IoT y nuevas tecnologías

Desafíos regulatorios en materia de seguridad y privacidad de datos

Federico Martínez

UNIVERSIDAD AUSTRAL
EDICIONES

Autor

- **Martínez, Federico.** Abogado por la Universidad Nacional de Tucumán. Especialista en Asesoría Jurídica de Empresas por la Universidad de Buenos Aires. Posgrado en Derecho de las Telecomunicaciones y Servicios TIC por la Asociación Argentina del Derecho de las Telecomunicaciones (AADT), con tesina publicada por dicha institución titulada *Evolución de las OTT, su relación con las ISP y la necesidad de un marco regulatorio universal*. Diplomado en Propiedad Intelectual por la Universidad Austral. Magíster en Propiedad Intelectual y Nuevas Tecnologías por la Universidad Austral. Ponente en diversas jornadas vinculadas a la implementación de tecnología en el ámbito legal. Ejerce la profesión de abogado y ha desempeñado, y actualmente desempeña, cargos gerenciales y directivos en empresas privadas de primera línea.

Índice

Resumen. El presente trabajo analiza las diferentes facetas del Internet de las cosas (*Internet of Things*, IoT), desde sus orígenes hasta su impacto actual, y en sus distintos ámbitos de aplicación, incluyendo el hogar, la industria y la sociedad en general. Asimismo, se describen los beneficios de esta tecnología, como la optimización de procesos y la automatización, pero también se examinan los riesgos que plantea, principalmente en materia de seguridad y privacidad de datos.

Se exponen las características y funciones de cada capa de la arquitectura del IoT, y se analizan las vulnerabilidades que pueden afectar a cada una de ellas, especialmente en relación con el acceso no autorizado a la información personal de los usuarios. El texto explora la normativa vigente en materia de protección de datos personales y la dificultad de regular una tecnología tan dinámica y cambiante como el IoT. En tal sentido, se destaca la necesidad de complementar la legislación actual sobre protección de datos personales con el principio de responsabilidad proactiva y los conceptos de seguridad por diseño y por defecto.

Finalmente, se plantea la necesidad de un marco regulatorio integral que aborde los desafíos que presenta esta tecnología en materia de seguridad y privacidad, además de promover el dictado de una ley específica de IoT, la adopción de estándares internacionales y la implementación de incentivos para su desarrollo responsable, destacando la importancia de concientizar y educar a la población sobre la relevancia de la privacidad y la seguridad en el uso de esta tecnología.

Palabras clave. Internet de las cosas (IoT), ciberseguridad, privacidad de datos, marco regulatorio, datos personales, vulnerabilidades tecnológicas, responsabilidad proactiva, estándares internacionales

Glosario

Abstracción de datos: proceso en el cual los datos relevantes se extraen de grandes conjuntos de datos para que las aplicaciones puedan optimizar sus operaciones.

Análisis de borde: procesamiento y análisis de datos que se realiza en el borde de la red, cerca del dispositivo IoT, en lugar de enviarlos a un servidor central en la nube.

Arquitectura IoT: describe la estructura y los componentes de un sistema IoT, incluyendo las capas de percepción, red, procesamiento y aplicación.

Asimetría de la información: situación en la que una parte tiene más información que la otra, lo que puede generar desequilibrios en las relaciones, por ejemplo, entre empresas que recopilan datos y los usuarios.

***Big data*:** grandes conjuntos de datos que son demasiado extensos o complejos para ser procesados mediante métodos tradicionales. Se requiere de tecnologías especializadas para analizarlos y extraer información valiosa.

Ciberseguridad: conjunto de herramientas, políticas y prácticas para proteger los sistemas informáticos y los datos frente a ataques maliciosos.

***Cloud computing*:** modelo de computación en el que los recursos informáticos —como servidores, almacenamiento y *software*— se proporcionan a través de Internet. Permite a empresas y organizaciones acceder a recursos de forma flexible y escalable, sin tener que invertir en infraestructura propia.

***Cookies*:** pequeños archivos de texto que los sitios web almacenan en el dispositivo del usuario para recopilar información sobre su actividad de navegación. Se utilizan para personalizar la experiencia del usuario, mostrar publicidad dirigida y realizar análisis web.

***Data analytics*:** proceso de examen de grandes conjuntos de datos con el fin de extraer información útil, identificar patrones y tendencias, y obtener conclusiones que permitan tomar decisiones informadas.

Datificación: conversión de la información en datos digitales para su procesamiento y análisis.

Domótica: conjunto de sistemas y tecnologías destinados a automatizar una vivienda, controlando la iluminación, la climatización, la seguridad y otros aspectos del hogar.

Encriptación de extremo a extremo: tipo de cifrado en el que solo el remitente y el receptor pueden leer la información transmitida, protegiéndola de accesos no autorizados.

***Edge computing*:** tecnología que permite procesar y analizar datos cerca de su fuente, en lugar de enviarlos al servidor central alojado en la nube, lo que reduce la latencia y mejora la eficiencia.

Escalabilidad: capacidad de un sistema para adaptarse al crecimiento y gestionar mayores volúmenes de datos o de usuarios sin afectar su rendimiento.

***Firmware*:** *software* integrado en un dispositivo que controla su funcionamiento básico. Es importante mantenerlo actualizado para corregir vulnerabilidades de seguridad.

***Habeas data*:** derecho que tienen las personas a acceder, rectificar y suprimir sus datos personales almacenados en bases de datos.

***Hackers*:** individuos que utilizan sus conocimientos de informática para acceder a sistemas o datos de forma no autorizada.

Huella digital: conjunto de datos que identifican de forma única a un usuario o dispositivo en el mundo digital.

Inteligencia artificial: capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, la resolución de problemas y la toma de decisiones.

Neutralidad de la red: principio que establece que los proveedores de servicios de Internet deben tratar todo el tráfico de datos de forma igualitaria, sin discriminar por contenido, aplicación o usuario.

***Malware*:** *software* malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.

***Onboarding*:** proceso de incorporación de un nuevo usuario a un sistema o servicio, generalmente implica proporcionar información personal y configurar preferencias.

Parches de seguridad: actualizaciones de *software* que corrigen vulnerabilidades de seguridad en los sistemas informáticos.

Perfilamiento: creación de un perfil de un usuario a partir de sus datos, que puede incluir información demográfica, intereses, hábitos de compra y otros datos personales.

Protocolo de interconexión: conjunto de reglas y estándares que permiten la comunicación entre dispositivos y sistemas.

Sensores: dispositivos que detectan y miden cambios en su entorno, como temperatura, movimiento, luz o sonido.

***Software*:** conjunto de programas y aplicaciones que se ejecutan en un dispositivo informático.

Tecnología 4.0: se refiere a la cuarta revolución industrial, caracterizada por la integración de tecnologías digitales en la industria, como el IoT, la inteligencia artificial y el análisis de *big data*.

Trazabilidad: capacidad de seguir el recorrido de un objeto o información a través de una cadena de suministro o proceso.

***Smart home*:** vivienda que utiliza dispositivos IoT para automatizar y controlar diversos aspectos del hogar, como la iluminación, la temperatura y la seguridad.

***Workflow*:** secuencia de pasos que se realizan para completar una tarea o proceso.