

ÍNDICE SISTEMÁTICO

PRÓLOGO	33
ABREVIATURAS	37
PARTE I. MARCO JURÍDICO DE LA ACTIVIDAD DIGITAL	49
CAPÍTULO I. CONCEPTO Y NORMATIVA SOBRE DERECHO DIGITAL	49
I. UNA APROXIMACIÓN AL CONCEPTO Y CARACTERIZACIÓN DEL DERECHO DIGITAL Y SU NORMATIVA	49
1. El «Derecho Digital»	49
2. Internet y tecnologías disruptivas	51
3. Sistematización de las normas reguladoras en el Derecho digital	54
3.1. El objeto: los «datos digitales»	54
3.2. Los sujetos: operadores en la sociedad digital	56
3.3. Los instrumentos de transmisión: telecomunicaciones, tecnologías disruptivas	61
3.4. Los resultados de la digitalización: digitalización de identidades y de procesos, y creación de figuras nuevas	61
4. Sistemática de esta obra	64
II. DERECHO INTERNACIONAL PRIVADO Y DERECHO DIGITAL	66
1. Internet como elemento multiplicador de la internacionalidad	66
2. Los Criterios de conexión de los Reglamentos RBI bis, RRI y RII en el entorno digital	67
2.1. Referencia a los foros del domicilio y sucursal en el RBI bis, y al concepto de residencia habitual del RRI	68

2.2.	El foro especial en materia de contratos en contratos que se ejecutan online	69
2.3.	Ilícitos a distancia y de daños plurilocalizados a través de Internet	69
A.	La «teoría de la ubicuidad» y la «teoría del mosaico»	69
B.	Aplicación de estas doctrinas a los casos de vulneración de derechos de la personalidad a través de Internet	70
C.	Daños plurilocalizados e ilícitos a distancia en casos de vulneración de marcas en Internet	72
D.	Aplicación del foro del art. 7.2 RBI bis a casos de vulneración de derechos de autor a través de Internet	73
E.	Aplicación del art. 7.2 RBI bis y del art. 6.1 RII en casos de competencia desleal a través de Internet	74
2.4.	Contratos de consumo en los que el profesional dirige sus actividades al Estado miembro del consumidor a través de Internet	75
2.5.	Celebración de acuerdos de elección de foro a través de medios electrónicos	78
3.	Incorporación de las tecnologías a los reglamentos comunitarios sobre notificación y obtención de pruebas	79
4.	Referencia a la e-Apostilla	81
III.	FISCALIDAD DE LA ECONOMÍA DIGITAL	82
1.	Objeto de estudio	82
2.	El IVA y el mercado de bienes y servicios digitales	83
2.1.	Dos ideas clave: predominancia de las prestaciones de servicios y tributación en el lugar de consumo	83
2.2.	Servicios de telecomunicaciones, televisión, radiodifusión y servicios prestados por vía electrónica	85
2.3.	Ventas a distancia de bienes. El papel de las interfaces digitales	88
A.	Ventas a distancia intracomunitarias de bienes	89
B.	Ventas a distancia de bienes importados de países y territorios terceros	90
3.	Economía digital y tributación internacional de los beneficios empresariales	91

3.1.	Desarrollos de política fiscal: los trabajos de la OCDE, la UE y la ONU	91
3.2.	El Impuesto sobre Determinados Servicios Digitales	94
IV.	DESINFORMACIÓN Y NOTICIAS FALSAS (LAS <i>FAKE NEWS</i>): MEDIDAS INTERNACIONALES Y EUROPEAS PARA COMBATIRLAS	99
CAPÍTULO II. INTERNET Y OTRAS TECNOLOGÍAS DISRUPTIVAS		105
I.	INTERNET. EVOLUCIÓN, RETOS Y GOBERNANZA	105
1.	Algunas consideraciones preliminares	105
2.	Evolución histórica de Internet.	107
3.	La web 2.0 y su evolución	113
4.	Internet: <i>common carrier</i> de nuevas tecnologías disruptivas y modelos de negocio	115
5.	Retos actuales: gobernanza y enfoques regulatorios de Internet.	116
II.	ALGUNAS TECNOLOGÍAS DISRUPTIVAS	119
1.	El «Internet of things» (IoT)	120
2.	Las «cadenas de bloques» (<i>blockchain</i>)	123
2.1.	La técnica de la «cadena de bloques» (<i>blockchain</i>)	123
A.	El comienzo: la <i>blockchain</i> de <i>bitcoin</i>	123
B.	La <i>blockchain</i> de <i>bitcoin</i> , y los demás sistemas DLT (<i>Distributed Ledger Technology</i>)	127
C.	La deriva actual: <i>blockchain</i> públicas y privadas, «con permisos» o «sin permisos»	128
D.	Eficacia y validez jurídica de redes informáticas basadas en tecnología DLT.	130
2.2.	Aplicaciones concretas y «casos de uso» de <i>blockchain</i>	132
2.3.	Intentos de regulación legal y creación de cadenas de bloques por parte de organismos oficiales y privados.	134
3.	La «computación en la nube» (<i>cloud computing</i>)	136
CAPÍTULO III. OPERADORES Y MODELOS DE NEGOCIO DE LA ECONOMÍA DIGITAL.		139
I.	INTRODUCCIÓN Y SISTEMÁTICA	139
II.	CATEGORÍAS LEGALES DE OPERADORES.	140

1.	Operadores de comunicaciones electrónicas.	140
2.	Operadores audiovisuales y medios de comunicación.	146
3.	Operadores en el mundo de Internet	149
4.	Reguladores y autoridades competentes	155
4.1.	Nacionales.	155
4.2.	Unión Europea.	158
III.	LOS PRINCIPALES MODELOS DE NEGOCIO.	159
1.	Los operadores de telecomunicaciones	159
1.1.	Grandes operadores de comunicaciones electrónicas.	160
1.2.	Operadores Móviles Virtuales (OMV)	162
1.3.	Prestadores de servicios de mensajería (SCI-IN)	163
1.4.	Prestadores de servicios de Internet of Things (IoT)	165
2.	El universo audiovisual y de los medios.	167
2.1.	Televisión	167
2.2.	Radio	169
2.3.	Prensa	169
3.	Las plataformas y otros intermediarios	170
3.1.	Mercados Virtuales	170
3.2.	Motores de búsqueda.	172
3.3.	Redes sociales	172
4.	Otros actores sectoriales	173
4.1.	Influencers	173
4.2.	Videojuegos.	174
4.3.	Blockchain.	175
IV.	LOS DELITOS DE DISCURSO DE ODIO EN LAS REDES SOCIALES	175
1.	El contexto de la regulación de los delitos de odio	175
2.	Iniciativas de la UE, el Consejo de Europa y el Tribunal Europeo de Derechos Humanos	176
3.	La polémica ley alemana «de las Redes Sociales» de 2017	177
4.	España, los delitos de discurso de odio	178
4.1.	Acciones que promueven un clima de violencia, hostilidad y odio	178
4.2.	Acciones con la motivación de discriminar por pertenecer a determinados grupos	180

4.3.	Enaltecimiento o justificación de delitos racistas, antisemitas o semejantes	180
4.4.	Difusión por redes sociales, la alteración de la paz pública, ámbito educativo	181
4.5.	Medidas de cese de la actividad del discurso de odio	182
CAPÍTULO IV. ÉTICA DIGITAL. AFECTACIÓN DE LOS DERECHOS DE LA PERSONALIDAD		183
I.	CÓMO LA ÉTICA DE LA VIRTUD PUEDE RELACIONARSE CON LA INTELIGENCIA ARTIFICIAL EN LOS NEGOCIOS.	183
1.	Definiciones de la IA y sus aplicaciones empresariales	183
2.	Vínculos entre la IA y la ética	185
3.	La ética de la virtud y la IA	188
4.	Conclusión	191
II.	VIDEOVIGILANCIA DIGITAL Y AFECTACIÓN DE LOS DERECHOS FUNDAMENTALES	191
1.	Videovigilancia, concepto y expansión. Desarrollo tecnológico y nuevos riesgos para los derechos.	191
2.	Marco regulatorio: complejidad y fragmentación.	193
2.1.	El régimen de la videovigilancia en la LOPDPGDD.	193
A.	La imagen como dato.	194
B.	Finalidad y legitimación para el tratamiento de los datos. Deber de información	195
C.	Fines, proporcionalidad e imprescindibilidad.	195
D.	Prohibiciones expresas.	196
E.	Conservación y destrucción de las imágenes	196
F.	Uso doméstico de la videovigilancia	197
2.2.	En particular, la videovigilancia en el ámbito de las relaciones laborales	197
2.3.	Regulación del uso de videocámaras por Fuerzas y Cuerpos de Seguridad	197
2.4.	Regulación del uso de videocámaras en el ámbito de la seguridad privada	199
2.5.	Videovigilancia en la investigación de delitos	199
2.6.	Otras previsiones	200

3.	Doble afectación y pluralidad de derechos y libertades fundamentales que pueden ser afectados por el uso de videocámaras.	200
III.	MENORES Y REDES SOCIALES	203
1.	La accesibilidad de las redes sociales en la era digital	203
2.	La afectación de los derechos de la personalidad de los menores en el entorno digital	205
2.1.	La difusión de contenido digital por parte de los progenitores.	206
2.2.	La difusión de contenido digital por parte de terceros	208
IV.	«RASTRO DIGITAL» Y «PATRIMONIO DIGITAL» AL FALLECIMIENTO DE LA PERSONA FÍSICA	209
1.	Introducción	209
2.	Derecho comparado	210
3.	Situación en España.	210
3.1.	La cuestión sucesoria en materia digital	210
3.2.	Regulación.	211
A.	LOPDPGDD	212
B.	Ley de Voluntades Digitales catalana	213
PARTE II. RÉGIMEN JURÍDICO DE LOS DATOS DIGITALES.		217
CAPÍTULO V. FUNDAMENTOS DEL RÉGIMEN JURÍDICO DE LOS DATOS DIGITALES.		217
I.	INTRODUCCIÓN: EL DATO COMO ACTIVO DIGITAL.	217
II.	EL CONCEPTO DE DATO DIGITAL Y SUS PRINCIPALES CATEGORÍAS	220
III.	LA ESTRATEGIA EUROPEA DE DATOS	223
IV.	EL ESTADO DE LA REGULACIÓN DEL DATO DIGITAL.	226
1.	Los datos personales y su protección prevalente en Europa	226
2.	La propiedad del dato digital (<i>data ownership</i>)	229
3.	La regulación de los datos abiertos (<i>open data</i>)	231
4.	Las normas sobre la libre circulación de datos no personales	232
5.	La gobernanza del dato (<i>data governance</i>).	234
V.	CONCLUSIONES	236

CAPÍTULO VI. PROTECCIÓN DE DATOS PERSONALES	237
I. IMPORTANCIA Y EVOLUCIÓN NORMATIVA	237
II. OBJETO Y ÁMBITO DE APLICACIÓN.	239
1. Objeto de protección.	240
2. Ámbito de aplicación material.	240
2.1. Datos personales	240
2.2. Tratamiento de datos personales	242
3. Ámbito de aplicación territorial	243
III. PRINCIPIOS GENERALES DEL TRATAMIENTO DE DATOS	243
1. Licitud, lealtad y transparencia	243
2. Limitación en la finalidad	244
3. Minimización de datos	245
4. Limitación del plazo de conservación	245
5. Exactitud	245
6. Integridad y seguridad	246
IV. BASES DE LEGITIMACIÓN O BASES JURÍDICAS DEL TRATAMIENTO. EN PARTICULAR EL CONSENTIMIENTO	247
V. DERECHOS DE LOS INTERESADOS	250
1. Derecho de acceso y el derecho a ser informado.	250
2. Derechos de rectificación, limitación en el tratamiento y supresión (derecho al olvido)	251
3. Derechos especialmente vinculados a tratamientos automatizados, <i>big data</i> e IA: derecho de oposición, a no ser objeto de decisiones basadas en perfiles, intervención humana y explicación	253
3.1. Derecho de oposición	253
3.2. Derecho a no ser objeto de una decisión automatizada individualizada basada en perfiles y derecho a obtener intervención humana	254
3.3. Derecho a la explicación	255
4. El derecho a la portabilidad de los datos	256
VI. RESPONSABLE DE TRATAMIENTO Y ENCARGADO DE TRATAMIENTO	257
VII. OBLIGACIONES, MEDIDAS E INSTRUMENTOS MATERIALES DE PROTECCIÓN.	259

1.	Medidas técnicas y organizativas de seguridad	259
2.	Evaluación de impacto en la protección de datos personales	260
3.	Registro de actividades de tratamiento.	261
4.	Obligación de notificación en caso de brechas de seguridad de datos personales	261
5.	Delegado de protección de datos	262
VIII.	TRANSFERENCIA DE DATOS A TERCEROS PAÍSES	263
1.	Transferencias basadas en una decisión de adecuación.	263
2.	Transferencias mediante garantías adecuadas	264
3.	Excepciones para situaciones específicas.	265
IX.	AUTORIDADES DE SUPERVISIÓN Y CONTROL. COOPERACIÓN Y RÉGIMEN SANCIONADOR.	266
X.	PROTECCIÓN DE DATOS PERSONALES EN LA IGLESIA	267
1.	La privacidad de las personas como bien jurídico canónico	267
2.	Ámbito competencial de la Iglesia y del Estado	268
3.	El Reglamento de la Unión Europea y el Decreto General de la Conferencia Episcopal Española	270
4.	La STS 698/2021, de 22 de febrero, sobre conservación de datos de antiguos miembros de una entidad religiosa	272
5.	Conclusión	273
CAPÍTULO VII. <i>BIG DATA</i> E INTELIGENCIA ARTIFICIAL.		275
I.	<i>BIG DATA</i> E INTELIGENCIA ARTIFICIAL	275
1.	Introducción al dato	275
1.1.	<i>Big data</i>	276
1.2.	Inteligencia artificial	277
1.3.	<i>Machine Learning</i>	280
1.4.	<i>Deep Learning</i>	281
1.5.	Retos de la inteligencia artificial	282
1.6.	La ciencia de los datos.	283
2.	Estadística	284
2.1.	Muestreo e inferencia	284
2.2.	Variables	284
2.3.	Estadística descriptiva	286
2.4.	Representaciones gráficas	288

2.5.	Probabilidad	291
2.6.	Distribución normal.	292
2.7.	Toma de decisiones	294
	A. Controversia del p-valor y reproducibilidad de los estudios	298
	B. Inferencia causal	299
	C. Estadística bayesiana	300
3.	Modelos	302
3.1.	Introducción	302
3.2.	Qué es un modelo de <i>Machine Learning</i>	304
3.3.	Cómo leer e interpretar los resultados de un modelo	305
	A. Ejemplo de regresión lineal múltiple	306
	B. Ejemplo de árbol de decisión.	308
	C. Ejemplo de regresión logística	309
	D. Algoritmos	310
	E. Cómo evaluar un modelo concreto	312
	F. Validación cruzada (<i>cross-validation</i>).	313
	G. Otros temas importantes al evaluar un modelo	315
	H. Selección de modelos	316
4.	<i>Big data</i> en el ámbito jurídico	317
4.1.	Sesgo cognitivo del tribunal	317
4.2.	Huella digital	319
4.3.	Casos similares	319
5.	<i>Big data</i> en las Ciencias Sociales	320
5.1.	Aporte del <i>big data</i> a las ciencias sociales	322
II.	PROBLEMAS JURÍDICOS QUE PLANTEAN ALGUNAS MANIFESTACIONES DE INTELIGENCIA ARTIFICIAL	323
1.	La regulación de la inteligencia artificial en el derecho de la Unión Europea	323
1.1.	Introducción	323
1.2.	Propuesta de Reglamento para una Ley de Inteligencia Artificial	324
	A. Objetivos	324
	B. Definición y ámbito de aplicación	325
	C. Visión: regulación en función del riesgo.	326
	D. Regulación e innovación	328

1.3.	Conclusión	328
2.	Códigos de conducta responsable en productos de IA	329
2.1.	Los códigos de conducta responsable en la era de la transformación digital	329
2.2.	Recomendaciones de buenas prácticas sobre elaboración de perfiles y decisiones automatizadas	330
A.	El Derecho a la información.	331
B.	El consentimiento como base del tratamiento.	331
C.	Derecho de acceso.	331
D.	Derecho de rectificación	332
E.	Derecho de oposición	332
F.	El establecimiento de garantías adecuadas	332
2.3.	Un caso concreto: el código de conducta responsable de Analizza.me	333
3.	Robots.	336
3.1.	Hacia un Derecho de los robots.	336
3.2.	La responsabilidad por daños causados por el robot	338
3.3.	Estatuto jurídico del robot	340
4.	<i>Smart cities</i>	341
4.1.	Definición de ciudad inteligente	341
4.2.	Aplicaciones	342
A.	Seguridad.	343
B.	Gestión de los recursos: agua, residuos y aire.	343
C.	Energía.	344
D.	Transporte y movilidad.	345
E.	Gestión de datos	345
4.3.	Normativa	346
4.4.	Planes y proyectos	347
4.5.	Organismos	348
CAPÍTULO VIII. CIBERSEGURIDAD		349
I.	CIBERSEGURIDAD: ASPECTOS TÉCNICOS	349
1.	Introducción	349
1.1.	Definición de Ciberseguridad	350
1.2.	Medios y objetivos de la ciberseguridad	352

1.3.	Riesgo	353
2.	Conocer, comprender y modelar las amenazas	355
2.1.	Ataques de hardware	355
2.2.	Ataques de observación	355
2.3.	Ataques de penetración	356
2.4.	Ataques de software dirigidos a <i>hardware</i>	356
2.5.	Ataques de red	356
2.6.	Ataques contra el sistema de nombres de dominio (DNS).	357
2.7.	Ataques contra el enrutamiento entre dominios del <i>Border Gateway Protocol</i> (BGP).	358
2.8.	Ataques de software	358
2.9.	Vulnerabilidades en la gestión de la memoria	359
2.10.	Vulnerabilidades en la generación de resultados estructurados.	360
2.11.	Ataques contra el usuario: ingeniería social y <i>phishing</i>	361
3.	Criptografía	362
3.1.	Primitivas criptográficas	363
3.2.	Esquemas criptográficos	364
3.3.	Protocolos y servicios criptográficos	364
4.	<i>Malware</i>	365
4.1.	Taxonomía del malware	366
4.2.	Programas potencialmente no deseados (PUPs)	368
II.	CIBERSEGURIDAD: VISIÓN JURÍDICA INTERNACIONAL Y UNIÓN EUROPEA	369
1.	La cibernética y el orden internacional: retos y respuestas.	369
2.	La ciberdefensa activa y pasiva: planteamientos generales y algunos ejemplos.	369
3.	Respuestas del Derecho Internacional frente a los ciberataques.	372
3.1.	El Derecho internacional de la responsabilidad y las contramedidas frente al ciberataque de un Estado o de un actor no-estatal	372
3.2.	El uso de la fuerza, según la Carta de las Naciones Unidas y la legítima defensa contra los ciberataques	375
A.	Los ciberataques como «ataques armados» en el sentido de la Carta de las Naciones Unidas	376

B.	Las operaciones cibernéticas y legítima defensa: contra quién, su necesidad y proporcionalidad.	378
4.	Las estrategias de ciberseguridad de la Unión Europea	381
4.1.	La ciberdefensa activa y pasiva de la UE: planteamientos generales	381
4.2.	La política transversal interna de la UE en ciberseguridad: algunos desarrollos normativos	382
4.3.	La ciberdiplomacia de la UE: algunos ejemplos más destacados	385
PARTE III. DIGITALIZACIÓN DE IDENTIDADES, ACTIVIDADES Y PROCESOS.		391
CAPÍTULO IX. IDENTIDAD DIGITAL, FIRMA ELECTRÓNICA Y REPUTACIÓN <i>ONLINE</i>		391
I.	IDENTIDAD DIGITAL Y FIRMA ELECTRÓNICA	391
1.	Planteamiento general	391
2.	Concepto de identidad digital	392
3.	Conceptos de firma electrónica y servicios de confianza	396
4.	Valor jurídico y valor probatorio de la firma electrónica	399
II.	REPUTACIÓN <i>ONLINE</i>	402
1.	Planteamiento general	402
2.	Reputación <i>online</i> y derecho al honor y a la propia imagen	403
3.	Libertad de información y de expresión	405
3.1	Distinción entre libertad de información y libertad de expresión	405
3.2.	Requisitos de la prevalencia de la libertad de información	405
3.3.	Requisitos de la prevalencia de la libertad de expresión	407
4.	Grupos de casos digitales	407
4.1.	Comentarios de consumidores y usuarios sobre las prestaciones ajenas	407
4.2.	Vindicación «ad personam».	408
4.3.	Utilización in consentida de la imagen de personas	409
4.4.	Caricaturas como excusa para la explotación ilícita del derecho a la imagen.	411

4.5.	Manifiestos en la red	411
4.6.	Papel de los prestadores de servicios de la sociedad de la información.	412
CAPÍTULO X. DIGITALIZACIÓN DE PROCESOS.		415
I.	ADMINISTRACIONES PÚBLICAS: ALGUNAS CUESTIONES DE DERECHO DIGITAL	415
1.	Datos abiertos y reutilización de la información pública	415
2.	La gobernanza de la interoperabilidad y el esquema nacional de interoperabilidad.	420
3.	Ciberseguridad de las Administraciones Públicas: el Esquema Nacional de Seguridad.	425
II.	<i>REGTECH Y SUPTECH</i>	428
III.	DIGITALIZACIÓN EN LA ADMINISTRACIÓN DE JUSTICIA	432
1.	Algunos aspectos de la digitalización en el proceso civil	432
1.1.	Prueba digital.	432
A.	Conceptos generales	432
B.	Proposición de la prueba digital.	434
C.	Admisión de la prueba.	436
D.	Práctica de la prueba	437
E.	Valoración de la prueba de instrumentos	438
1.2.	Expediente judicial electrónico	439
1.3.	Subasta electrónica	442
2.	Digitalización y administración de Justicia Penal.	444
2.1.	Introducción	444
2.2.	Las medidas de investigación tecnológicas [Libro II, Título VIII, capítulos IV a X, arts. 588 bis.a) a 588 bis.k) LECrim]	445
A.	Las disposiciones comunes a las medidas de investigación tecnológica.	445
B.	La interceptación de las comunicaciones telefónicas y telemáticas	447
C.	La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos	451

	D.	La utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización	452
	E.	El registro de dispositivos de almacenamiento masivo de información.	454
	F.	El registro remoto sobre equipos informáticos	454
	G.	Las medidas de aseguramiento.	456
3.		Los medios alternativos de solución de controversias en el entorno digital	456
3.1.		Introducción: desarrollo e impulso de los ADRs y ODRs.	456
3.2.		Los sistemas ODR según UNCITRAL: concepto, principios y procedimiento	458
3.3.		Un ejemplo de ODR: el sistema europeo <i>online</i> de solución de conflictos en materia de consumo.	460
3.4.		El arbitraje electrónico en España	461
	A.	La validez y eficacia jurídica del convenio arbitral, del procedimiento y del laudo arbitral por medios electrónicos.	461
	B.	La previsión del arbitraje electrónico en el Sistema Arbitral de Consumo	464
IV.		<i>LEGALTECH</i>	466
	1.	Concepto y significación	466
	2.	Aplicaciones de <i>LegalTech</i> más comunes	467
	3.	Implicaciones jurídicas	469
V.		REGISTROS PÚBLICOS Y DIGITALIZACIÓN	470
	1.	Introducción	470
	2.	Registro telemático: presentación remota de documentación	471
	3.	Registro gráfico: interoperabilidad de la información territorial.	473
	4.	Registro digital: digitalización del contenido del registro y publicidad formal	477
	5.	Registro distribuido: ¿una oportunidad para <i>blockchain</i> ?	479
VI.		FE PÚBLICA Y DIGITALIZACIÓN	481
	1.	Introducción	481
	2.	La firma electrónica de los notarios	482
	3.	El documento notarial electrónico.	483

4.	Los deberes de colaboración notarial con la Administración electrónica.	486
5.	Facultades de actuación notarial remota	487
6.	Legitimación notarial de firmas electrónicas	489
VII.	LA DIGITALIZACIÓN DE PROCESOS EN SOCIEDADES MERCANTILES: CONSTITUCIÓN Y OPERATIVA DE LOS ÓRGANOS SOCIETARIOS.	491
1.	La digitalización de la constitución y la publicidad registral de sociedades mercantiles	491
2.	Llevanza de registros de socios mediante <i>blockchain</i> y otros mecanismos DLT	493
3.	Digitalización en las comunicaciones y en los órganos de las sociedades de capital	494
3.1.	Consideraciones generales.	494
3.2.	La página web corporativa como instrumento de información	495
3.3.	Comunicaciones societarias.	497
3.4.	La digitalización de la junta general.	498
A.	La convocatoria por medios digitales	498
B.	El derecho de información previo a la celebración de la junta	499
C.	La asistencia a la junta general	501
D.	El voto anticipado	506
3.5.	Incidencia de la tecnología en el órgano de administración.	507
3.6.	Anomalías en el funcionamiento y uso incorrecto de los dispositivos digitales.	509
VIII.	JUEGO ONLINE. ESPORTS	511
1.	Juego <i>online</i>	511
2.	Los <i>eSports</i>	514
IX.	EHEALTH Y MHEALTH	516
	CAPÍTULO XI. DIGITALIZACIÓN DE ACTIVIDADES Y CONTRATOS	521
I.	SMART CONTRACTS	521
1.	Preliminar	521
2.	Origen, evolución y aplicaciones	523

3.	Delimitación, naturaleza jurídica y diseño y dinámica funcionales.	527
4.	Caracterización, fuentes regulatorias y problemática jurídica	534
5.	Observaciones finales	544
II.	PROTECCIÓN DEL CONSUMIDOR Y DERECHO DIGITAL	544
1.	El fundamento de la tutela a los consumidores en el marco del Derecho digital	544
2.	El consumidor digital: concepto y ámbitos de protección	546
2.1.	El usuario de los servicios de juego de azar en línea	547
2.2.	El usuario de una plataforma en línea en la que negocia instrumentos financieros.	548
2.3.	El usuario de una plataforma en línea en la que ofrece la venta de bienes nuevos y usados.	549
2.4.	El usuario de una red social en la que publica contenidos personales y profesionales.	550
3.	El <i>corpus</i> normativo de tutela del consumidor digital	551
4.	Los derechos del consumidor digital	553
4.1.	El derecho a la información pre-contractual.	553
4.2.	El derecho de desistimiento	554
4.3.	El derecho a la garantía legal de conformidad	555
III.	COMERCIO ELECTRÓNICO. CONTENIDOS DIGITALES	555
1.	Introducción	555
2.	Contratación de bienes y servicios digitales.	556
2.1.	El contrato de suministro de contenidos y servicios digitales	556
A.	Objeto del contrato	556
B.	El precio.	557
2.2.	El contrato de compraventa de bienes muebles con elemento digital.	559
3.	Protección al consumidor de bienes, contenidos y servicios digitales.	560
3.1.	Entrega o suministro de los bienes, contenidos o servicios digitales	560
3.2.	Conformidad de los bienes, contenidos o servicios digitales entregados o suministrados con el contrato	561

3.3.	Régimen de las acciones o remedios por el defecto o falta de conformidad de los bienes, contenidos o servicios digitales entregados o suministrados	563
A.	Remedios primarios	563
B.	Remedios secundarios	564
3.4.	Plazos	567
3.5.	Modificación de los contenidos o servicios digitales	568
IV.	ACTIVIDADES FINANCIERAS Y DE PAGO EN EL MARCO DIGITAL	568
1.	La actividad financiera y la digitalización	568
1.1.	Tecnologías digitales y financiación	568
1.2.	El <i>Digital Finance Package</i> comunitario	569
2.	El sistema de pagos dentro de la economía digital	571
2.1.	Contexto y marco general	571
A.	Servicios de pago minorista	572
B.	Servicios y sistemas de pago al por mayor	573
2.2.	Los sujetos en la actividad de servicios de pagos minoristas	575
2.3.	Servicios de pago y derecho a acceder a una cuenta de pago	576
2.4.	Derechos y obligaciones	579
3.	El dinero electrónico	581
4.	Los «criptoactivos» o «tokens»	583
4.1.	Concepto y clases de criptoactivos	583
4.2.	Los «mercados de criptoactivos»: emisores, plataformas de creación e intercambio de criptoactivos, exchanges y wallets	587
4.3.	Regulación sobre criptoactivos	590
A.	Derecho Comunitario. Propuesta de Reglamento comunitario sobre mercados de criptoactivos (<i>Markets in cryptoassets Proposal</i>)	590
B.	España	594
4.4.	En particular, criptomonedas	597
A.	Las criptomonedas	597
B.	En particular, las «stablecoins»	599
C.	En particular, las «divisas digitales de Banco Central» (<i>CBDC</i> o <i>GovCoins</i>)	600

4.5.	En particular, <i>security tokens</i> e «instrumentos financieros»	601
4.6.	Financiación a través de la emisión de tokens: ICOs y STOs	603
	A. Generalidades	603
	B. Características de la emisión: el « <i>white paper</i> »	604
	C. Riesgos para el <i>tokenholder</i>	605
	D. Regulación legal. Diferencias con otras formas de financiación	607
4.7.	Tratamiento fiscal de los criptoactivos	608
5.	El universo de servicios y entidades <i>FinTech</i> y <i>TechFin</i>	612
6.	Economía colaborativa y plataformas digitales de pago o financiación.	617
V.	APLICACIÓN DE TÉCNICAS DIGITALES EN LA ACTIVIDAD CONTRACTUAL EN OTROS ÁMBITOS AJENOS A LA FINANCIACIÓN	618
1.	Operativa de sociedades a través de <i>smart contracts</i> : la DAO	618
2.	Uso de plataformas en la negociación privada.	620
3.	Prestación de servicios, arrendamiento de bienes y distribución: <i>advising</i> , <i>car sharing</i> y <i>dropshipping</i>	622
4.	Digitalización y transporte.	624
	4.1. Planteamiento	624
	4.2. Documentación electrónica.	625
	4.3. Redes blockchain aplicadas al comercio marítimo.	626
	A. Como forma de mejorar la eficiencia portuaria, o de operar la intermediación entre los sujetos	626
	B. Como forma de monitorizar diversos aspectos de la situación de la mercancía	628
	C. Como forma de programar el cumplimiento automático de ciertas prestaciones objetivas	629
	D. Como forma de combinar todos los aspectos señalados	629
5.	Digitalización y seguros: <i>Insurtech</i>	630
	5.1. El fenómeno InsurTech	630
	5.2. Supuestos de InsurTech	632

5.3.	InsurTech y la regulación de acceso y ejercicio de la actividad	635
6.	Digitalización y contratos sobre energía	637
6.1.	Planteamiento	637
6.2.	Trazabilidad de energías renovables	639
6.3.	Redes de autoconsumo colaborativo	639
VI.	DERECHO LABORAL Y DERECHO DIGITAL	641
1.	El marco jurídico de la Unión Europea	641
1.1.	Inteligencia artificial (IA) y robótica	642
1.2.	Transformación digital y nuevas competencias	645
1.3.	Protección de datos	645
1.4.	Regulación del teletrabajo	647
1.5.	Mejora de las condiciones laborales de los trabajadores de plataformas	648
2.	El marco jurídico en España.	650
2.1.	Protección de la privacidad e intimidad en el puesto de trabajo	651
2.2.	La clarificación de las nuevas formas de trabajo: el debate sobre la calificación jurídica de los «riders»	660
2.3.	El derecho a la desconexión fuera del horario de trabajo	662
2.4.	Otros aspectos	662
	CAPÍTULO XII. CIBERCRIMINALIDAD	665
I.	LOS DELITOS INFORMÁTICOS O CIBERDELITOS	665
1.	Introducción	665
2.	El nuevo escenario criminológico y el Derecho penal	666
3.	Clasificación de la delincuencia informática	667
4.	Análisis de los tipos delictivos concretos	668
4.1	Delitos que tienen como objeto los sistemas informáticos. Cibercriminología	668
A.	Los daños y sabotajes a sistemas informáticos (arts. 264, 264 bis, 264 ter y 264 quáter CP).	668
B.	Otros cibercriminológicos	669
4.2.	Delitos por medios informáticos	670
A.	Delincuencia económica	671

	B.	Delincuencia sexual	672
	C.	El terrorismo en el ciberespacio	673
II.		RESPONSABILIDAD POR DELITOS EN CONTEXTOS DIGITALES	675
	1.	Introducción	675
	2.	Determinación de la responsabilidad.	676
	2.1.	Responsabilidad de la persona física	676
	2.2.	Responsabilidad junto con la persona física.	678
	2.3.	Responsabilidad más allá de la persona física	681
	3.	Consecuencias sancionatorias	683
III.		<i>BIG DATA</i> , INTELIGENCIA ARTIFICIAL Y PREVENCIÓN DE DELITOS.	683
	1.	Introducción	683
	2.	Los niveles de la inteligencia artificial y su relación con la criminología y el Derecho penal	684
	3.	Los efectos de la inteligencia artificial débil sobre el Sistema penal.	687
PARTE IV. COMPETENCIA Y PROPIEDAD INTELECTUAL EN LA SOCIEDAD DIGITAL.			693
CAPÍTULO XIII. DEFENSA DE LA COMPETENCIA EN MERCADOS DIGITALES.			693
I.		INTRODUCCIÓN	693
II.		ESPECIALES CARACTERÍSTICAS DE LOS MERCADOS DIGITALES	698
	1.	El comercio electrónico como nuevo canal de distribución.	699
	2.	Las plataformas digitales como nuevos modelos de negocio	699
III.		EL MERCADO RELEVANTE	703
IV.		PROHIBICIÓN DE ACUERDOS RESTRICTIVOS DE LA COMPETENCIA EN MERCADOS DIGITALES	705
	1.	Prohibición de acuerdos horizontales. Nuevas formas de cárteles	705
	2.	Prohibición de acuerdos verticales en mercados digitales	708
	2.1.	Fijación de precio de reventa.	710
	2.2.	Restricción de ventas pasivas y geobloqueo.	711
	2.3.	Prohibiciones de venta en canales <i>online</i>	712
	2.4.	Las «cláusulas de paridad» o NMF.	714

V.	ABUSO DE POSICIÓN DE DOMINIO EN MERCADOS DIGITALES	717
VI.	CONCENTRACIONES EN MERCADOS DIGITALES	726
	ANEXO	731
CAPÍTULO XIV. COMPETENCIA DESLEAL EN LA SOCIEDAD DIGITAL		735
I.	CONSIDERACIONES INTRODUCTORIAS	735
	1. Encuadramiento sistemático	735
	2. Caracterización del ilícito de competencia desleal y ámbito objetivo	737
	3. Estructura normativa y técnica de aplicación	738
	4. Relaciones con otras disciplinas de la competencia	740
	4.1. Propiedad intelectual (entendida en sentido amplio como propiedad industrial e intelectual) y competencia desleal	740
	4.2. Libre competencia y competencia desleal	741
II.	TIPOS ESPECIALES DE DESLEALTAD	741
	1. Actos de engaño y omisiones engañosas	741
	1.1. Contenido	741
	1.2. Grupos de casos digitales	742
	2. Actos de confusión	743
	2.1. Contenido	743
	2.2. Grupos de casos digitales	743
	3. Prácticas agresivas	744
	3.1. Contenido	744
	3.2. Grupos de casos digitales	745
	4. Actos de denigración	745
	4.1. Contenido	745
	4.2. La denigración en el ámbito de Internet	746
	5. Actos de comparación	747
	5.1. Contenido	747
	5.2. Grupos de casos digitales	747
	6. Actos de imitación	748
	6.1. Contenido	748

6.2.	Grupos de casos digitales.	749
7.	Actos de explotación de la reputación ajena	749
7.1.	Contenido	749
7.2.	Grupos de casos digitales.	749
8.	Violación de secretos.	751
8.1.	Contenido	751
8.2.	El software como secreto empresarial	751
9.	Inducción a la infracción contractual.	752
9.1.	Contenido	752
9.2.	Grupos de casos digitales.	752
A.	<i>Cracking</i>	752
B.	<i>Screen scraping</i>	753
10.	Violación de normas	753
10.1.	Contenido	753
10.2.	Grupos de casos digitales.	753
11.	Discriminación y dependencia económica	754
11.1.	Contenido	754
11.2.	Grupos de casos digitales.	755
III.	CLÁUSULA GENERAL DE DESLEALTAD.	755
1.	Contenido	755
2.	Grupos de casos digitales	758
 CAPÍTULO XV. PROPIEDAD INTELECTUAL		761
I.	DE LA SOCIEDAD DE LA INFORMACIÓN AL MERCADO ÚNICO DIGITAL	761
II.	LOS NUEVOS OBJETOS DE PROTECCIÓN POR LA PROPIEDAD INTELECTUAL EN LA ERA DIGITAL	765
1.	La protección de los programas de ordenador	766
2.	La protección de las bases de datos electrónicas	770
III.	ADAPTACIÓN DE LOS DERECHOS DE EXPLOTACIÓN AL ENTORNO DIGITAL	773
1.	El derecho de reproducción.	773
2.	El derecho de distribución	776
3.	El derecho de comunicación al público.	778
3.1.	El concepto de «acto comunicativo»	779
3.2.	El concepto de «público».	782

IV.	ADAPTACIÓN DE LOS LÍMITES AL ENTORNO DIGITAL	785
1.	La copia para uso privado en el entorno digital	788
2.	La minería de textos y datos.	791
3.	Ilustración de la enseñanza en un entorno digital transfronterizo.	792
4.	Obras huérfanas y obras fuera del circuito comercial	793
4.1.	El límite de obras huérfanas	794
4.2.	El límite de obras fuera del circuito comercial	795
5.	La agregación de contenidos en línea	797
V.	ADAPTACIÓN DE LOS MEDIOS DE TUTELA AL ENTORNO DIGITAL	798
1.	Novedades en los medios de tutela civil	799
2.	Novedades en los medios de tutela penal	800
3.	Novedades en los medios de tutela administrativa.	801
CAPÍTULO XVI. PROPIEDAD INDUSTRIAL Y DERECHO DIGITAL		803
I.	INTRODUCCIÓN	803
II.	INTRODUCCIÓN A LOS SIGNOS DISTINTIVOS EN EL ENTORNO DIGITAL.	803
1.	Marcas.	804
2.	Nombres de dominio.	805
3.	Carácter territorial de la propiedad industrial y globalidad del entorno digital	807
III.	GRUPOS DE CASOS DE UTILIZACIÓN DE MARCAS EN EL ENTORNO DIGITAL	809
1.	Uso de marcas como nombres de dominio	809
2.	Reproducción de marcas en el entorno digital.	811
3.	Uso de marcas en buscadores	814
3.1.	Adwords y enlaces patrocinados	815
3.2.	Resultados naturales de búsquedas	816
4.	Comercio electrónico y agotamiento del derecho de marca	817
5.	Otros casos de uso de signos en la economía digital	819
IV.	LAS INVENCIÓNES Y EL DERECHO DE PATENTES EN EL ENTORNO DIGITAL	820
1.	Algunas notas introductorias	820

2.	Exclusiones, prohibiciones y requisitos de patentabilidad . .	821
2.1.	Exclusiones	821
2.2.	Prohibiciones	823
2.3.	Requisitos de patentabilidad	824
3.	Contenido del derecho y alcance de la protección	825
3.1.	Contenido del derecho	825
3.2.	Alcance de la protección	826
	ÍNDICE ANALÍTICO	827
	NORMATIVA DE DERECHO DIGITAL	853