dentro de EU. Redacción en lenguaje claro, sencillo y comprensible sobre las cláusulas de privacidad.
4. Registro de las actividades de tratamiento. Concreción de códigos de conducta y certificación o sellos de marca.

5. Notificación de una violación de la seguridad de los datos personales a la autoridad de control. Se estatuye como derecho para los usuarios.
6. Evaluación de impacto relativa a la protección de datos.
7. Consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento
8. Regulación de las transferencias internacionales de datos
9. Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas
10. Multas de hasta el 4 % de la facturación global de las empresas en caso de infracción y derecho a indemnización.
11. la necesidad de "consentimiento claro y afirmativo" de la persona concernida al tratamiento de sus datos personales.

Para el cumplimiento de estas normativas, el órgano competente de contralor deberá:

1. Identificar el riesgo del tratamiento en un informe previo.
2. La evaluación de riesgos en términos de origen, naturaleza, probabilidad y gravedad.
3. La identificación de buenas prácticas para mitigar el riesgo, como son procedimientos, certificaciones, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos.

El Consejo Europeo de Protección de datos, integrado por miembros de todos los países de la Unión Europea, desempeñará el rol de tribunal judicial con competencia en el tema. Se encuentran embebidos del poder sancionador materializado en multas administrativas, y facultades para establecer indemnizaciones para las personas afectadas. Si de delitos se trata, la competencia de este Consejo queda relegada a la justicia europea cuyo tratamiento refiera al ciber delito.

Las leyes propuestas siguen un código de práctica voluntario para los fabricantes de IOT.

c- Brasil

Brasil presentó el plan de Internet de las Cosas a mediados de 2019, tras cuatro años de un debate. "Se pretende dar más certeza y seguridad jurídica para implementar soluciones con más eficiencia y previsibilidad", indicaron por entonces las autoridades. También puso tres verticales como prioridades: agroindustria, salud y ciudades inteligentes. Creó luego una cámara de gobernanza por una de ellas, que se agregaron a la Cámara de Industria 4.0.

El Consejo Director de la Agencia Nacional de Telecomunicaciones (Anatel) aprobó una serie de alteraciones regulatorias con el ojo puesto en fomentar el desarrollo de Internet de las Cosas (IoT, por sus siglas en inglés) y las comunicaciones máquina a máquina (M2M). La definición más relevante es que quedó escrito que los servicios prestados por dispositivos IoT tendrán que soportar una carga tributaria más baja que las de telecomunicaciones.

Otras especificaciones quedarán definidas en los requisitos técnicos. Según la legislación de cada municipio, este servicio de valor agregado puede ser susceptible del impuesto al servicio (ISS).

Otra ley que cobra importancia en el tema es la Ley General de Protección de Datos de Brasil (LGPD). La ley entró en vigor en agosto de 2020 pero las penalizaciones comenzarán a hacerse efectivas en agosto de 2021. Si bien en general hay muchas similitudes entre la LGPD y el GDPR, aquí están algunas de las diferencias más importantes:

- La LGPD no define los tipos de datos de la forma en que lo hace el GDPR, esto significa que el reglamento es muy amplio y puede aplicarse a los datos vinculados directos o indirectamente a una persona o grupo de personas.
- El GDPR permite a las empresas utilizar libremente los datos anónimos sin revelarlos, lo que no ocurre con la LGPD, ya que no existe un lenguaje relativo a los tipos de datos, lo que significa que, independientemente de la anonimización, la recopilación debe ser revelada.
- La LGPD da a las empresas solo 15 días para responder a las solicitudes de datos por parte de los consumidores, frente a los 30 días que otorga la GDPR.
- Las multas máximas que puede imponer la LGPD son del 2% de los ingresos globales o 50 millones de reales, lo que equivale aproximadamente al 50% del valor de la multa que puede llegar a imponer el GDPR.
- La LGPD no tiene un tiempo definido en el que una empresa debe reportar que ha sido víctima de una violación de datos, en la actualidad solo establece un "tiempo razonable". La GDPR obliga a hacerlo en un plazo de 72 horas.

Cualquier empresa que procese datos de un individuo que se encuentre en Brasil tendrá que cumplir con los requisitos de la LGPD. La LGPD se aplica a cualquier persona ubicada en Brasil cuyos datos hayan sido recolectados o procesados, independientemente del lugar donde se encuentre la empresa que los recoge.

En el IoT destacan los llamados "wearables" se refiere a objetos cotidianos y ropa, tales como relojes inteligentes o gafas de realidad aumentada, en los que se han incluido sensores para ampliar sus funcionalidades y que pueden grabar información sobre sus propios hábitos y estilos de vida, todos ellos aún sin norma específica y con reglas generales no tan pertinente a su condición. Esta reflexión vertida en el año 2017 por Espacio Asesoría, que reflejaba la realidad europea. Cruzando el océano, en el cono sur, en la Argentina ocurre lo mismo.

Todos estos dispositivos plantean dudas acerca de la protección de los usuarios en sus datos, su identidad o su seguridad, pero también sobre el respeto al derecho a la competencia, sin que actualmente existe una regulación específica al respecto, teniendo que estarse a lo que o de forma genérica tanto de manera estatal como en el marco de la Unión Europea se establece al respecto, amplía el artículo de Espacio Asesoría. Respecto a la protección de datos y propiedad de los mismos, las novedades europeas provienen del Reglamento UE 2016/679 del parlamento Europeo y del Consejo del 27 de abril de 2016. Estas normas han venido a modernizar y actualizar la legislación. Mediante estas normativas se articula respecto a la protección de las personas físicas en lo que refiere al tratamiento datos personales y a la libre circulación de estos. Esta regulación legislativa ha de permitir a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores. No obstante, un problema que habrá que resolver es la migración voluntaria de datos de una empresa a otra en caso de cambiar de servicio. También habrá que regular claramente la cesión de datos para que en ningún caso el consumidor desconozca su acumulación o su traspaso a terceros.

4- IOT EN ARGENTINA

La Cámara Argentina de Internet (Cabase) anuncio en noviembre de 2020 la creación de la Cámara Argentina de IoT con el objetivo de promover el desarrollo del ecosistema de

empresas y organizaciones vinculadas a Internet de las Cosas. Se trata de una continuación de un trabajo que venía llevando adelante la organización con su Marketplace, un espacio de diálogo entre especialistas y referentes del mundo de la tecnología, compañías y PyMEs de la industria, desarrolladores, universidades y centros de estudios y autoridades gubernamentales, además de empresas y proveedores.

El vertical de mayor potencialidad de desarrollo para IoT es el de ciudades inteligentes, según el 43 por ciento de los profesionales de la industria de telecomunicaciones encuestados para un reporte de TeleSemana.com. Le siguen los servicios públicos con el 11 por ciento, agronegocios (nueve por ciento) y transporte (ocho por ciento), entre otros.

Mediante la Resolución 8/2016, se 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 del ecosistema de internet. Por su parte, 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. Se conformó el Grupo de Trabajo de Servicios de Internet para estudiar el tema.

En abril de 2018 se realizo el evento organizado por el Ministerio de Modernización de Argentina y la Unión Internacional de Telecomunicaciones (UIT), Foro que exploró el papel de las nuevas tecnologías, incluida la conectividad de alta velocidad, resistente y de baja latencia y tecnologías como la computación distribuida, el IoT, el aprendizaje automático y la IA: para abordar los desafíos urbanos y dar forma a ciudades más inteligentes y más sostenibles.

Como producto final se realizó la Declaración de Buenos Aires en la cual los participantes hicieron un llamado a la acción, incluida la necesidad de crear conciencia sobre el papel de la IA e IoT en el desarrollo de las ciudades inteligentes; renovar las políticas públicas para prepararse para un futuro de IA; promover la producción y el suministro de tecnologías inteligentes; alentar la colaboración y la asociación entre los sectores público y privado; aprovechar el potencial de AI para asegurar el IoT; construir una plataforma para compartir mejores prácticas y datos; e incorporar AI a los servicios públicos.

En 2019, IoT fue noticia. En primer lugar, el Congreso de la Nación aprobó la ley de economía del conocimiento, que promueve el desarrollo de las industrias TIC (tecnología de la información y la comunicación) otorgando entre otras cosas beneficios impositivos y arancelarios, e incluye explícitamente a Internet de las cosas. En segundo lugar, en la Ciudad de Buenos Aires se realizaron varios eventos que incluyeron el IoT day de la Cámara Argentina de Internet y la Expo Smart Cities BA.

En el marco de la segunda edición argentina de la Smart City Expo World Congress, la SeTIC presentó la primera prueba piloto de Internet de la Cosas orientada al transporte público que se implementará en la Ciudad de Buenos Aires.

Hay factores tecnológicos, competitivos, macroeconómicos y de políticas públicas que pueden acelerar o demorar el desarrollo de soluciones IoT en Argentina. Por el lado de las comunicaciones, en nuestro país se utilizan desde hace años las redes de las empresas de telefonía móvil, a través de servicios M2M (machine-to-machine)- para conectar dispositivos. Esa tecnología es adecuada para muchas aplicaciones de IoT, pero no para todas.

Como factor macroeconómico se destaca la necesidad de crédito para el despliegue de soluciones IoT. Muchos proyectos demandan grandes inversiones en compra e instalación de dispositivos y el costo de la financiación puede hacer inviable el negocio.

Analizando casos de otros países, en donde se encuentran ecosistemas IoT muy desarrollados, se evidencia que están siendo fuertemente impulsados por políticas públicas que tienen como objetivo potenciar el crecimiento de la economía digital. En ese sentido, que se haya aprobado la Ley de Economía del Conocimiento es un paso importante en la dirección del desarrollo.

Durante el año 2020 Logicalis, empresa global de soluciones y servicios integrados de Tecnologías de la Información y las Comunicaciones (TIC), presentó los resultados de la cuarta edición de su estudio IoT Snapshot, en donde analiza la evolución de 'Internet de las cosas' (IoT, por sus siglas en inglés) y su adopción en la Argentina, Brasil, Colombia, Chile y México. Una de las conclusiones principales fue que en la actualidad esta tecnología, más que una promesa, es algo que ya está sucediendo y es posible ver proyectos en su fase de implementación.

Según el estudio, para el 42% de las empresas IoT es un tema de importancia alta, mientras que el 74% predice que en los próximos 3 a 5 años, será una cuestión de alta o muy alta relevancia dentro de las corporaciones. A la hora de enumerar los beneficios clave para adoptar IoT se destacan: la reducción de costos, la rapidez y eficiencia operativa que se logra con la misma. Como contrapartida, el costo y la cultura organizacional son los principales inhibidores.

En el caso particular de Argentina la importancia de esta tecnología se incrementó en comparación con la edición anterior del estudio, pasando de un 3% al 19% quienes afirman que es de alta importancia. Asimismo, disminuyó el porcentaje de quienes piensa que su importancia es baja o muy baja.

En octubre de 2020 el IEDS aplica "Internet de las cosas" a la medición de consumos de energía de instalaciones y edificios, con el fin de digitalizar datos en tiempo real y realizar diagnósticos energéticos, dando los primeros pasos en la planificación de un Sistema de Gestión de la Energía. En la época en que vivimos resulta fundamental disponer de datos en tiempo real con el fin de realizar las innovaciones y cambios que conducen al uso inteligente de la energía. se genera una monitorización inteligente y se dispone de una amplia base de datos para analizar, y tomar decisiones de acuerdo con objetivos de eficiencia. Todo esto genera experiencias que pueden ser trasladadas a otras instalaciones de la misma Institución.

El desarrollo de Internet de las Cosas requiere de un enfoque multidimensional, que incluya diferentes actores del sector público, privado, académico y la sociedad civil. Bajo este marco, la Jefatura de Gabinete busca acelerar el despliegue de IoT y trazar un camino para impulsar el desarrollo económico y social de Argentina apalancado en esta tecnología.

Para ello, trabajan en un Plan Nacional de Internet de las Cosas a partir de la interacción de diferentes ámbitos de Gobierno, con la inclusión de actores del sector público, privado, académico y la sociedad civil.

El trabajo con los diferentes espacios públicos consiste en la identificación de sectores verticales prioritarios para el desarrollo económico nacional, la identificación de líneas de financiamiento y la conjugación con las tareas de Investigación y Desarrollo de las Universidades.

La SubSETIC también estrechará vínculos con el sector privado relacionado con IoT, a sabiendas de los varios emprendimientos que llevan adelante operadores de telecomunicaciones, empresas grandes, PyMES, emprendedores y cámaras sectoriales.

La articulación del Estado con actores privados es una instancia clave para la integración de cadenas globales de suministro, el cuidado del medioambiente, la conformación de ciudades digitales, el avance de la industria 4.0, el crecimiento de IoT en la producción agropecuaria, como así también en sectores relacionados con la minería, el petróleo y la energía eléctrica, domótica, por mencionar algunos.

El Plan Nacional de Internet será exitoso solamente si se estrechan las colaboraciones público/privadas para madurar el ecosistema IoT y colaborar con la transformación digital de los diferentes ámbitos -productivos, económicos y sociales- de Argentina.

En marzo del año 2021, se realizó el primer encuentro entre el sector público y el privado donde se compartieron experiencias sobre el desarrollo del ecosistema IoT en nuestro país y se acordaron los próximos pasos para impulsar su crecimiento.

La Subsecretaria de Economía del Conocimiento mencionó que desde el Ministerio de Producción “estamos trabajando en la oferta de las soluciones de las empresas pymes que tengan la capacidad de brindar este tipo de tecnología”. Asimismo destacó: “Las empresas pymes tienen mucha capacidad para aportar, por eso buscamos impulsar y fortalecer la exportación de este tipo de soluciones tecnológicas”.