

EL IMPACTO DE

INTERNET DE LAS COSAS

EN LA CIUDADANÍA EUROPEA

Coordinador

Rafael Rodríguez Prieto



Este libro ha sido financiado por el Fondo Europeo de Desarrollo Regional (FEDER) y por la Consejería de Economía, Conocimiento, Empresas y Universidad, de la Junta de Andalucía, en marco del programa operativo FEDER Andalucía 2014-2020. Objetivo específico 1.2.3. «Fomento y generación de conocimiento frontera y de conocimiento orientado a los retos de la sociedad, desarrollo de tecnologías emergentes») en marco del Proyecto UPO-1380664: Impacto del internet de las cosas sobre la ciudadanía europea (IDICCE). Porcentaje de cofinanciación FEDER 80%.



UNIVERSIDAD
PABLO DE OLAVIDE





eBook gratuito en COLEX Online

- Acceda a la página web de la editorial **www.colex.es**
- Identifíquese con su usuario y contraseña. En caso de no disponer de una cuenta regístrese.
- Acceda en el menú de usuario a la pestaña “Mis códigos” e introduzca el que aparece a continuación:

RASCAR PARA VISUALIZAR EL CÓDIGO

- Una vez se valide el código, aparecerá una ventana de confirmación y su eBook estará disponible en la pestaña “Mis libros” en el menú de usuario

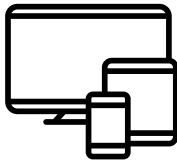
No se admitirá la devolución si el código promocional ha sido manipulado y/o utilizado.



¡Gracias por confiar en Colex!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook



Acceso desde cualquier dispositivo



Idéntica visualización a la edición de papel



Navegación intuitiva



Tamaño del texto adaptable

Puede descargar la APP “Editorial Colex” para acceder a sus libros y a todos los códigos básicos actualizados.



Síguenos en:



EL IMPACTO DE INTERNET DE LAS COSAS EN LA CIUDADANÍA EUROPEA

EL IMPACTO DE INTERNET DE LAS COSAS EN LA CIUDADANÍA EUROPEA

Coordinador:

Rafael Rodríguez Prieto

*Catedrático de Filosofía del Derecho de la
Universidad Pablo de Olavide de Sevilla*



Este libro ha sido financiado por el Fondo Europeo de Desarrollo Regional (FEDER) y por la Consejería de Economía, Conocimiento, Empresas y Universidad, de la Junta de Andalucía, en marco del programa operativo FEDER Andalucía 2014-2020. Objetivo específico 1.2.3. «Fomento y generación de conocimiento frontera y de conocimiento orientado a los retos de la sociedad, desarrollo de tecnologías emergentes» en marco del Proyecto UPO-1380664: Impacto del internet de las cosas sobre la ciudadanía europea (IDICCE). Porcentaje de cofinanciación FEDER 80%.



COLEX 2023

Copyright © 2023

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. del Código Penal). El Centro Español de Derechos Reprográficos (www.cedro.org) garantiza el respeto de los citados derechos.

Editorial Colex S.L. vela por la exactitud de los textos legales publicados. No obstante, advierte que la única normativa oficial se encuentra publicada en el BOE o Boletín Oficial correspondiente, siendo esta la única legalmente válida, y declinando cualquier responsabilidad por daños que puedan causarse debido a inexactitudes e incorrecciones en los mismos.

Editorial Colex S.L. habilitará a través de la web www.colex.es un servicio online para acceder a las eventuales correcciones de erratas de cualquier libro perteneciente a nuestra editorial, así como a las actualizaciones de los textos legislativos mientras que la edición adquirida esté a la venta y no exista una posterior.

© Rafael Rodríguez Prieto, © Fernando Martínez Cabezudo, © Adriana Fillol Mazo, © Miguel Ángel Martín López, © Borja Montes Toscano, © Pablo Antonio Fernández Sánchez, © Alejandro Manzorro Reyes, © Ana Cristina Gallego Hernández, © Luis Miguel Arroyo Yanes, © Christian Domínguez Expósito, © Noelia Arjona Hernández, © Virginia Gutiérrez Barbarrusa, © Manuel Jesús López Baroni

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, C.P. 15004
info@colex.es
www.colex.es

I.S.B.N.: 978-84-1194-132-7
Depósito legal: C 1910-2023

SUMARIO

INTRODUCCIÓN:

LAS BASES DE LA CIUDADANÍA EUROPEA Y EL DESAFÍO DEL IoT

Rafael Rodríguez Prieto y Fernando Martínez Cabezado

SECCIÓN PRIMERA:

Estado, ciudadanía e Internet de las cosas. Europa ante el desafío tecnológico

INTERNET DE LAS COSAS Y CIUDADANÍA EUROPEA: ¿COMPLEMENTO O CONFLICTO?

Rafael Rodríguez Prieto

1. INTRODUCCIÓN	27
2. IoT Y CIUDADANÍA	32
3. ¿DERECHOS DIGITALES O DERECHOS FUNDAMENTALES EN EL ECOSISTEMA CIBERNÉTICO?	37
4. CIUDADANÍA Y SU SIGNIFICACIÓN EN LA ERA DE IoT	43
5. CONCLUSIONES: ALGUNAS PROPUESTAS DE CIUDADANÍA FUERTE.....	56

EL USO DEL *BIG DATA* PARA LOGRAR SEGURIDAD ALIMENTARIA Y PREVENIR CRISIS ALIMENTARIAS

Adriana Fillol Mazo y Miguel Ángel Martín López

1. INTRODUCCIÓN: LA RELACIÓN ENTRE EL USO DEL <i>BIG DATA</i> Y LA SEGURIDAD ALIMENTARIA	59
2. INICIATIVAS RELATIVAS AL USO DE MACRO DATOS EN LA SEGURIDAD ALIMENTARIA	63
3. POSIBLES ÁMBITOS DE APLICACIÓN PARA MEJORAR LA INFORMACIÓN A TRAVÉS DEL INTERNET DE LAS COSAS Y EL USO DEL <i>BIG DATA</i>	68
3.1. Los alimentos kilométricos o food miles	68

SUMARIO

3.2. El establecimiento de reservas alimentarias para las situaciones de crisis: exigencia del derecho a la alimentación y la seguridad alimentaria y aportes desde el internet de las cosas y el <i>big data</i>	71
3.3. La malnutrición: su necesaria limitación por el derecho a la alimentación y su control con el apoyo de los <i>big data</i> y el internet de las cosas	74
4. LIMITACIONES Y ELEMENTOS CRÍTICOS EN LA UTILIZACIÓN DEL <i>BIG DATA</i> EN LA SEGURIDAD ALIMENTARIA	76
4.1. Recomendaciones sobre la gobernanza y gestión de los datos obtenidos para aplicarlos efectivamente a la mejora de la seguridad alimentaria	79
5. CONCLUSIONES	80

INTERNET DE LAS COSAS Y CONFLICTOS ARMADOS: DESAFÍOS Y DILEMAS EN LA DETERMINACIÓN DE LA RESPONSABILIDAD INTERNACIONAL

Borja Montes Toscano

1. INTRODUCCIÓN	83
2. INTERNET DE LAS COSAS MILITARES	84
2.1. Áreas de implementación: ¿Hacia una mayor dependencia?	84
2.2. ¿Nuevo escenario de combate?	86
3. RIESGOS QUE CONLLEVA LA AUTONOMÍA Y EL INTERNET DE LAS COSAS	88
3.1. Amenazas actuales	88
3.2. Posibles líneas de acción: ¿Seguir confiando el control a los humanos?	90
4. COMO CALIFICAR A LOS COMPORTAMIENTOS ALGORÍTMICOS	92
4.1. Perspectivas y clases	92
4.2. ¿Ataques armados?	94
4.3. Aclaración sobre las nociones de «Producto» o «Servicio»	95
5. LA DIFICULTAD DE ATRIBUCIÓN / IMPUTACIÓN DE LOS HECHOS	97
5.1. Aproximación hacia la responsabilidad penal individual	97
5.2. Atribución de los hechos a los Estados: Revisión del armamento y capacidades	98
6. CONCLUSIONES	100

SECCIÓN SEGUNDA:

Derechos humanos frente al desarrollo de IoT

EL DERECHO A LA HERENCIA DIGITAL EN EL ÁMBITO EUROLATINOAMERICANO

Pablo Antonio Fernández Sánchez

1. INTRODUCCIÓN	105
2. LA SITUACIÓN ACTUAL DE LA HERENCIA DIGITAL EN EL ENTORNO EUROLATINOAMERICANO	106

SUMARIO

3. EL PATRIMONIO DIGITAL	111
4. LA NORMATIVA EMPRESARIAL, ¿LEX SPECIALIS?	115
5. LOS DERECHOS CIVILES DIGITALES VERSUS DERECHOS PATRIMONIALES..	118
6. LA DIGNIDAD COMO PRINCIPIO INSPIRADOR DEL EJERCICIO DE LOS DERECHOS DIGITALES.	122
7. CONCLUSIONES..	128

ALEXA, LOS DISPOSITIVOS ECHO Y LA PRIVACIDAD. A VUELTAS CON LA LOPDGDD

Alejandro Manzorro Reyes

1. BREVE REFERENCIA INTRODUCTORIA AL INTERNET DE LAS COSAS	131
2. LA INTERCONEXIÓN ENTRE EL DERECHO AL HONOR Y EL INTERNET DE LAS COSAS.	133
3. ALEXA, LOS DISPOSITIVOS ECHO Y LA PRIVACIDAD	135
4. CONTROL DE OFICIO POR LOS JUZGADOS Y TRIBUNALES	137

SALUD DIGITAL Y DERECHOS HUMANOS

Ana Cristina Gallego Hernández

1. INTRODUCCIÓN	143
2. ¿QUÉ ES LA SALUD DIGITAL?	145
3. CÓMO INCIDE LA SALUD DIGITAL EN LA GARANTÍA DEL DERECHO A LA SALUD.	148
4. DERECHOS QUE SE VEN LIMITADOS POR EL USO DESPROPORCIONAL DE LA SALUD DIGITAL.	151
5. LA SALUD DIGITAL COMO HERRAMIENTA ANTE EMERGENCIAS SANITARIAS	152
6. CONCLUSIONES	154

SECCIÓN TERCERA:

El cuerpo físico del IoT: desentrañando la complejidad de la
infraestructura de la Red

LA IMPLANTACIÓN DE LA NUEVA TECNOLOGÍA DE TELEFONÍA 5G Y SUS IMPLICACIONES JURÍDICO-ADMINISTRATIVAS

Luis Miguel Arroyo Yanas

1. INTRODUCCIÓN	159
2. LA IMPLANTACIÓN DE LA TECNOLOGÍA DE TELEFONÍA 5G Y EL FORTALECIMIENTO DE LAS COMPETENCIAS ESTATALES EN MATERIA DE TELECOMUNICACIONES	161

SUMARIO

3. LOS NUEVOS ELEMENTOS QUE SIRVEN PARA SUSTENTAR LA POTENCIACIÓN DE LAS COMPETENCIAS ESTATALES FRENTE A LAS COMPETENCIAS AUTONÓMICAS Y LOCALES.....	164
3.1. Las redes públicas de muy alta capacidad	164
3.2. Las redes y estaciones como infraestructuras.....	166
3.3. La implantación de redes y estaciones como obras públicas de interés general	167
4. LA LGT Y SU LECTURA DE LOS TÍTULOS COMPETENCIALES AFECTADOS POR SUS PREVISIONES	168
4.1. Breve extracto de la jurisprudencia constitucional sobre las leyes previas de telecomunicaciones	168
4.2. La protección de la salud de las personas	171
4.3. La protección ambiental y los controles administrativos	176
4.4. La ordenación urbana y territorial	179
4.5. La protección del patrimonio histórico	182
4.6. La seguridad pública, de las personas y de las cosas.	183
5. EXCURSO SOBRE LOS DERECHOS FUNDAMENTALES, LAS LIBERTADES PÚBLICAS Y LOS DERECHOS ORDINARIOS DE LOS CIUDADANOS.....	185
6. REFLEXIÓN FINAL	187

CONECTANDO EL IOT CON EL MUNDO: UN ANÁLISIS DEL RÉGIMEN JURÍDICO INTERNACIONAL DE LAS COMUNICACIONES POR SATÉLITE

Christian Domínguez Expósito

1. INTRODUCCIÓN: EL INTERNET DE LAS COSAS Y LAS COMUNICACIONES POR SATÉLITE.....	191
2. DERECHO INTERNACIONAL ESPACIAL Y LAS COMUNICACIONES POR SATÉLITE.....	194
2.1. Tratado del Espacio	195
2.2. Convenio de Responsabilidad	201
2.3. Convenio de Registro.....	206
3. RÉGIMEN JURÍDICO DESARROLLADO EN EL SENO DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES Y LAS COMUNICACIONES POR SATÉLITE.....	207
3.1. La gestión de las frecuencias del espectro radioeléctrico por la UIT	210
3.2. La gestión de las comunicaciones por satélite por la UIT	213
4. CONCLUSIONES.....	217

LOS CABLES SUBMARINOS SMART PARA LA OBSERVACIÓN DEL OCÉANO Y DE LA TIERRA

Noelia Arjona Hernández

1. INTRODUCCIÓN	221
-----------------------	-----

SUMARIO

2. EL CONCEPTO DE CABLES SUBMARINOS VERDES O CABLES <i>SMART</i>	229
3. EL DERECHO DEL MAR EN MATERIA DE CABLES SUBMARINOS.	232
3.1. Cables submarinos y CNUDM	233
3.2. Investigación científica marina	235
3.2.1. Obligaciones de publicación de la investigación científica marina .	238
3.3. Meteorología marina y oceanografía operativa	239
4. RÉGIMEN JURÍDICO APLICABLE A LOS CABLES <i>SMART</i>	241
4.1. Cables en zonas situadas fuera de la jurisdicción nacional.	243
5. CONCLUSIONES	244

SECCIÓN CUARTA:

IoT: ¿nuevas realidades, viejos desafíos?

IOT Y DEMOCRACIA: ¿PARA QUÉ, PARA QUIÉN?

Virginia Gutiérrez Barbarrusa

1. ¿UNA NUEVA REALIDAD VIRTUAL? EL IoT AFLORA EN EL MUNDO REAL? . .	249
2. EL INTERNET DE LAS COSAS (IoT) Y LAS <i>SMARTCITIES</i>	250
3. LA BRECHA DIGITAL Y DESIGUALDAD SOCIAL	253
4. LOS ODS Y EL DESARROLLO DIGITAL: PROPUESTAS PARA PARA REDUCIR LA BRECHA DIGITAL	258
5. MECANISMOS DIGITALES PARA EL DESARROLLO DE LAS POLÍTICAS DE PARTICIPACIÓN	266
6. EL IoT: ¿PARA QUÉ? ¿PARA QUIÉN?	269

BIOÉTICA E INTERNET DE LAS COSAS

Manuel Jesús López Baroni

1. INTRODUCCIÓN	271
2. PROBLEMAS CONCEPTUALES	272
3. EL IMPACTO DEL INTERNET DE LAS COSAS EN LA BIOMEDICINA	275
3.1. Enfermedades que carecen de cura conocida	276
3.2. Estudios estigmatizantes.	281
4. EL IMPACTO DEL INTERNET DE LAS COSAS EN LAS NEUROTECNOLOGÍAS. .	284
5. CONCLUSIONES	294

INTELIGENCIA ARTIFICIAL Y PLUSVALÍA EN RED: UNA MIRADA SOBRE LA EXTRACCIÓN DEL BENEFICIO Y LAS NUEVAS REALIDADES TECNOLÓGICAS

Fernando Martínez Cabezudo

1. INTRODUCCIÓN	295
2. INTELIGENCIAS ARTIFICIALES: DEFINICIÓN, CONCEPTOS SIMILARES Y FUNCIONAMIENTO	297
2.1. Figuras Colindantes	299
2.2. Funcionamiento básico de las Inteligencias Artificiales basadas en Redes Neuronales	301
3. DERECHOS DE AUTOR Y LICENCIAS <i>COPYLEFT</i> . COLISIONES DE DERECHOS: CUESTIONES RELATIVAS AL EJERCICIO DE LAS FACULTADES ECONÓMICAS Y MORALES	303
3.1. Breve referencia al Sistema de Derechos de Autor	304
3.2. Licencias Libres	306
4. PLUSVALÍA EN RED. UNA APROXIMACIÓN A LAS NUEVAS FORMAS DE EXPLOTACIÓN EN LA ESFERA VIRTUAL	307
5. LAS INTELIGENCIAS ARTIFICIALES, EXTERNALIDADES Y GENERACIÓN DE BENEFICIO	310
5.1. Inteligencias Artificiales y Derechos de Autor	311
5.2. Inteligencias Artificiales y Licencias Libres	315
6. INTELIGENCIAS ARTIFICIALES Y LA EXPLOTACIÓN DE LAS ENERGÍAS SOCIALES	317
AUTORES	321

INTRODUCCIÓN

LAS BASES DE LA CIUDADANÍA EUROPEA Y EL DESAFÍO DEL IoT

Rafael Rodríguez Prieto y Fernando Martínez Cabezudo

Es sábado. La jornada de reflexión en cualquier elección que se celebra en España. Alrededor de las 7 de la mañana se ha comenzado a compartir un vídeo en el que se ve al candidato favorito recibir un maletín con mucho dinero en un ambiente bastante turbio. Incluso se le llega a escuchar. Dice algo muy comprometido. Probablemente delictivo. A las 12 de la mañana el vídeo se ha convertido en el más visto del año. Por la tarde, hay protestas en las calles frente a la sede de su partido. El resultado del domingo no fue el que preveían las encuestas. Ha cambiado. El martes por la mañana varios expertos en Inteligencia Artificial (IA) afirman, sin ninguna duda, que el vídeo es falso. Que la voz y la cara del candidato han sido generadas por un software de última generación, alimentado por miles de millones de datos. Lo peor de esta fabulación es que no existe ninguna razón para pensar que no pueda suceder. La ingente cantidad de datos que, gracias al internet de las cosas (IoT), hace posible la IA más potente de la historia, puede ayudar al ser humano a mejorar su vida. Sin embargo, dicha herramienta tecnológica también podría ser capaz de hundir nuestras democracias y rebajar la ciudadanía a un mero estatus de consumidor. O incluso menos: de usuario.

La ciudadanía europea se definió por primera vez en los artículos 9 a 12 del Tratado Fundacional de la Unión Europea (TFUE). Los artículos 18 a 25 del TFUE establecen los derechos derivados de la misma¹. Entre los principales derechos se encontrarían el derecho a circulación y residencia, el derecho a ser elector y elegible en las elecciones municipales y al Parlamento Europeo en el país de residencia, la protección diplomática y consular fuera de la UE, el derecho de petición al Parlamento Europeo o el recurso al Defensor del Pueblo Europeo, derechos lingüísticos, no ser discriminado en razón de la

1 <https://eur-lex.europa.eu/ES/legal-content/glossary/eu-citizenship.html>

nacionalidad, poder usar la iniciativa ciudadana y acceder a documentación de la UE. No obstante, el elemento que nos interesa resaltar es que esta ciudadanía es un complemento de la que las personas tienen por ser parte de un Estado miembro. Como sintetiza CRUZ LUNA, no define una relación jurídico-política pura, sino una relación que vincula a un sujeto físico desde su nacionalidad originaria; lo que es relevante es el tradicional lazo entre el individuo y el Estado, al que se une el de la UE². Los derechos y deberes de uno y otro vínculo se suman. Esta complementariedad otorga a la ciudadanía de la UE un valor que traspasa la mera condición de ser producto de un tratado entre Estados. Esta ciudadanía se inserta en la tradición de los valores democráticos, ligados a la idea de Estado social y democrático de derecho.

Con el desarrollo de IoT, el procesamiento de datos amplía tanto su complejidad como sus posibilidades de uso, entre los que destaca la IA. Al mismo tiempo, se identifican una serie de efectos colaterales de esta tecnología que impactan en el corazón de nuestros Estados representativos: los derechos fundamentales. Los datos, y la forma en que son procesados, los riesgos para la ciudadanía de que sus vidas diarias sean vigiladas o intervenidas, junto con la manera en que IoT impacta en la formación y educación cívica —verdaderos motores de una ciudadanía democrática—, son cuestiones que deben ser cuidadosamente analizadas.

El desarrollo de IoT genera grandes beneficios para las sociedades en diversos campos como puede ser el sector industrial o el médico, sin olvidar las posibilidades ligadas a la mejora de la prevención de riesgos y amenazas potenciales para las personas e infraestructuras. No obstante, tampoco se puede caer en su mitificación, ya que también se perciben conflictos en relación con los derechos fundamentales y, en definitiva, la buena salud de los Estados de derecho. La infraestructura o cuerpo físico que hace posible el IoT es un pilar decisivo del impacto de esta tecnología en la ciudadanía y debe estar sometida a un escrutinio crítico.

El papel de la regulación es esencial en esta profunda transformación tecnológica en la que nos encontramos. Por un lado, se debe garantizar que los Gobiernos no van a utilizar esta tecnología con el fin de establecer férreos controles sobre los ciudadanos, como ya acontece en dictaduras como China. Por otro, la existencia de entes privados, formales o informales, con un gran poder e influencia, gracias a esta tecnología, debe ser un aspecto a vigilar y controlar por las instituciones democráticas. Casos como los de *Cambridge*

2 CRUZ LUNA, A., «Ciudadanía de la Unión y nacionalidad. La incidencia del derecho de la Unión en las competencias sobre la nacionalidad de los estados miembros», *Revista de Estudios Europeos*, 71, 2018, 171-188. Para esta autora la jurisprudencia del Tribunal de Justicia de la UE ha ampliado el número de beneficiarios del estatuto de ciudadano de la UE. Los derechos que integran este estatuto se reconocerían a ciudadanos de terceros países, familiares de ciudadanos europeos que no posean la condición de ciudadano europeo o residentes, tanto personas físicas o jurídicas.

Analytica, la transferencia de datos de jóvenes europeos a China con TikTok, las reiteradas multas a Google por la Comisión Europea por abuso de posición dominante o las prácticas laborales de empresas como *Amazon*, *Uber* o *Deliveroo* son solo algunos ejemplos de la necesidad de estar vigilantes.

El IoT supone un verdadero desafío a los derechos fundamentales. Cuestiones como la separación de las esferas públicas y privada, derecho de libertad de conciencia, el derecho a la libertad de expresión o la privacidad e intimidad de las personas son directamente afectadas por una tecnología con consecuencias en relación al paradigma jurídico clásico. El IoT, como el entramado de los chips, sensores y aparatos electrónicos que permiten la interconexión entre diferentes dispositivos de uso diario, junto con la información generada, supone un salto cualitativo y cuantitativo respecto al internet tradicional. La UE ha realizado un notable esfuerzo legislativo, que ha situado a su territorio como el área del mundo con una legislación más garantista y avanzada democráticamente, en lo referido a la protección de derechos en el ecosistema cibernético.

La necesidad de una protección eficaz de bienes jurídicos esenciales para el mantenimiento y fortalecimiento del Estado de derecho en el ámbito de internet no resulta tarea fácil en el marco de una tecnología con un alcance decisivamente global. Su desarrollo podría generar serias intromisiones en el ejercicio de la ciudadanía, según la manera en que se apliquen las tecnologías del *big data* en la nueva capa de internet, cuya dinámica la capacita para obtener datos de aparatos que se comunican entre sí. Estas son serias amenazas para la separación pública-privada que supuso el establecimiento de la concepción de ciudadanía occidental. No existe actualmente un marco jurídico que permita dar una respuesta adecuada a la consolidación del IoT. La identificación y análisis de las relaciones de poder y dominio es también un elemento clave, a nivel metodológico, presente en esta investigación³.

3 RODRÍGUEZ PRIETO, R. Y MARTÍNEZ CABEZUDO, F., *Poder e internet. Un análisis crítico de la Red*. Cátedra, Madrid, 2016. En este libro identificamos dos polos: Dictanet y Free(share)net. Estas categorías son ideales, es decir, no tienen representación real en su totalidad, nos sirven como haces donde agrupamos tendencias que son observables respecto de cómo se configura el equilibrio fuerzas en la Red. Primero, en el conjunto que hemos dado en llamar Dictanet se agruparían las tendencias hacia la concentración del poder, la jerarquización y control central, así como la extrema mercantilización de los contenidos y los datos producidos por usuarios. El segundo de los haces sería Free(share)net, como reflejo invertido del anterior. Son las tendencias hacia la apertura, las estructuras más horizontales con procesos democráticos de apropiación de la Red y la tendencia hacia al mayor beneficio social del procomún. Esta metodología es útil para el análisis de procesos complejos como los que tienen lugar en internet. En una misma acción podemos analizar cómo convergen tendencias de estos dos haces. No se trata de una forma maniquea de estudiar los procesos. Se examinan los espacios comunes donde podemos ubicar las acciones que se observan en una misma trama de sentido, de tal manera que cuando analizamos el comportamiento de determinados actores podemos ver como conviven elementos que podrían ser agrupados en un conjunto o en otro. Es especialmente útil para el análisis de los conflictos entre los proveedores de contenido y las empresas de acceso a la

Este libro analiza el uso que de estos nuevos dispositivos pudieran hacer entes privados y públicos, además de actores difusos o colectivos criminales que supongan un riesgo y amenaza contra el espacio de seguridad libertad y justicia. Al mismo tiempo, con el fin de realizar un estudio integral de la problemática, se estudiará la forma en que inciden en las definiciones de los pilares del ordenamiento jurídico, así como cuestiones que afectan a su infraestructura. Una nueva tecnología de extracción y producción masiva de datos requiere un esfuerzo regulatorio que preserve el ideal democrático. De su análisis se inferirán una serie de consecuencias cuyo fin es la mejora de la regulación autonómica, nacional y europea.

En síntesis, la conexión entre la capacidad de recabar datos, trazar perfiles, realizar predicciones, junto con su desarrollo exponencial gracias al IoT, son cuestiones que, junto a una legislación deficiente, pueden suponer un grave riesgo para los derechos fundamentales y para la propia configuración y desarrollo de la ciudadanía en la UE. Las razones que justifican este libro son ofrecer propuestas regulatorias y diseño de políticas públicas efectivas para garantizar el desarrollo y salvaguarda de la democracia y los derechos humanos, una vez que se han identificado y analizado los retos que se derivan del IoT.

Esta investigación ha generado una serie de iniciativas concretas para mejorar la ciudadanía en el espacio cibernético que serán presentadas en la Comisión de Peticiones del Parlamento Europeo. Las principales propuestas están relacionadas con creación de repositorios de software sujetos a auditoría ciudadana, el fortalecimiento del respeto a la intimidad y privacidad de los ciudadanos de la UE y el desarrollo de una infraestructura más participada por la sociedad civil europea.

* * * * *

Este libro es resultado de una investigación que ha sido financiada por el Fondo Europeo de Desarrollo Regional (FEDER) y por la Consejería de Economía, Conocimiento, Empresas y Universidad, de la Junta de Andalucía, en marco del programa operativo FEDER Andalucía 2014-2020. Objetivo específico 1.2.3. «Fomento y generación de conocimiento frontera y de conocimiento orientado a los retos de la sociedad, desarrollo de tecnologías emergentes») en marco del proyecto de investigación de referencia UPO-1380664. Porcentaje de cofinanciación FEDER 80 %.

Se trata de una obra interdisciplinar. Dentro del ámbito jurídico, destacan las aportaciones desde el derecho internacional, la filosofía del derecho o el derecho administrativo. No obstante, también se realizan aportaciones desde

Red. Afrontar escenarios con tanta complejidad como el impacto social de las tecnologías de la comunicación, precisa de herramientas de análisis que no recurran a simplificaciones o falseen las conclusiones, ni a un exceso de inputs que conlleve una parálisis total. Esta metodología hace posible realizar un estudio de internet insertado en una tradición donde los procesos materiales y el análisis de la construcción de sentido son esenciales.

la política, la bioética o la sociología. El trabajo se divide en cuatro secciones. La primera se titula *Estado, ciudadanía e Internet de las cosas. Europa ante el desafío tecnológico*. En esta parte de la investigación se estudia el IoT como una ampliación sin precedentes en la capacidad de recogida, procesamiento de datos. Las posibilidades que abren estas nuevas capacidades para el Estado y la ciudadanía son cuantiosas. Desde una mayor eficiencia de los servicios públicos hasta la mejora en la trazabilidad y, por tanto, mayor seguridad, de los alimentos que consumimos. Sin embargo, existen una serie de interrogantes en relación a la dimensión política de las implicaciones de esta extensión. Estas nuevas capacidades no son inocuas. La recolección y procesamiento de datos por parte de agentes centrales que concentren gran parte de este poder puede afectar al propio ejercicio de derechos por la ciudadanía. La naturaleza jurídico-política de estos cambios y las nuevas posibilidades constituyen puntos de reflexión interesante que deben analizarse con el fin de obtener una mejor capacidad de predicción sobre el impacto que puede tener el IoT sobre los derechos que marcan la vida social y política de los ciudadanos de la Unión. En el primer capítulo se analiza la insuficiencia de la legislación europea sobre la tecnología que hace posible el IoT y la IA, aunque se trate de la más avanzada y garantista del mundo. Las razones de sus carencias están ligadas a su enfoque. Al analizar los motivos que se establecen en las principales normas de la UE para el ecosistema cibernético, se percibe que los derechos fundamentales son situados en un plano secundario y se privilegia un enfoque neoliberal. Esta lectura crítica de las proposiciones, donde se destaca una fuerte presencia de criterios economicistas en el enfoque general de las principales regulaciones del ciberespacio, puede derivar en un desequilibrio entre la explotación de estos nuevos servicios y un ejercicio más garantista de los derechos cívico-políticos. Sin embargo, la investigación no se queda en una mera crítica, ya que se realizan proposiciones que reorienten esta perspectiva para darle el papel preeminente a un mayor disfrute de las libertades civiles. Como vía de solución, se plantea la necesidad de que los derechos fundamentales, junto con los principios generales del derecho, sean la base desde donde se legisle. Finalmente, se presentan una serie de iniciativas concretas cuyo fin es el fortalecimiento de la ciudadanía en Europa. Los profesores Adriana Fillol Mazo y Miguel Ángel Martín López examinan las implicaciones y limitaciones del uso de los macrodatos a la hora de contribuir a la seguridad alimentaria mundial. Para ello se destacan algunas iniciativas relativas a cómo se está utilizando actualmente el *Big data* para informar las iniciativas humanitarias de seguridad alimentaria, así como algunos ámbitos prioritarios relacionados con aspectos de la misma seguridad alimentaria, en los que podría tener aplicación futura el internet de las cosas y el *Big data*. En este sentido, los autores plantean nuevos ámbitos de aplicación para mejorar la información a través del IoT y el *Big data*: la reducción de los alimentos kilométricos, el establecimiento de reservas alimentarias para situaciones de crisis y el control de la malnutrición. Sin embargo, a pesar de los avances, también se plantean limitaciones

y elementos críticos en el uso del *Big data* en seguridad alimentaria. Por ello, se plantean recomendaciones relativas a la gobernanza adecuada y gestión efectiva de los datos para garantizar la protección de la privacidad y el consentimiento informado de las comunidades. Además, se enfatiza la importancia de una evaluación exhaustiva de toda la cadena alimentaria digital, considerando la diversidad de los sistemas alimentarios y evitando sesgos en la recopilación y uso de datos. Finalmente, para el investigador Borja Montes Toscano, las nuevas tecnologías están más presentes que nunca en los conflictos armados actuales, en especial el IoT y, de forma progresiva, la IA. Así, se está permitiendo a las fuerzas armadas reforzar sus ventajas estratégicas, facilitándose el ciclo de toma de decisiones en sus operaciones y ejercicios. Sin embargo, determinados riesgos pueden afectar a la seguridad de estas aplicaciones (e.g. Ataques de «spoofing» o «Input attacks»), quedando sus capacidades deshabilitadas para cumplir la misión encomendada. Estas vulnerabilidades han de ser observadas con cautela por los órganos estatales, en un mundo en el que están proliferando los conflictos híbridos, así como la búsqueda de lagunas jurídicas en diferentes sistemas normativos. Este capítulo analiza los comportamientos algorítmicos reproducidos por estas tecnologías, así como el grado de involucración humana necesario para que valores fundamentales, como la vida humana, no sean puestos en cuestión. Del mismo modo, se estudia el papel de las partes implicadas tanto en el proceso de fabricación como de desarrollo y despliegue de estos dispositivos. Esta cuestión se abordará teniendo presente el Derecho Penal, así como recientes propuestas de la Comisión Europea para la regulación de la Inteligencia Artificial. Igualmente se analizará la responsabilidad estatal desde la perspectiva de la diligencia necesaria y la provisión de reparaciones.

En la segunda sección denominada *Derechos humanos frente al desarrollo de IoT* se analiza el impacto de esta tecnología en derechos fundamentales concretos. Los trabajos agrupados en esta sección investigan las consecuencias de la interacción entre empresas, el ejercicio del poder del Estado para establecer los marcos regulatorios y el propio ejercicio de los derechos civiles y libertades públicas. El IoT es un importante reto jurídico tanto para los ordenamientos jurídicos nacionales como para el derecho internacional. La fluidez de las relaciones entre sujetos de diferentes nacionalidades, que conlleva la extensión del IoT, implica un nuevo desafío que debe ser problematizado respecto al ejercicio de los derechos humanos.

En esta parte presentamos tres trabajos que se refieren a elementos concretos del ordenamiento jurídico en relación a derechos fundamentales. Por su extrema relevancia en la configuración socioeconómica de los estados miembros de la UE, el derecho a la herencia supone un punto fundamental en la dinámica social. El profesor Pablo Antonio Fernández Sánchez toma este elemento como punto central de su investigación estudiando las diferentes soluciones a las que han llegado los Estados para acomodar el nacimiento e incremento de valor de estos nuevos bienes digitales producto del

IoT y el ejercicio de un derecho fundamental como la herencia, que cuenta con una compleja y profunda reglamentación. El segundo de los capítulos de esta sección es redactado por el magistrado juez Alejandro Manzorro Reyes, que considera que la interconexión entre el derecho al honor y el IoT plantea importantes desafíos legales y éticos. En su capítulo analiza cómo la recopilación, el procesamiento y el uso de datos personales generados por dispositivos IoT pueden afectar la reputación y el honor de las personas si no se manejan adecuadamente. Con este fin, estudia el dispositivo Alexa y estima que es esencial que se articulen mecanismos y medidas sólidas de protección de la privacidad, seguridad y transparencia para garantizar que los individuos mantengan el control y la dignidad en un entorno digital cada vez más interconectado. En definitiva, se discuten los límites, las protecciones y los deberes de transparencia que deberíamos tener en cuenta, con el fin de garantizar bienes jurídicos básicos de nuestro ordenamiento. En el capítulo final de la sección, a cargo de la profesora Ana Cristina Gallego Hernández, se estudia la salud digital o como generalmente se está denominando eHealth. Esta constituye la base para el desarrollo de la tecnología emergente en salud y, al mismo tiempo, el *Internet de la Salud*, como medio para el desarrollo de toda esta revolución tecnológica. Se trata de un desafío fundamental para la gobernanza. Así las cosas, es preciso tener presente que el uso del *big data* en el cuidado de la salud permite reunir una cantidad extraordinaria de información biológica, clínica, ambiental y sobre el estilo de vida de los individuos, la cual se recopila de los registros médicos electrónicos, redes sociales, datos genómicos, referencias farmacéuticas, ensayos clínicos, aplicaciones de móviles, telemedicina, indicadores socioeconómicos o hábitos. Su principal consecuencia de utilizar el *big data* o la IA en la medicina es promover el bienestar y la seguridad de las personas. En síntesis, las tecnologías digitales emergentes están incrementando el grado de garantía del derecho a la salud en la UE. La incorporación de nuevos dispositivos capaces de generar un caudal de datos que son útiles en el campo médico puede ser una de las ayudas más importantes que puede tener el Estado para gestionar los recursos sanitarios con la finalidad de optimizar recursos y alcanzar una mayor protección en sus derechos para los ciudadanos de la UE.

En la tercera sección titulada *El cuerpo físico del IoT: desentrañando la complejidad de la infraestructura de la Red* nos centramos en la infraestructura material que hace posible IoT. Habitualmente, cuando se analizan las cuestiones relacionadas con la tecnología, la política y el derecho, el objetivo es estudiar desafíos que se concretan en conflictos entre aplicaciones, usos o conductas dentro de la Red. Sin embargo, este hecho conlleva cierto alejamiento de la materialidad de la misma. A nuestro juicio, es necesario mantener en la cabeza esta infraestructura como un elemento central de la crítica. De no realizar este esfuerzo, corremos el riesgo de tratar lo que sucede en el mundo digital como perteneciente a una especie de realidad evanescente que circula por/entre la sociedad como una especie de fantasma incorpóreo.

Sin embargo, Internet supone la acción de una miríada de dispositivos trabajando de manera coordinada, discos duros en servidores, cables que llevan información entre continentes, puntos de intercambio neutros, centros de datos u ordenadores domésticos. Todos ellos constituyen el cuerpo físico de la Red y no los podemos entender sin tener en cuenta que la localización y el régimen jurídico de estos la marcan de manera determinante. El IoT supone una ampliación de la capacidad de recogida y tratamiento de los datos, gracias a que los límites de este cuerpo físico se ven ensanchados por la incorporación de nuevos dispositivos a esta maya que la dotan de nuevos sentidos. Así, esta infraestructura de base se convierte en algo aún más importante, pues es lo que permite que esa nueva capa funcione de manera integrada y coordinada. Internet es una superestructura tecnológica que integra diferentes subestructuras para conformar una red de redes, este sentido hay que tener en cuenta que no nos referimos a algo unitario, sino de una integración de partes.

En esta sección trataremos tres importantes aspectos de esta cuestión donde se analizarán los retos más relevantes ligados a dicho *cuerpo físico*. En primer lugar, una de las consecuencias más importantes de la incorporación de esos nuevos dispositivos del IoT es la necesidad de que los canales de comunicación entre los mismos sean rápidos y fluidos. Esta exigencia trae aparejada la implantación de la tecnología 5G como medio de garantizar una conexión constante y de alta calidad, por lo que la infraestructura técnica que habilita esta tecnología se vuelve de vital importancia. El profesor Luis Miguel Arroyo Yanes analiza la producción legislativa a este respecto con una mirada que nos propone una aproximación crítica a legislación que muestra nacientes conflictos de intereses entre las operadoras, el ejercicio de derechos cívicos y el principio de precaución. En segundo lugar, si las conexiones inalámbricas que implica el nuevo 5G son importantes, los cables submarinos que entretrejen la red a nivel intercontinental no lo son menos. En su aportación, la profesora Noelia Arjona Hernández se remonta al siglo XIX para el análisis de los cables submarinos contemporáneos. Esta tecnología data del 29 de julio de 1858 cuando se completó el primer cable transatlántico del mundo que se extendía desde Irlanda hasta Terranova. La reina Victoria y el presidente James Buchanan intercambiaron telegramas el 16 de agosto de 1858 y sus mensajes combinados, de menos de 100 palabras, tardaron 17 horas y 40 minutos en transmitirse, lo que representó el mensaje más rápido jamás enviado entre Washington y Londres. Fue tan revolucionario entonces como lo fue internet para nosotros, cuando se lanzó en la década de 1990. Si sustituimos, respectivamente, «cables de fibra óptica» y «correo electrónico» o «mensaje de texto» por «cables marítimos telegráficos» y «telegrama», queda patente que la naturaleza crítica del mantenimiento de los «cables marítimos» es tan pertinente como ya lo era en 1880. Además de ser utilizados para el transporte de datos regulares de telecomunicaciones (estos cables de propiedad privada transportan alre-

dedor del 99 % de las comunicaciones digitales transoceánicas), podrían desempeñar una función en la recogida y transporte de datos oceanográficos para detectar a tiempo un temblor marino que no solo serviría para evitar interrupciones en la comunicación, sino también para algo mucho más importante: impedir la catástrofe que deja un tsunami. Según un grupo de científicos integrantes de *Joint Task Force* (JTF), el método más rápido, sencillo y económico consiste en volver «inteligentes» los cables submarinos, esto es, sumar los cables de internet a la llamada Internet de las cosas, desarrollando el concepto de Cables SMART. En definitiva, se ofrece una visión general de los denominados Cables SMART, analizando el régimen jurídico que podría regirlos según la Convención de las Naciones Unidas sobre el Derecho del Mar. Finalmente, el investigador Christian Domínguez Expósito estima que IoT ha surgido como una tecnología innovadora que ha impactado en gran medida diversos aspectos de la vida humana. Al conectar objetos y personas a través de internet, se está logrando una interconexión sin precedentes en prácticamente todos los ámbitos. Sin embargo, la interconexión de objetos inteligentes plantea desafíos particulares en áreas remotas o de difícil acceso para las redes terrestres convencionales. Es en este contexto, las comunicaciones por satélite han demostrado ser fundamentales. Al ofrecer conectividad global, las comunicaciones por satélite permiten superar las limitaciones geográficas y establecer una comunicación segura y simultánea entre lugares distantes. Esta capacidad resulta especialmente relevante en escenarios donde las infraestructuras terrestres tradicionales no son efectivas. No obstante, su marco jurídico, resulta complejo y abarca múltiples aspectos. A este respecto, este trabajo se centra en los dos regímenes jurídicos principales que regulan estas comunicaciones a nivel internacional. En concreto, el análisis se enfoca en los aspectos jurídico-internacionales de carácter convencional más importantes, con el objetivo de comprender los derechos y obligaciones de los diversos actores involucrados, ya sean Estados, organizaciones internacionales o empresas proveedoras de servicios.

En la última sección denominada *IoT: ¿nuevas realidades, viejos desafíos?* se analizan una serie de campos donde el IoT puede tener un efecto transformador extremo, pero donde las regulaciones, por su novedad y celeridad, no llegan a establecer marcos suficientemente garantistas. Esta circunstancia es especialmente importante dado que tanto la biotecnología como el desarrollo de las inteligencias artificiales o las *smart cities* están en el centro de las revoluciones tecnológicas que pueden alterar de manera significativa la vida social. La producción y procesamiento de datos que deriva del IoT es un factor que multiplica exponencialmente el impacto de los casos que se analizan en esta sección. Es imprescindible una profunda comprensión del calado de las transformaciones, e implicaciones para nuestro modelo político-social, que tienen tanto los avances en biología como la IA o la implementación de sensores que hacen posibles las ciudades inteligentes.

En primer lugar, la socióloga Virginia Gutiérrez Barbarrusa analiza, el concepto de *smart city*, o ciudad inteligente, para referirse básicamente a la utilización de un universo de dispositivos digitales diseñados para la mejora de la gestión pública municipal. Pero, ¿cómo se puede lograr que esa gestión sea lo más democrática posible involucrando a las y los ciudadanos? Cuando lo virtual se convierte en una parte de la realidad social, la participación ciudadana que se promueve en este escenario debe incluir algunos aspectos que requieren de una reflexión crítica, atendiendo entre otras cosas a la brecha digital, o a las políticas que se articulan a distintos niveles, sobre lo que se ha denominado la transformación digital. En este sentido, se presenta una revisión del concepto de IoT, haciendo mención a la aplicación de este a la gestión inteligente de las ciudades. También se extraen algunos datos que nos hacen reflexionar sobre las brechas sociales que se abren en este contexto y se revisan las políticas que inciden en lo que se ha denominado la transformación digital, tendentes, entre otras cosas a disminuir la citada brecha con un doble objetivo: extender las infraestructuras necesarias para que el acceso a internet sea universal y establecer mecanismos para capacitar a la gente para su uso. La necesidad de arbitrar mecanismos que propicien la capacidad de incidencia de las personas en este nuevo espacio conduce a la pregunta que guía este trabajo, IoT: ¿para qué, para quién? Desde una óptica sociológica, tanto la forma en que las Nuevas Tecnologías de la Comunicación y la Información —NTIC— son aplicadas a la gestión pública y desarrolladas por grandes corporaciones, como la propuesta de implementar medidas que hagan posibles las startup cities, incidiendo en la promoción de pymes, y otras organizaciones empresariales de carácter local. Este capítulo plantea la necesidad de reorientar el debate hacia propuestas que reivindiquen la soberanía digital, o del rescate los «data common», como «base para fomentar una economía más democrática». En su capítulo el iusfilósofo Manuel Jesús López Baroni, analiza la emergencia del IoT y su impacto en la UE. A su juicio, afectará a múltiples disciplinas, entre ellas, a la bioética. Sin embargo, las carencias para afrontar los retos que plantea dicha tecnología deberían ser tenidas en consideración, dado que el Convenio de Oviedo data de 1997, y el artículo 3 de la Carta de los Derechos Fundamentales de la UE se elaboró en 2000. Además, la normativa de la Unión Europea sobre protección de datos e Inteligencia Artificial no se ha elaborado desde la atalaya de los derechos humanos, sino con objeto de armonizar el mercado interior, esto es, con una perspectiva eminentemente económica. Obviamente, estamos ante un importante desfase entre la normativa y los interrogantes que irrumpirán cuando los objetos que nos rodean comiencen a recibir y emitir información a gran escala. Hemos de tener en cuenta que estos datos serán procesados por poderosos algoritmos con una enorme capacidad predictiva, lo que indudablemente refinará hasta límites insospechables el análisis de nuestros patrones comportamentales y biomédicos. En este capítulo se analizarán algunas de las implicaciones ético-jurídicas de estos problemas.

Finalmente, el profesor Fernando Martínez Cabezudo considera que la irrupción de las IA en la vida social ha supuesto un gran impacto debido a las capacidades que demuestran. Desde las que componen textos a dibujos o se utilizan en retoque fotográfico, hasta las usadas para el tratamiento de la voz. Hoy en día cada vez son más los ámbitos donde las podemos observar. En su trabajo se concentra en un tipo específico de IA, las generativas, que se caracterizan por ser capaces de generar obras partiendo de instrucciones que se les dan. Por ejemplo, la descripción de un paisaje para que este sea dibujado. Este tipo de software requiere un proceso de entrenamiento sobre el que se ciernen razonables dudas sobre su estatuto legal en el marco de la UE, además de implicar la apropiación y extracción de energías sociales, gracias a procesos y técnicas que tienen que ser problematizados. En este capítulo se analizan las interacciones que se dan entre el derecho de autor, la implicación de esos procesos de entrenamiento y esa extracción de beneficio. Con este fin, se presentarán y desarrollarán ideas como *plusvalía en red* y *general intellect* en red como herramientas conceptuales críticas para comprender como se establecen este tipo de relaciones.

EL IMPACTO DE INTERNET DE LAS COSAS EN LA CIUDADANÍA EUROPEA

Con el desarrollo de IoT (internet de las cosas), el procesamiento de datos amplía tanto su complejidad como sus posibilidades de uso, entre los que destaca el desarrollo de la IA. Al mismo tiempo, se identifican una serie de efectos colaterales de esta tecnología que impactan en nuestra democracia. Los datos, y la forma en qué son procesados, conllevan riesgos para la ciudadanía, cuya amenaza principal es que sus nuestras vidas diarias sean vigiladas o intervenidas. No obstante, junto con estos conflictos, el IoT genera grandes beneficios para las sociedades en diversos campos como puede ser el sector industrial o el médico, sin olvidar las posibilidades ligadas a la mejora de la prevención de riesgos potenciales para las personas e infraestructuras. En cualquier caso, no se puede caer en su mitificación ni en el pesimismo. El papel de la regulación es esencial en esta profunda transformación tecnológica en la que nos encontramos. El IoT supone un verdadero desafío para la ciudadanía europea. La UE ha realizado un notable esfuerzo legislativo, que nos ha situado como el área del mundo con una legislación más avanzada en la protección de derechos en el ecosistema cibernético. Pero no es suficiente. Este libro ofrece no solo una evaluación de la situación actual, sino también realiza propuestas para construir una ciudadanía europea en la que la tecnología sea una aliada, no una amenaza.

COORDINADOR

Rafael Rodríguez Prieto

AUTORES

Rafael Rodríguez Prieto, Fernando Martínez Cabezado, Adriana Fillol Mazo,
Miguel Ángel Martín López, Borja Montes Toscano, Pablo Antonio Fernández Sánchez,
Alejandro Manzorro Reyes, Ana Cristina Gallego Hernández,
Luis Miguel Arroyo Yanes, Christian Domínguez Expósito,
Noelia Arjona Hernández, Virginia Gutiérrez Barbarrusa, Manuel Jesús López Baroni

PVP: 32,00 €

ISBN: 978-84-1194-132-7



9 788411 941327