

INTERNET DE LAS COSAS

Moisés Barrio Andrés

2ª edición

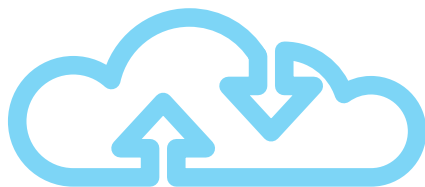


INTERNET DE LAS COSAS

Moisés Barrio Andrés

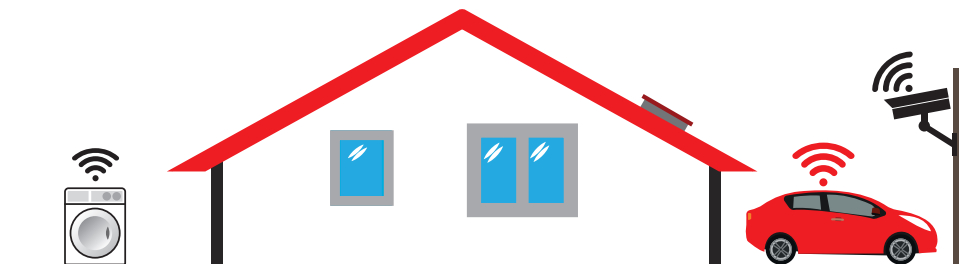
Letrado del Consejo de Estado
Doctor en Derecho
Profesor en las Universidades Carlos III, ICADE,
CEU-San Pablo y Complutense de Madrid
Abogado y consultor

Segunda edición



REUS
EDITORIAL

Madrid, 2020



© Moisés Barrio Andrés
© Editorial Reus, S.A. para la presente edición
C/ Rafael Calvo, 18, 2º C – 28010 Madrid
Teléfonos: (34) 91 521 36 19 – (34) 91 522 30 54

reus@editorialreus.es
www.editorialreus.es
2.ª edición REUS, S.A. (2020)
ISBN: 978-84-290-2200-1
Depósito Legal: M-5672-2020
Diseño de portada: Amanda Guglieri
Impreso en España

Imprime: *Estilo Estugraf Impresores S.L.*

Editorial Reus no responde del contenido de los textos impresos, cuya originalidad garantizan sus autores. Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra sólo puede ser realizada con la autorización expresa de Editorial Reus, salvo excepción prevista por la ley. Fotocopiar o reproducir ilegalmente la presente obra es un delito castigado con cárcel en el vigente Código penal español.

*A Álvaro y Roberto, visionarios
y emprendedores de éxito*

*A Amanda Olivia Guglieri Lillo, del equipo editorial,
por su esmerado diseño de portada
y las atinadas sugerencias formuladas*

ABREVIATURAS

ADPIC.	Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, de 15 de abril de 1994.
AIOTI.	Alliance for Internet of Things Innovation.
APIs.	Application Programming Interfaces.
CBPOLA.	Convenio de Berna para la Protección de las Obras Literarias y Artísticas, de 9 de septiembre de 1886.
CC.	Código Civil español.
CDM.	Collaborative Decision Making.
CERT.	Computer Emergency Response Team.
CNPIC.	Centro Nacional para la Protección de las Infraestructuras Críticas.
CSIRT.	Computer Security Incident Response Team.
DC-IoT.	Dynamic Coalition on the Internet of Things.
Directiva marco de telecomunicaciones.	Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, sustituida por la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.
Directiva NIS.	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
DNS.	Domain Name System.
DSM.	Vid.

ENISA.	Agencia de la Unión Europea para la Ciberseguridad.
EPC.	Electronic Product Code.
EPCIS.	Electronic Product Code Information Services.
FTC.	Federal Trade Commission.
ICT.	Vid. TIC.
IERC.	European Research Cluster on the Internet of Things.
IoT.	Internet of Things.
ITU.	Vid. UIT.
LEC.	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
LMPIC.	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
LOPD.	Anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LOPDGDD.	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LSEN.	Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
LSN.	Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
M2M.	Machine-to-Machine.
MUD.	Mercado Único Digital de Europa.
NFC.	Near Field Communication.
OMC.	Organización Mundial del Comercio.
ONS.	Object Naming Service.
ONU.	Organización de las Naciones Unidas.
Reglamento e-privacy.	Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).
RFID.	Radio Frequency Identification.

- RGPDE. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- RLOPD. Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- SCADA. Supervisory Control and Data Acquisition.
- SOA. Service Oriented Architecture.
- TIC. Tecnologías de la Información y la Comunicación.
- UIT. Unión Internacional de Telecomunicaciones.
- WSNs. Wireless sensor networks.

PRÓLOGO A LA PRIMERA EDICIÓN

El «Internet de las Cosas» (*Internet of Things*, habitualmente referido por sus siglas inglesas IoT), también denominado por algunos «Internet de los Objetos» (IO) es un supraconcepto que caracteriza la próxima gran transformación en la evolución de Internet¹: su expansión más allá de la comunicación entre las personas, o entre las personas y el contenido digital, que ahora se extiende a miles de millones de objetos cotidianos. Los sistemas IoT implican la adquisición de datos de sensores y la entrega de órdenes a dispositivos que interactúan o forman parte del mundo real. También reconocen eventos y cambios, y pueden reaccionar de forma autónoma y apropiada. El Internet de las Cosas se equipara a menudo con electrodomésticos y bienes de consumo, como las ropas tecnológicas (*wearables*) o los coches inteligentes. Por lo tanto, muchas de las preocupaciones iniciales se han centrado en los productos de consumo.

La atención a este fenómeno es urgente por muchas razones. La mayor parte del tráfico actual de Internet ya es originado por la interconexión de los objetos, no de las personas, y las proyecciones globales del impacto económico del IoT son potencialmente de once billones de euros para 2025². También es apremiante porque la expansión de Internet en objetos cotidianos utilizados por las personas crea retos de interés público sin precedentes sobre cómo también transformará la intimidad-privacidad y la seguridad humana (incluyendo la ciberseguridad).

¹ Nos hemos ocupado ampliamente de ello en BARRIO ANDRÉS, Moisés: *Fundamentos del Derecho de Internet*. Editorial Centro de Estudios Políticos y Constitucionales, Madrid, 2017.

² MANYIKA, James (dir): «Unlocking the potential of the Internet of Things». Informe del *McKinsey Global Institute*, de junio de 2015. Disponible en <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>

Ahora bien, la exclusiva atención a los productos de consumo desconoce que la mayor parte de aplicaciones del Internet de las Cosas se ha producido fuera del ámbito doméstico. En efecto, la gran mayoría de usos del IoT se encuentran en casi todos los sectores industriales. Las suministradoras de gas y petróleo por ejemplo dependen de sensores de energía interconectados digitalmente. Las empresas de transporte y navegación utilizan tecnologías de IoT para el seguimiento de vehículos y paquetes. Los sistemas médicos se basan cada vez más en dispositivos de monitorización, diagnóstico y tratamiento conectados a Internet. Las empresas manufactureras emplean sistemas IoT para gestionar el manejo de materiales, la optimización de inventarios y la conexión de sistemas robóticos. Las administraciones locales son cada vez más un ámbito relevante del IoT en el sentido de que los servicios públicos municipales, el alumbrado, los sistemas de control del tráfico y otras aplicaciones inteligentes de las *smart cities*³ forman ahora parte del ecosistema del Internet de las Cosas. Todos los sectores económicos, desde la agricultura hasta la venta al por menor, hoy son entornos en los que el ciberespacio “toca” el mundo físico. Y estos sistemas de IoT, aunque a menudo utilizan algunas tecnologías patentadas, también dependen de los protocolos subyacentes y de las infraestructuras abiertas de red de Internet o se conectan a Internet para funciones de administración y control.

Por todo ello, este libro examina las claves tecnológicas del Internet de las Cosas, sus riesgos y elementos disruptivos, así como también las aplicaciones prácticas ya en uso más frecuentes. Hay que tener en cuenta cómo el IoT tiene el potencial para generar nuevos y mejores modelos de negocio y procesos de gestión en prácticamente todos los sectores de la economía, desde la agricultura hasta la investigación científica de vanguardia, y ofrece asimismo ventajas y oportunidades sin precedentes a los ciudadanos individuales, a las empresas y a las administraciones públicas.

Pero, en verdad, el Internet de las Cosas carece de una regulación jurídica propia y autónoma. Sin embargo, plantea un buen ramillete de nuevos desafíos legales, fundamentalmente en la protección de la intimidad-privacidad en relación con el tratamiento de datos y la

³ BARRIO ANDRES, Moisés: «La smart city: versión 2.0 del municipio», en *Documentación Administrativa: Nueva Época*, Nº 3, 2016.

ciberseguridad de los sistemas. Ante la falta de un grupo normativo particular, este libro ofrece también un marco jurídico general, examinando asimismo su problemática jurídica y proponiendo, igualmente, soluciones prácticas en aspectos claves como son los relativos a la titularidad de los datos recopilados y generados en entornos IoT, la circulación y el acceso a los datos, o incluso la evaluación de impacto para asegurar el *compliance* de los sistemas del Internet de las Cosas por parte de los fabricantes, integradores y demás actores involucrados.

Madrid-Cambridge (Massachusetts, Estados Unidos), febrero de 2018.

Moisés BARRIO ANDRÉS
Letrado del Consejo de Estado
Doctor en Derecho
Profesor de Derecho
Abogado
www.moisesbarrio.es
 @moisesbarrioa




PRÓLOGO A LA SEGUNDA EDICIÓN

La gran acogida por los lectores a la primera edición de la obra motivó que se agotara a los pocos meses, e incluso ha sido seguida de varias reimpressiones posteriores.

Esta segunda edición no sólo incluye las novedades legislativas acaecidas con posterioridad en los ámbitos de protección de datos y ciberseguridad, sino que también incorpora un nuevo capítulo relativo a la responsabilidad en el ámbito del Internet de las Cosas. Asimismo, todos los hipervínculos están operativos a fecha 22 de diciembre de 2019.

Concluyo este prólogo agradeciendo a varios amables lectores las sugerencias enviadas respecto a áreas puntuales que estaban necesitadas de ampliación. Esa es la auténtica finalidad de esta obra: tratar de ser un instrumento útil y práctico en una materia cambiante, compleja, extensa y excepcionalmente atractiva.

Madrid-Lima (Perú), diciembre de 2019.

Moisés BARRIO ANDRÉS
Letrado del Consejo de Estado
Doctor en Derecho
Profesor de Derecho
Abogado y consultor
www.moisesbarrio.es
 @moisesbarrioa



ÍNDICE

ABREVIATURAS	9
PRÓLOGO A LA PRIMERA EDICIÓN	13
PRÓLOGO A LA SEGUNDA EDICIÓN	17
CAPÍTULO I - INTRODUCCIÓN AL INTERNET DE LAS COSAS	19
1. INTRODUCCIÓN	19
2. CONCEPTO	21
3. CARACTERÍSTICAS	26
4. RIESGOS.....	29
CAPÍTULO II - FUNDAMENTOS TÉCNICOS Y ALGUNAS APLICACIONES DEL INTERNET DE LAS COSAS	35
1. INTRODUCCIÓN	35
2. ELEMENTOS TÉCNICOS	37
2.1. Hardware específico: sensores, actuadores y controladores.....	38
2.2. Radio Frequency Identification (RFID)	39
2.3. Electronic Product Code (EPC)	39
2.4. Object Naming Service (ONS)	41
2.5. EPC Discovery Service	42
2.6. Capa de comunicaciones	43
3. OTRAS TECNOLOGÍAS EMPLEADAS EN EL INTERNET DE LAS COSAS	43
3.1. Service Oriented Architecture (SOA)	43
3.2. Collaborative Decision Making (CDM).....	44
3.3. Cloud Computing	45
3.4. Big Data.....	45
3.5. Blockchain y smart contracts	46
4. ALGUNAS APLICACIONES ACTUALES DEL INTERNET DE LAS COSAS	49
4.1. Juguetes	50

4.2. Ropas tecnológicas (<i>wearables</i>).....	50
4.3. Transporte	51
4.4. Contadores inteligentes	52
4.5. Monitorización agrícola y ganadera.....	54
CAPÍTULO III - REGULACIÓN JURÍDICA DEL INTERNET DE LAS COSAS	57
1. INTRODUCCIÓN.....	57
2. ELEMENTOS JURÍDICAMENTE RELEVANTES	58
3. SUJETOS INVOLUCRADOS	63
3.1. Fabricantes de dispositivos.....	64
3.2. Proveedores de plataformas.....	64
3.3. Desarrolladores de aplicaciones	64
3.4. Integradores	65
4. ANTECEDENTES	65
4.1. Comisión Europea	65
4.2. Alliance for Internet of Things Innovation	67
4.3. European Research Cluster on the Internet of Things.....	68
4.4. Federal Trade Commission.....	69
4.5. Unión Internacional de Telecomunicaciones	71
4.6. Dynamic Coalition on the Internet of Things.....	71
5. MARCO JURÍDICO GENERAL	72
CAPÍTULO IV - LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS EN EL INTERNET DE LAS COSAS	79
1. INTRODUCCIÓN	79
2. RÉGIMEN JURÍDICO.....	84
3. PROPIEDAD DE LOS DATOS	88
3.1. Propiedad colectiva.....	89
3.2. Portabilidad de los datos	90
3.3. Acceso a los datos	91
3.4. Intercambio y explotación de datos	94
3.5. Hacia un marco normativo	95
4. RETOS SUSCITADOS	98
CAPÍTULO V - LA SEGURIDAD EN EL INTERNET DE LAS COSAS	109
1. INTRODUCCIÓN	109
2. RÉGIMEN JURÍDICO.....	111
3. RETOS SUSCITADOS	125

CAPÍTULO VI - LA RESPONSABILIDAD EN EL INTERNET DE LAS COSAS	131
1. INTRODUCCIÓN	131
2. RÉGIMEN JURÍDICO.....	134
2.1. Responsabilidad contractual.....	138
2.2. Responsabilidad por productos defectuosos	139
2.3. Responsabilidad extracontractual.....	143
2.4. Protección de datos	145
3. RETOS SUSCITADOS	146
EPÍLOGO	149
BIBLIOGRAFÍA GENERAL	155

El Internet de las Cosas («IoT» por sus siglas en inglés) es la próxima revolución en un mundo cada vez más interconectado. Todo, desde prendas tecnológicas o electrodomésticos hasta ciudades inteligentes o infraestructuras públicas, está aprovechando el potencial de esta tecnología en beneficio de los ciudadanos, las empresas y las administraciones públicas, pero también acarrea amenazas crecientes a la intimidad-privacidad y a la seguridad.

Este libro examina primero las claves tecnológicas del Internet de las Cosas, sus riesgos y elementos disruptivos, así como también las aplicaciones prácticas más frecuentes ya en uso, que incluye sistemas con blockchain y smart contracts. En segundo lugar, y dado que el Internet de las Cosas carece de una regulación propia, la obra analiza los marcos legales aplicables y también propone soluciones jurídicas a los problemas que esta tecnología está planteando.

La obra no solo es de gran interés para los abogados y los demás operadores jurídicos, sino también para todos aquellos profesionales de las ciencias sociales y asimismo del sector tecnológico, ya que ofrece un enfoque global que aborda los problemas junto con respuestas prácticas para dar sentido a estos cambios y, lo que es más importante, para entender cómo incorporarlos de una forma jurídicamente adecuada y eficaz.

Esta segunda edición incorpora las novedades legislativas que se han producido en materia de protección de datos y ciberseguridad, e incluye un nuevo capítulo sobre la responsabilidad en el IoT.



REUS
EDITORIAL

