IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

RESEÑA

Reseña del libro *Internet de las cosas*, de Moisés Barrio Andrés (2018), Editorial Reus

Laura Caballero Trenado
Profesora doctora (UNIR)

Fecha de publicación: febrero de 2019

La arquitectura tecnológica del IoT se basa en un conjunto heterogéneo de tecnologías habilitantes. «Uno de los bloques de construcción clave» (Barrio Andrés, 2018, pág. 33) que posibilitan el IoT es el sistema de radiofrecuencia RFDI,[1] una tecnología utilizada para identificar, rastrear y localizar recursos de forma exclusiva, precisa y automática mediante ondas de radio inalámbricas.[2]

Espoleada por la implementación de las redes móviles 5G, las posibilidades de interconexión digital de objetos, materiales e inmateriales, así como el *corolario* de aplicaciones que introduce esta tecnología (entre otras), son infinitas, pero, a su vez, los riesgos inherentes que comporta son múltiples.

En la presente investigación, que se estructura en cinco capítulos, el autor realiza en clave prospectiva una cartografía del potencial de la tecnología IoT, sus elementos disruptivos y sus riesgos.

Entre otras muchas cuestiones, responde de manera concisa y muy pedagógica a las siguientes preguntas: ¿cómo afectarán los intentos de armonizar los marcos jurídicos de privacidad y seguridad en los sistemas IoT al ritmo fotónico de la innovación?, ¿qué efectos tendrán las normas jurídicas estatales fronterizas en los sistemas y empresas de IoT transfronterizos?, ¿los operadores de servicios esenciales se adaptarán adecuadamente al crecimiento proyectado en el número de dispositivos interconectados del IoT?, o ¿hasta qué punto los ciberataques de alto nivel erosionarán la confianza de los consumidores y ralentizarán la adopción de sistemas IoT?

En el capítulo I, titulado «Introducción al internet de las cosas», el más breve de esta obra, tras contextualizar el fenómeno IoT, analiza el término, rastrea en las raíces de la paternidad del concepto (que atribuye al pionero de la tecnología británica Kevin Ashton), y perfila y delimita sus características (en apretada síntesis: comunicación y cooperación, identificación, direccionamiento, detección, actuación o procesamiento de información integrado).

1. *Radio Frequency Identification*.
2. *Ibidem*.

Cierra este primer capítulo introductorio un elenco de los principales riesgos que presenta esta nueva tecnología, resultado de una compilación de la literatura doctrinal consolidada breve pero muy completa.

El «potencial catálogo de peligros» sitúa el eventual menoscabo de los bienes jurídicos privacidad e intimidad en el vértice de los mismos. Otros riesgos que se reseñan son la creciente fascinación por las TIC, por cuanto a medida que el IoT prolifere podría capturar a los usuarios y convertirlos en «rehenes»; la dependencia tecnológica; la impredicibilidad; la subordinación y la brecha tecnológica, categorizadora potencial de usuarios de primera (países con producción tecnológica propia) y de segunda, o el aumento de la cibercriminalidad.

La criminalidad es consustancial a todos los tiempos y, aunque el derecho penal se ha ido adaptando a través de la incorporación en los textos punitivos de tipificaciones de distintas figuras delictuales, es un hecho que el derecho va siempre a remolque de la realidad criminal. No resulta sencillo, pues, incardinar la ciberdelincuencia y el universo de delitos tecnológicos, que constituyen una realidad mutante, en la rígida normativa del sistema punitivo. De hecho, algunos de los ciberdelitos están plagados de confusas remisiones y una técnica legislativa mejorable, cuando no están adecuadamente ubicados, lo que conduce a afirmar que la reforma operada por el legislador español en 2015 adolece de cierta rotundidad.

Como puede comprobarse fácilmente, los retos que plantea la tecnología IoT se acumulan tanto para los legisladores como para el conjunto de operadores jurídicos, de ahí que resulte esencial, en primer lugar, tener un conocimiento amplio de las cuestiones técnicas.

De ello se ocupa el siguiente Capítulo, cuya rúbrica es «Fundamentos técnicos y algunas aplicaciones actuales del internet de las cosas». Sorprende la facilidad con la que conecta el lector, que orilla enfrascarse en tecnicismos, gracias a la prosa natural y didáctica del texto, que avanza en fluidez.

El autor proyecta los trazos de un futuro que se visualiza muy presente, pues, con el cincel de un escultor y la pericia de un entomólogo, diseccionа las claves y esculpe los escenarios que posibilitan los ecosistemas del IoT a través de autopistas virtuales interconectadas. Desde hogares inteligentes, con frigoríficos que avisan al usuario de cuándo necesita reponer leche, a ropa inteligente (*wearables*), automóviles autónomos con suministro de conectividad a internet o contadores inteligentes, que permiten individualizar, priorizar y empaquetar mercancías y clientes, *smart cities*, etcétera.

Para Barrio Andrés, «el conjunto de estas tecnologías forma una *red ubicua* caracterizada por una integración automática de conexiones entre objetos equipados con sensores o etiquetas inteligentes, capaces de detectarse y entrar en comunicación» (*op. cit.*, pág. 49) por lo que afirma, en clave de advertencia: «Esta recolección de datos omnipresente se caracteriza por su falta de visibilidad y transparencia, motivada por diversos factores de los cuales destacaremos dos: el propio diseño de la tecnología, que busca ser autónoma y le resta control al usuario, y la multitud de actores e intermediarios involucrados, tanto de ámbito público como privado. De esta forma, cada vez estará menos claro quién tiene el control de los datos y quién tiene acceso a ellos».[3]

El capítulo III, que lleva por título «Regulación jurídica del internet de las cosas», concentra la problemática jurídica que plantea esta nueva tecnología.

3. *Ibidem*.

Tras llamar la atención sobre la dificultad que entraña amoldar las especificidades del IoT en el plano legal, sitúa el análisis jurídico desde la atalaya tecnológica, cuyos elementos estructurales abonan, dan consistencia y nutren a esa tecnología, a la par que originan efectos jurídicos concretos.

Entre los componentes de los elementos jurídicamente relevantes, destacan los siguientes: la conectividad, la interoperabilidad y la necesidad de emplear un conjunto de protocolos que la hacen posible, los algoritmos, los datos y la información (la materia prima del IoT), la portabilidad, la utilización de software abierto o la impresión 3D.

El capítulo, que también analiza la cadena de actores involucrados en el ecosistema del internet de las cosas (desde fabricantes a proveedores de plataformas y desarrolladores de aplicaciones), incluye un repaso de los antecedentes del desarrollo de esta tecnología, que cristalizaron en iniciativas de índole diversa por parte del legislador europeo, así como de otras instituciones y organismos internacionales públicos y privados.

En el epígrafe titulado «Marco jurídico general», el autor advierte de los riesgos que supone dejar el desarrollo de esta tecnología en manos de la iniciativa privada exclusivamente, pues muchos de estos cambios deben involucrar también a los poderes públicos, responsables políticos y a ciudadanos.

En el seno de la UE, en el marco del conjunto de iniciativas diseñadas para fomentar el Mercado único digital, destaca la publicación del trabajo *Avanzando el Internet de las Cosas* en Europa, en abril de 2016, lo que da cuenta del deseo del legislador de potenciar la introducción de esta tecnología. Cierra este capítulo una relación de la normativa sectorial aplicable en España.

De cuestiones eminentemente jurídicas se ocupa también el capítulo IV, rubricado «La privacidad y la protección de datos en el internet de las cosas», en el que aborda los retos que plantea la introducción de esta nueva tecnología, que amplía la delimitación de la intimidad y la privacidad.

La promulgación del RGPD constata la apuesta del legislador europeo por un estándar de protección reforzado, pero su ejecución suscita muchas preocupaciones (por ejemplo, la prestación del consentimiento) y comporta numerosos retos para los operadores jurídicos, habida cuenta de la naturaleza del internet de las cosas, «marcado por las propias características seminales de esta tecnología».[4] Quién sabe, tal vez, alumbrado en el oxímoron de cuerpo legal obsoleto, este instrumento normativo acaso tenga poco recorrido, pues fue concebido y desarrollado sin tener en cuenta la nueva realidad tecnológica.

Con frecuencia, los avances tecnológicos trastocan los principios regulatorios que presiden los ordenamientos jurídicos. Lejos de mantenerse al margen en actitud pasiva y neutral, las autoridades reguladoras deben llevar a cabo acciones tuitivas encaminadas a proteger intereses clave.

De esta cuestión, entre otras, se ocupa el último capítulo del libro («La seguridad en el internet de las cosas»).

Con carácter general, el conjunto de paquetes regulatorios que está introduciendo el legislador adelantan la responsabilidad de los titulares de los sistemas de IoT, que ha basculado de activa a proactiva,

4. *Op. cit*., pág. 72.

e implican una apuesta decidida por la seguridad, que se ha concretado en el establecimiento de unos requisitos comunes de seguridad mínimos para operadores de servicios esenciales y proveedores de servicios digitales.

Sin embargo, IoT introduce desafíos únicos. Cuatro son para el autor las vulnerabilidades principales que, eventualmente, pueden derivarse de la inexistencia de cifrado en las comunicaciones, de insuficientes mecanismos de autenticación y autorización, de la utilización de interfaces web inseguros, así como de software y *firmware* (el software encargado de controlar el hardware para que las instrucciones externas se ejecuten de manera correcta) inseguros.

La cuestión de la seguridad es crítica, de ahí la importancia del desarrollo de la futura ley española sobre seguridad de redes y, sobre todo, de la IoT Cibersecurity Improvement Act, de 2017. Al igual que otra normativa inherente a internet, probablemente se convierta, en opinión del autor (convencimiento que comparto) en la norma *de facto* a escala mundial.

Pone el broche de oro a esta obra, que atesora excelencia, un epílogo en el que el autor esboza las cuestiones que urge abordar para algo, el internet de las cosas, «que lleva cierto tiempo entre nosotros»[5] y que pueden resumirse, a riesgo de simplificación, en la necesidad de elaborar estándares tecnológicos y jurídicos que provean entornos seguros y fiables.

La obra de Moisés Barrio Andrés se anticipa a una realidad –un ecosistema virtual interconectado invisiblemente– y crea la necesidad de propiciar un nuevo entorno regulatorio que ahorme la dimensión poliédrica que introduce la tecnología IoT.

Cita recomendada

CABALLERO TRENADO, Laura (2019). «Reseña del libro *Internet de las cosas*, de Moisés Barrio Andrés (2018), Editorial Reus». *IDP. Revista de Internet, Derecho y Política*. N.º 28, págs. 127-131. UOC. [Fecha de consulta: dd/mm/aa]
‹http://dx.doi.org/10.7238/idp.v0i28.3181›

5. *Op. cit*., pág.117.

Sobre la autora
Laura Caballero Trenado
laucab01@ucm.es

Profesora doctora
Universidad Internacional de la Rioja

Profesora de Propiedad Intelectual y Nuevas Tecnologías y de Gestión y Comercialización de los Derechos de Propiedad Intelectual en el máster en Propiedad Intelectual y Derecho de las Nuevas Tecnologías de la Universidad Internacional de La Rioja. Actualmente ejerce como asesora legal de *Tech Law* & *Entertainment Law* (Propiedad Intelectual e Industrial, Nuevas Tecnologías, PD y Derecho al Honor, Intimidad e Imagen, *eSports* y Audiovisual). Previamente, ha trabajado en el Departamento Internacional de la Entidad de Gestión Colectiva AISGE.

Miembro del Comité Científico de *Common Ground Research Networks* (University of Illinois), ha impartido docencia en centros académicos de reconocido prestigio, como la Universidad Metropolitana de Puerto Rico, CTY Spain (Johns Hopkins University), USC University y las universidades CEU.

Fulbrighter (EE. UU., 2010-2011), es doctora en Ciencias de la Comunicación, con Premio Extraordinario (Universidad CEU), graduada en Derecho y máster en Acceso a la Abogacía (Universidad Complutense); ha cursado el máster en International Relations y el Programa Avanzado en Entertainment Law (IE Business School).

Calle Almansa, 101
28040 Madrid