

INTERNET DE LAS COSAS

Moisés Barrio Andrés

3ª edición



INTERNET DE LAS COSAS

Moisés Barrio Andrés

Letrado del Consejo de Estado

Doctor en Derecho

Director del Diploma de Alta Especialización en Legal Tech y transformación digital (DAELT), de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid
Profesor en las Universidades Carlos III, ICADE, CEU-San Pablo y Complutense de Madrid
Abogado y consultor

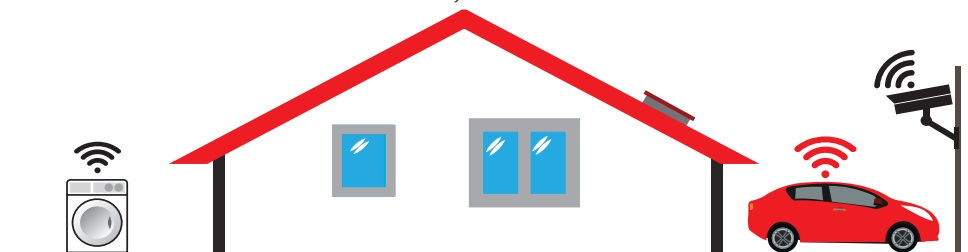
TERCERA EDICIÓN



REUS

EDITORIAL

Madrid, 2022



© 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

3.ª edición REUS, S.A. (2022)
ISBN: 978-84-290-2609-2
Depósito Legal: M-4332-2022
Diseño de portada: Amanda Guglieri

Impreso en España
Imprime: *Ulzama Digital*.

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 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. MUD.
ENISA.	Agencia de la Unión Europea para la Ciberseguridad.
EPC.	Electronic Product Code.
EPCIS.	Electronic Product Code Information Services.
FTC.	Federal Trade Commission.
IA.	Inteligencia Artificial.
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. Vid. LOPDGDD.
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.
LSSI.	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
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 del Parlamento Europeo y del Consejo 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).

Reglamento IA.	Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial o Artificial Intelligence Act) y se modifican determinados actos legislativos de la Unión.
RFID.	Radio Frequency Identification.
RGPDE/ RGPD.	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 Adquisition.
SOA.	Service Oriented Architecture.
TIC.	Tecnologías de la Información y la Comunicación.
TRLGDCU.	Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre.
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 transfor-

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. Hay una segunda edición de 2020. También BARRIO ANDRÉS, Moisés: *Manual de Derecho digital*. Editorial Tirant lo Blanch, Valencia, 2020.

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>.

mará la intimidad-privacidad y la seguridad humana (incluyendo la ciberseguridad).

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

³ BARRIO ANDRES, Moisés: «La smart city: versión 2.0 del municipio», en *Documentación Administrativa: Nueva Época*, N.º 3, 2016.

nuevos desafíos legales, fundamentalmente en la protección de la intimidad-privacidad en relación con el tratamiento de datos y la 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 y consultor
<https://www.moisesarrio.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 reimpresiones 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, diciembre de 2019.

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



PRÓLOGO A LA TERCERA EDICIÓN

Esta tercera edición es consecuencia y tributo a la cálida acogida que esta obra ha tenido tanto en España como en Latinoamérica. De hecho, constituye uno de mis libros más citados. Quiero por ello volver a reiterar mi gratitud a los lectores por este éxito editorial.

Los dos años transcurridos desde la edición anterior han puesto de relieve cómo un número cada vez mayor de dispositivos y servicios se están volviendo mucho más “inteligentes”. Gracias a esta evolución, los usuarios pueden acceder a una gama cada vez más amplia de aquéllos, aumentándose también su interconexión dentro y fuera de sus hogares y negocios. También se ha producido una mayor disponibilidad y proliferación de los asistentes de voz como interfaz de usuario que permite la interacción con los objetos inteligentes y los servicios del IoT de consumo y del hogar inteligente, lo cual suscita nuevos retos jurídicos en lo que se refiere a la estandarización, la interoperabilidad y varias cuestiones de Derecho de la Competencia, entre otros.

En suma, la progresiva extensión del Internet de las Cosas convierte a las cosas en *infómatas*, es decir, en actores que procesan información. El mundo digital cada vez se hibrida de manera más profunda con el mundo real, hasta el punto de confundirse entre sí, haciendo la existencia humana cada vez más intangible y fugaz. Así ha sucedido ya en Internet con la convergencia tecnológica, donde la tradicional línea de cobre telefónica hoy es un servicio más de Internet, la VozIP, como el correo electrónico o la Web. Incluso, más a medio plazo⁴, los avances en el conocimiento del cerebro, en combinación con el progreso de la inteligencia artificial, las interfaces persona-máquina y la

⁴ Sobre ello, ya nos pronunciábamos en las dos ediciones de BARRIO ANDRÉS, Moisés (dir.): *Derecho de los Robots*. Editorial Wolters Kluwer, Madrid, 2019, 2ª edición, en especial pág. 130 y ss.

computación en sus variedades clásica y cuántica están generando un panorama en el que podremos manejar los sistemas IoT directamente con la mente, además de alimentar nuestros circuitos neuronales con información generada en el mundo externo, también con habilidades aprendidas por terceros en nuestro lugar.

Por el momento, en el año 2022, los dispositivos del IoT nos cuidan y se preocupan por nosotros. La inteligencia artificial, que progresivamente se va incorporando a los mismos, optimiza la vida y nos descarga de preocupaciones. Así, el hogar inteligente (o *smart home*) supone una mayor comodidad, eficiencia energética, seguridad y facilidad a la hora de disfrutar de nuestra casa. Tener una *smart home* es muy sencillo hoy en día, ya que no es necesario modificar nuestra residencia para dotarla de inteligencia. El hardware requerido cada vez resulta más asequible y son muy pocos los cambios precisados.

Pero la vivienda inteligente prolonga la monitorización y vigilancia también durante las horas de sueño. La vigilancia se va imponiendo de modo creciente y subrepticio en la vida cotidiana, como si fuera lo conveniente y sin una reflexión meditada. Las cosas del IoT se revelan como informadores eficientes que nos controlan y espían constantemente. Por eso, también hay una mayor intranquilidad por los riesgos que plantea esta tecnología. En 2021, el 13 % de los ciudadanos en la UE⁵ esgrimió la preocupación por la privacidad y la protección de los datos personales generados por los dispositivos y sistemas del IoT como su razón para no utilizar esta tecnología personalmente o en su hogar. En esta dirección, los factores de calidad, ciberseguridad, privacidad y soporte técnico son los elementos competitivos más relevantes y apreciados por los usuarios a la hora de escoger la concreta solución de IoT en particular.

Esta nueva edición supone una puesta al día de todos los contenidos. Incluye las novedades normativas en materia de regulación de la IA y las modificaciones operadas en el TRLGDCU por el Real Decreto-ley 7/2021, de 27 de abril. A ello hay que sumar la pandemia del *COVID-19*, que ha suscitado inéditas controversias en el ámbito del Internet de las Cosas. En efecto, la pandemia no es únicamente una emergencia de salud pública, sino que ha obligado a reevaluar hasta

⁵ Eurostat disponible en https://ec.europa.eu/eurostat/databrowser/view/isoc_iiot_bx/.

qué punto la protección de datos debe ceder ante las amenazas a la salud pública y las innovaciones tecnológicas resultantes que ofrece el IoT. Y ha planteado la cuestión de si los marcos legales que rigen la privacidad deben flexibilizarse para hacer frente a los problemas de salud pública, y si tal flexibilización continuará después de la pandemia para socavar permanentemente nuestra intimidad.

Confío que este libro siga teniendo benévola acogida por parte de estudiosos y prácticos del Derecho, así como de otras disciplinas.

Madrid, enero de 2022.

Moisés BARRIO ANDRÉS
Letrado del Consejo de Estado
Doctor en Derecho. Profesor de Derecho
Abogado y consultor
<https://www.moisesarrio.es>
 @moisesbarrioa



ÍNDICE

ABREVIATURAS	7
PRÓLOGO A LA PRIMERA EDICIÓN	11
PRÓLOGO A LA SEGUNDA EDICIÓN.....	15
PRÓLOGO A LA TERCERA EDICIÓN.....	17
CAPÍTULO I. INTRODUCCIÓN AL INTERNET DE LAS COSAS .	21
1. INTRODUCCIÓN	21
2. CONCEPTO	23
3. CARACTERÍSTICAS	29
4. RIESGOS.....	32
CAPÍTULO II. FUNDAMENTOS TÉCNICOS Y ALGUNAS APLI- CACIONES ACTUALES DEL INTERNET DE LAS COSAS	41
1. INTRODUCCIÓN	41
2. ELEMENTOS TÉCNICOS	43
2.1. Hardware específico: sensores, actuadores y controladores.....	44
2.2. Radio Frequency Identification (RFID).....	45
2.3. Electronic Product Code (EPC)	46
2.4. Object Naming Service (ONS)	47
2.5. EPC Discovery Service.....	48
2.6. Capa de comunicaciones.....	49
3. OTRAS TECNOLOGÍAS EMPLEADAS EN EL INTERNET DE LAS COSAS	49
3.1. Service Oriented Architecture (SOA)	50
3.2. Collaborative Decision Making (CDM)	50
3.3. Cloud Computing.....	51
3.4. Big Data	52
3.5. Blockchain y smart contracts.....	53
4. ALGUNAS APLICACIONES ACTUALES DEL INTERNET DE LAS COSAS	56
4.1. Juguetes	57

4.2. Ropas tecnológicas (wearables).....	58
4.3. Hogar inteligente.....	59
4.4. Transporte.....	61
4.5. Contadores inteligentes.....	62
4.6. Smart cities.....	64
4.7. Monitorización agrícola y ganadera	64
CAPÍTULO III. REGULACIÓN JURÍDICA DEL INTERNET DE LAS COSAS	67
1. INTRODUCCIÓN.....	67
2. ELEMENTOS JURÍDICAMENTE RELEVANTES	68
3. SUJETOS INVOLUCRADOS	74
3.1. Fabricantes de dispositivos	75
3.2. Proveedores de plataformas	75
3.3. Desarrolladores de aplicaciones.....	76
3.4. Integradores.....	76
4. ANTECEDENTES	77
4.1. Unión Europea	77
4.2. Alliance for Internet of Things Innovation.....	80
4.3. European Research Cluster on the Internet of Things.....	81
4.4. Estados Unidos.....	82
4.5. Unión Internacional de Telecomunicaciones	85
4.6. Dynamic Coalition on the Internet of Things.....	85
5. ESTANDARIZACIÓN	86
6. MARCO JURÍDICO GENERAL	90
CAPÍTULO IV. LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS EN EL INTERNET DE LAS COSAS	99
1. INTRODUCCIÓN.....	99
2. RÉGIMEN JURÍDICO.....	106
3. PROPIEDAD DE LOS DATOS	112
3.1. Propiedad colectiva	114
3.2. Portabilidad de los datos.....	115
3.3. Acceso a los datos.....	117
3.4. Intercambio y explotación de datos	120
3.5. Hacia un marco normativo.....	121
4. RETOS SUSCITADOS	126
CAPÍTULO V. LA SEGURIDAD EN EL INTERNET DE LAS COSAS	139
1. INTRODUCCIÓN.....	139
2. RÉGIMEN JURÍDICO.....	142
2.1. Directiva NIS.....	143
2.2. Reglamento europeo de ciberseguridad	149

2.3. Marco general en España.....	154
2.4. Protección de infraestructuras críticas.....	155
2.5. Seguridad Nacional.....	157
2.6. Trasposición de la Directiva NIS.....	159
3. RETOS SUSCITADOS.....	163
CAPÍTULO VI. LA RESPONSABILIDAD EN EL INTERNET DE LAS COSAS.....	169
1. INTRODUCCIÓN.....	169
2. RÉGIMEN JURÍDICO.....	172
2.1. Responsabilidad contractual.....	176
2.2. Responsabilidad por productos defectuosos.....	178
2.3. Responsabilidad por compraventa de bienes y de suministro de contenidos o servicios digitales.....	186
2.4. Responsabilidad extracontractual.....	191
2.5. Protección de datos.....	192
2.6. Ciberseguridad.....	194
3. RETOS SUSCITADOS.....	195
EPÍLOGO.....	199
BIBLIOGRAFÍA GENERAL.....	209

El Internet de las Cosas («IoT» por sus siglas en inglés) es la nueva revolución en nuestro 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 y 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 tercera edición incorpora las novedades legislativas que se han producido en la materia, tanto en la UE como en España

REUS
EDITORIAL

ISBN 978-84-290-2609-2



9 788429 026092