REVISTA ELECTRÓNICA DE DIREITO

RED

Recensión a Moisés Barrio, Andrés, *Internet de las cosas*, Madrid, Editorial Reus, 2022, 221 pp. (ISBN 9788429026092)

Book review of Moisés Barrio Andrés, *Internet de las cosas*, Madrid, Editorial Reus, 2022, 221 pp. (ISBN 9788429026092)

David López Jiménez

Profesor agregado, EAE Business School

Calle del Príncipe de Vergara, 156, 28002 Madrid, España

dlopez@eae.es

https://orcid.org/0000-0002-7013-9556

Diciembre 2022

RESUMO: Recensión a Moisés Barrio, Andrés, *Internet de las cosas*, Madrid, Editorial Reus, 2022, 221 pp. (ISBN 9788429026092)

PALAVRAS-CHAVE: Consumidores; Derecho; Internet de las cosas; privacidad; tecnología.

ABSTRACT: Book review of Moisés Barrio Andrés, *Internet de las cosas*, Madrid, Editorial Reus, 2022, 221 pp. (ISBN 9788429026092)

KEY WORDS: Consumers; Law; Internet of things; privacy; technology.

Recensión a Moisés Barrio, Andrés, *Internet de las cosas*, Madrid, Editorial Reus, 2022, 221 pp. (ISBN 9788429026092)

El Internet de las cosas —IoT— se encuentra vinculado con la gran transformación de la evolución de la Red. El fenómeno al que nos referimos está relacionado con la adquisición de datos de sensores, así como la transmisión de órdenes a dispositivos que son parte del mundo real. Todo ello es visible en electrodomésticos, ropas tecnológicas —wearables— o vehículos autónomos/inteligentes. Nótese que estamos ante una realidad con una enorme proyección de futuro. En la actualidad, la mayor parte del tráfico de Internet se produce por la interconexión de los objetos —y no por las personas—. Las cifras que se manejan, en cuanto al impacto económico del Internet de las cosas, son de 11 billones de euros para 2025. Con el progreso tecnológico, cada vez más dispositivos y servicios son más "inteligentes", con lo que se aumenta la interconexión tanto fuera como dentro de sus hogares y negocios. A todo ello ha coadyubado los asistentes de voz, lo que, a su vez, da lugar a nuevos retos jurídicos. En toda esta materia está desempeñando un papel significativo la inteligencia artificial.

El autor de la obra es Moisés Barrio Andrés. Es letrado del Consejo de Estado, Doctor en Derecho, Académico de diversas Universidades —Carlos III; ICADE; San Pablo CEU; y Complutense de Madrid— y abogado. Ha efectuado estudios de postgrado en la Universidad de Harvard y en London School Economics. Es también director del postgrado en Legaltech y transformación digital de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid (España). Finalmente, cabe aludir a la intensa actividad investigadora en materia de Derecho digital.

En cuanto a la sistemática de la obra, la misma ostenta un total de seis capítulos que, a continuación, se analizarán de manera somera. Los dos primeros son de carácter introductorio abordando, en un sentido amplio, los fundamentos del Internet de las cosas. Entre otros aspectos, se analiza su delimitación conceptual, riesgos, elementos técnicos, tecnologías a las que se recurre y aplicaciones prácticas actuales. Los cuatro capítulos posteriores se refieren a cuestiones particulares de este fenómeno. El tercer capítulo versa sobre la regulación legal de esta sugerente materia. El siguiente trata las cuestiones relativas a la privacidad que se suscitan. Seguidamente, el capítulo quinto alude a la seguridad en el Internet de las cosas. Por su parte, la responsabilidad en esta materia se contempla el último capítulo de la obra.

Como el autor establece, en el primer capítulo de la obra, IoT se refiere a una tecnología que se fundamenta en la conexión de objetos de toda índole a la Red que intercambian, agregan y procesan información en relación a su entorno físico con el objetivo de dar servicios de valor añadido a los usuarios. De igual forma, reconoce eventos y cambios, por lo que tales sistemas pueden reaccionar de manera autónoma y adecuada. Existen múltiples definiciones respecto al Internet de las cosas, si bien, a fecha de hoy, no hay una definición unánime. Cualquier objeto puede ser incorporado al IoT, con lo que podría ser una fuente de datos, no exenta de eventuales riesgos. Tales propiedades están modificando la manera de hacer negocios, la organización del sector público y los hábitos de millones de personas.

Los fundamentos técnicos y ciertas aplicaciones prácticas del IoT se analizan en el capítulo segundo. El fenómeno que se aborda se fundamenta en múltiples tecnologías habilitantes. Dentro de las mismas, podemos citar, sin ánimo agotador, los sistemas de identificación por radiofrecuencia —RIFD—, redes de sensores inalámbricas —WSNs—, sistemas de máquina a máquina —M2M, big data, cloud computing y software que hace uso de sistemas de inteligencia artificial —IA—. Con carácter complementario, deben considerarse las capacidades que da la tecnología blockchain y los contratos inteligentes —smart contracts—. Como el autor indica en el capítulo que se describe, el IoT es una tecnología compleja que busca la interconexión de objetos, basada en cosas materiales o inmateriales, que han sido etiquetadas para su correspondiente identificación.

La regulación jurídica del IoT se aborda en el capítulo tercero. La cuestión central a la que la presente obra se refiere, plantea problemas sui generis de regulación legal por su naturaleza interconectada y heterogénea. En toda esta situación confluyen tres elementos —tecnología, economía y derecho— que dan lugar a lo que algunos han denominado una suerte de tormenta perfecta. El IoT engloba entornos personales —ropas inteligentes y monitores médicos—, entornos domésticos —electrodomésticos inteligentes, climatización, riego del jardín, y sistemas domóticos— entornos empresariales, industriales y entornos públicos —ciudades inteligentes y redes de comunicaciones—. No puede dejarse en manos del sector privado la ordenación de esta sugerente cuestión. Los notables cambios sociales que el IoT está suscitando deben ser gestionados por los propios poderes públicos y los responsables políticos europeos. Todo ello se encuentra relacionado con la soberanía tecnológica de la Unión Europea. Debe advertirse que ni a nivel europeo ni español, existe un grupo normativo sectorial relativo al IoT ni es probable que vaya a existir en un futuro cercano. En el ámbito comunitario, cabe enunciar la Agenda Digital para Europa de 2010, y la Estrategia para el Mercado Único Digital de Europa de 2015.

Un tema nuclear que debe tenerse en consideración es la incidencia del IoT sobre la privacidad. Repárese en que los metadatos que se recopilan en los entornos del IoT afectan a lo que los individuos realizan en sus hogares; automóviles; trabajos; e incluso lugares públicos. La recopilación de datos privados de objetos y actividades cotidianas incrementa las oportunidades de vigilancia gubernamental sobre las mismas. Estamos frente a una problemática ciertamente compleja, pues debe considerarse que, en ciertas ocasiones, las personas afectadas no son conscientes de la recogida de datos ambientales por parte de los dispositivos físicos del IoT. Cabe la posibilidad de que las personas estén cerca de estos dispositivos y desconozcan su existencia. Así, a título de ejemplo, podríamos referirnos a los asistentes de voz como Alexa —Amazon—. La implantación del IoT depende, en gran medida, del respeto a la privacidad y a la protección de los datos personales.

La trascendencia de la seguridad en el IoT va más allá de la tutela de la protección de datos, convirtiéndose, de este modo, en otro de los grandes bloques de la regulación jurídica de esta sugerente materia. A todo ello se refiere el capítulo quinto. Como el autor de la obra establece, en esta materia, deben implementarse medidas de seguridad adecuadas que puedan proteger,

de manera razonable, los datos frente a ciberataques y otros incidentes informáticos. Los dispositivos del IoT son potenciales objetivos de los ciberdelincuentes, siendo, asimismo, vectores de ataque desde los que se pueden lanzar otros ciberataques.

Existen múltiples problemas de responsabilidad que tienen lugar en el IoT. Los instrumentos jurídicos tradicionales como la responsabilidad contractual, la responsabilidad por productos defectuosos y la responsabilidad extracontractual no son suficientes en el entorno en el que nos movemos. Los retos en este caso pueden limitarse a dos. En primer lugar, la necesidad de establecer un sistema ampliado de la responsabilidad por producto defectuoso. En segundo lugar, asegurar la responsabilidad proactiva en materia de protección de datos.

El IoT ha suscitado importantes avances tecnológicos y a medida que se incrementa su alcance puede impulsar la próxima revolución de Internet. En este sentido, cabe precisar que el IoT está generando unos flujos de datos tan significativos y rápidos que escapan a las capacidades humanas. Resulta conveniente encontrar el equilibrio entre fomentar esta innovación y garantizar que la seguridad y la privacidad estén protegidas, mientras está tecnología continúa desarrollándose.

La presente monografía analiza las claves tecnológicas del denominado Internet de las cosas, los eventuales riesgos y elementos disruptivos, y las aplicaciones prácticas en uso más frecuentes. Como el autor de la obra indica, el fenómeno que se examina genera nuevos y mejores modelos de negocio y procesos de gestión en todos los sectores de la economía, desde la agricultura hasta la investigación científica. De igual manera, debe considerarse que ofrece ventajas y oportunidades a los ciudadanos, a las empresas y al sector público.

En definitiva, como ha quedado patente, el Internet de las cosas constituye una realidad con un futuro prometedor. Ahora bien, en la actualidad, no cuenta con una regulación legal independiente. En este sentido, se suscitan un importante elenco de desafíos legales, sobre todo en la salvaguarda de la privacidad respecto al tratamiento de datos y la ciberseguridad de los sistemas. La obra reseñada ofrece un marco jurídico general, examinando su problemática jurídica, proponiendo sugerentes soluciones en ciertos aspectos clave. En esta materia se precisan marcos jurídicos claros, pero sobre todo europeos e internacionales para poder brindar seguridad jurídica.