

## Índice general

### Página

#### **HACIA NUEVOS RETOS Y METAS EN EL USO DE LA INFORMACIÓN Y LOS DATOS PERSONALES EN LOS PROCESOS Y EN LOS PROCEDIMIENTOS SANCIONADORES**

IGNACIO COLOMER HERNÁNDEZ ..... 25

#### **PRIMERA PARTE**

#### **INFORMACIÓN Y DATOS PERSONALES EN LAS INVESTIGACIONES PENALES**

#### **HALLAZGOS CASUALES EN REGISTROS SOBRE DISPOSITIVOS ELECTRÓNICOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN O EN REGISTROS Y RASTREOS REMOTOS DE EQUIPOS INFORMÁTICOS**

RODRIGO MORENO FUENTES ..... 47

#### **1. Los hallazgos casuales y sus clases ..... 48**

1.1. *La noción de hallazgo casual* ..... 48

1.2. *Las clases de hallazgos* ..... 52

1.2.1. Hallazgo casual subjetivo y hallazgo casual objetivo ..... 52

1.2.2. Hallazgo casual obtenido en el curso de una diligencia de entrada y registro en domicilio, y hallazgo casual obtenido en el curso de una medida de intervención de las comunicaciones ..... 55

<b>2. La regulación de los hallazgos casuales en las diligencias de intervención de las comunicaciones y tecnológicas</b> .....	56
2.1. <i>Las diligencias de intervención de las comunicaciones y tecnológicas</i> .....	57
2.2. <i>Los arts. 579 bis y 588 bis I de la LECRIM</i> .....	59
<b>3. El supuesto de investigaciones sobre dispositivos electrónicos de almacenamiento masivo y los registros y rastreos remotos de equipos informáticos</b> .....	65
3.1. <i>Hallazgo casual en el registro de dispositivos de almacenamiento masivo de información</i> .....	66
3.1.1. El análisis de dispositivos electrónicos de almacenamiento masivo .....	66
3.1.2. La autorización judicial de acceso al dispositivo ...	68
3.1.3. Los hallazgos casuales en esta diligencia de investigación .....	72
3.1.3.1. Valor meramente investigador de lo encontrado y necesidad de cobertura de la autorización judicial original .....	74
3.1.3.2. Eventual valor probatorio de lo hallado en casos de flagrancia .....	77
3.1.3.3. El juego del principio de proporcionalidad .	83
3.2. <i>Hallazgo casual en el registro y rastreo remoto sobre equipos informáticos</i> .....	85
3.2.1. El registro y rastreo remoto sobre equipos informáticos .....	85
3.2.2. La autorización judicial de acceso al dispositivo ...	88
3.2.3. Los hallazgos casuales en esta diligencia de investigación .....	89
3.2.3.1. Valor investigador o probatorio de lo encontrado y necesidad de cobertura de la autorización judicial original en función de si se interceptan las comunicaciones o no ...	89
3.2.3.2. El juego del principio de proporcionalidad .	92
<b>4. Conclusiones</b> .....	97

## LA UTILIZACIÓN EN LA INVESTIGACIÓN PENAL DE DISPOSITIVOS TÉCNICOS DE SEGUIMIENTO Y DE LOCALIZACIÓN

PABLO GRANDE SEARA .....	101
<b>1. Introducción .....</b>	<b>101</b>
<b>2. Afectación de derechos fundamentales .....</b>	<b>106</b>
<b>3. La utilización de dispositivos técnicos de seguimiento y localización en la LECRIM .....</b>	<b>109</b>
3.1. <i>Situación anterior a la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre</i> .....	109
3.2. <i>Régimen jurídico actual de la utilización en la investigación penal de dispositivos técnicos de seguimiento y localización</i> .....	112
3.2.1. <i>Solicitud de autorización judicial. Los indicios de criminalidad</i> .....	113
3.2.2. <i>Autorización judicial de la medida</i> .....	116
3.2.2.1. <i>Juez competente</i> .....	116
3.2.2.2. <i>Contenido del auto habilitante</i> .....	117
3.2.3. <i>Adopción policial de la medida</i> .....	122
3.2.4. <i>Duración de la medida</i> .....	125
3.2.5. <i>Sujetos obligados a la asistencia y colaboración</i> ...	127
3.2.6. <i>Control judicial de la práctica de la medida</i> .....	128
<b>4. Bibliografía .....</b>	<b>129</b>

## EL INFORME GOING DARK: ¿EL FUTURO DE LA LEGISLACIÓN EUROPEA EN MATERIA DE ACCESO A LOS DATOS ELECTRÓNICOS?

JUAN ALEJANDRO MONTORO SÁNCHEZ .....	131
<b>1. Introducción: el nuevo contexto digital y sus implicaciones para la justicia penal .....</b>	<b>132</b>
<b>2. El análisis forense digital en la Unión Europea: desafíos actuales y estrategias para el fortalecimiento de las capacidades ...</b>	<b>137</b>

	<u>Página</u>
2.1. <i>Soluciones propuestas por el grupo de alto nivel para el análisis forense digital</i> .....	140
<b>3. La retención de datos de comunicaciones electrónicas con fines penales: desafíos persistentes y propuestas del grupo de alto nivel para un marco renovado</b> .....	142
3.1. <i>Propuestas y recomendaciones del grupo de alto nivel para la conservación de metadatos de tráfico</i> .....	145
<b>4. La interceptación de comunicaciones en la Unión Europea: desafíos en la era digital y propuestas para mejorar su eficacia</b> ..	148
4.1. <i>Propuestas del grupo de alto nivel para la interceptación de las comunicaciones</i> .....	155
<b>5. Conclusiones</b> .....	157

## NUEVOS RETOS EN LA LEGISLACIÓN Y JURISPRUDENCIA ESPAÑOLA SOBRE CONSERVACIÓN PREVENTIVA DE DATOS RELATIVOS A LAS COMUNICACIONES

JOSÉ LUIS RODRÍGUEZ LAINZ .....	161
<b>1. Introducción</b> .....	161
<b>2. De la negación absoluta de regímenes de conservación generalizada e indiscriminada de datos relativos a las comunicaciones a la búsqueda de líneas de apertura</b> .....	165
<b>3. Hacia la convergencia del Tribunal Europeo de Derechos Humanos con la jurisprudencia del TJUE</b> .....	178
<b>4. El difícil reto de la STJUE del caso La Quadrature du NET II</b> ..	189
<b>5. La delicada situación de la legislación y jurisprudencia nacionales sobre conservación generalizada e indiscriminada de datos relativos a comunicaciones electrónicas</b> .....	195
5.1. <i>Diagnosis crítica de la ley española de conservación de datos frente a la hostil jurisprudencia del TJUE</i> .....	195
5.2. <i>La escasa permeabilidad de la jurisprudencia del TJUE sobre conservación preventiva de datos relativos a las comunicaciones en la jurisprudencia de Sala 2.<sup>a</sup> del Tribunal Supremo</i> .....	214
<b>6. Bibliografía</b> .....	222

**OBTENCIÓN, CONSERVACIÓN, CUSTODIA Y CESIÓN DE LAS VIDEOGRABACIONES DE VÍAS Y ESPACIOS PÚBLICOS REALIZADAS POR LOS SISTEMAS DE SEGURIDAD PRIVADA**

PABLO AZAÚSTRE RUIZ .....	227
1. Introducción .....	227
2. Obtención y captación de imágenes y sonidos por los sistemas de grabación de la seguridad privada .....	229
3. Consecuencias previstas en la Ley de Seguridad Privada por la captación de imágenes y sonidos en vías y espacios públicos .	230
4. Conservación y cesión de las videograbaciones a las causas penales .....	234
5. Conclusiones .....	236
6. Bibliografía .....	237

**SEGUNDA PARTE**

**INFORMACIÓN Y DATOS PERSONALES  
EN LOS PROCESOS PENALES**

**LA DIALÉCTICA ENTRE INFORMACIÓN, PRUEBA Y DATOS EN LA EVOLUCIÓN DE LAS CULTURAS JUDICIALES EUROPEAS**

STEFANO RUGGERI .....	241
1. Premisa. La creciente movilidad de información, prueba y datos y los retos para una protección adecuada de los derechos individuales en la era de la comunicación digital .....	242
2. La movilidad de información, prueba y datos en el marco de la liberalización de las relaciones entre procedimientos y al hilo de la evolución del principio de reconocimiento mutuo .....	243
3. La contaminación mutua .....	250
3.1. La «datificación» de la prueba penal .....	250
3.2. La «probatificación» de informaciones y datos .....	254
4. Conclusiones. Las transformaciones del fenómeno probatorio y su involución hacia la lógica demostrativa .....	256

## **PRIVACIDAD Y DATOS PERSONALES EN EL PROCESO PENAL ITALIANO: CUESTIONES CRÍTICAS EN LA ERA DE LA INNOVACIÓN DIGITAL**

ANTONELLA FALCONE .....	261
<b>1. Introducción .....</b>	<b>261</b>
<b>2. Privacidad y protección de datos personales: desafíos estructurales en el marco del proceso penal .....</b>	<b>264</b>
<b>3. Privacidad y protección de datos personales: entre estándares de derecho supranacional y normativa nacional .....</b>	<b>267</b>
<b>4. Principio de proporcionalidad, privacidad y protección de datos personales: perfiles críticos en el sistema jurídico italiano .....</b>	<b>277</b>
4.1. <i>El principio de proporcionalidad en el marco de la normativa europea en tema de data retention .....</i>	<i>277</i>
4.2. <i>La retención de datos personales entre desproporcionalidad normativa y riesgos sistémicos .....</i>	<i>283</i>
<b>5. Tratamiento «diferenciado» de los datos personales .....</b>	<b>290</b>
<b>6. Conclusión .....</b>	<b>293</b>

## **LA VIDEOVIGILANCIA POR PARTICULARES A TRAVÉS DE CÁMARAS ON BOARD Y SU UTILIZACIÓN COMO PRUEBA EN EL PROCESO PENAL**

M. <sup>a</sup> ÁNGELES CATALINA BENAVENTE .....	295
<b>1. Introducción: la utilización de cámaras <i>on board</i> con fines de videovigilancia .....</b>	<b>296</b>
<b>2. El derecho a la protección de datos y la utilización de cámaras <i>on board</i> .....</b>	<b>300</b>
2.1. <i>La licitud del tratamiento de datos personales que implica la utilización de cámaras on board .....</i>	<i>301</i>
2.2. <i>El principio de minimización en el tratamiento de los datos personales captados por las cámaras on board .....</i>	<i>310</i>
2.2.1. <i>Ubicación de las cámaras on board .....</i>	<i>310</i>
2.2.2. <i>Período de grabación de imágenes por las cámaras on board .....</i>	<i>312</i>
2.2.3. <i>Personas que tienen acceso a las imágenes grabadas por las cámaras on board .....</i>	<i>315</i>

	<u>Página</u>
2.3. <i>Los derechos de información, acceso y supresión de las grabaciones de las cámaras on board</i> .....	317
<b>3. Otros derechos fundamentales que pueden verse afectados por la utilización de las cámaras on board</b> .....	321
<b>4. La utilización como prueba en un proceso penal de las imágenes grabadas por las cámaras on board</b> .....	332
4.1. <i>La validez probatoria de las grabaciones videográficas legítimamente obtenidas</i> .....	333
4.2. <i>La (también) validez probatoria de las grabaciones videográficas ilegítimamente obtenidas</i> .....	337
4.2.1. La conexión de antijuricidad .....	341
4.2.2. La violación de derechos fundamentales por particulares y la flexibilización de la regla de exclusión .	346
4.2.3. La prueba ilícita y las grabaciones de las cámaras on board .....	357
4.2.4. La obligación de entregar a la policía las grabaciones efectuadas por las cámaras on board .....	359
4.3. <i>El valor probatorio de las imágenes captadas por las cámaras on board</i> .....	363
4.3.1. La inmediatez, autenticidad e integridad de las imágenes aportadas .....	363
4.3.2. La reproducción de las imágenes en el juicio oral ..	369
<b>5. Bibliografía</b> .....	370

## INTELIGENCIA ARTIFICIAL EN FAVOR DE LA LEY: LA IA COMO FUENTE Y COMO OBJETO DE PRUEBA PERICIAL

ELOY VELASCO NÚÑEZ .....	375
<b>1. Algunas consideraciones acerca del contenido conceptual de la inteligencia artificial y su enfoque regulatorio</b> .....	375
<b>2. La IA asistencial como prueba pericial, como herramienta/aplicación práctica útil en la justicia, y especialmente en la jurisdicción penal</b> .....	381
<b>3. La IA como objeto de prueba</b> .....	386
<b>4. La IA como medio de prueba</b> .....	389

## **LA INFORMACIÓN CONFIDENCIAL EN EL PROCESO PENAL: CUESTIONES EN MATERIA DE SECRETO PROFESIONAL A LA LUZ DE LA LEY ORGÁNICA DEL DERECHO DE DEFENSA**

RAFAEL CASTILLO FELIPE .....	395
<b>1. Introducción .....</b>	<b>396</b>
<b>2. El secreto profesional como instrumento de salvaguarda de derechos fundamentales .....</b>	<b>397</b>
<b>3. El secreto profesional cuando el cliente es parte en el proceso penal .....</b>	<b>402</b>
3.1. <i>Ámbito del secreto profesional tras la LODD .....</i>	402
3.2. <i>La renuncia al secreto para introducir la información protegida mediante pruebas de descargo .....</i>	405
3.3. <i>Renuncia al secreto por parte del cliente que ocupa la posición de acusador .....</i>	409
3.4. <i>Renuncia al secreto y eventual afectación del derecho de defensa de los directivos de la persona jurídica .....</i>	410
<b>4. El secreto profesional cuando el cliente es un tercero en el proceso penal .....</b>	<b>412</b>
4.1. <i>El objeto de protección del secreto en el caso del tercero son los derechos fundamentales relacionados con la vida privada del cliente .....</i>	412
4.2. <i>Protección del secreto profesional que afecta a terceros: registro de despachos en la LODD y la ausencia de previsiones sobre los registros de equipos informáticos .....</i>	413
4.3. <i>Defensa del secreto profesional por sus titulares en un proceso penal en el que son terceros .....</i>	415
<b>5. Aportación de comunicaciones entre letrados .....</b>	<b>418</b>
<b>6. Otras cuestiones insuficientemente resueltas por la LODD ...</b>	<b>422</b>
<b>7. Bibliografía .....</b>	<b>423</b>

## **JUSTICIA Y BLOCKCHAIN: LA NUEVA FRONTERA EN LA CUSTODIA DE EVIDENCIAS DIGITALES**

ALBA LANCHARRO CASTELLANOS .....	427
<b>1. Introducción .....</b>	<b>428</b>



	<i>Página</i>
<b>2. La tecnología Blockchain</b> .....	429
2.1. Componentes .....	431
2.2. Fundamentos .....	434
<b>3. Integración de Blockchain con otras tecnologías</b> .....	437
3.1. Contratos inteligentes (smart contracts) .....	437
3.2. Internet de las cosas .....	439
<b>4. Hacia una cadena de custodia digital con Blockchain</b> .....	440
4.1. Fases del proceso de la cadena de custodia .....	442
4.1.1. Identificación .....	442
4.1.2. Adquisición .....	443
4.1.3. Preservación .....	444
4.1.4. Análisis .....	445
4.1.5. Presentación .....	445
4.2. Criterios en el marco de preservación de evidencias .....	447
4.2.1. Criterios generales .....	447
4.2.2. Criterios específicos .....	449
4.3. Formulario de la cadena de custodia forense-digital .....	451
<b>5. Desafíos en la implementación de la cadena de bloques en investigaciones penales</b> .....	453
<b>6. Ventajas del uso de Blockchain para evidencias digitales</b> .....	456
<b>7. Conclusiones</b> .....	459
<b>8. Bibliografía</b> .....	460

### TERCERA PARTE

#### DERECHO PENAL Y TRATAMIENTO DE LA INFORMACIÓN

#### LA COMUNICACIÓN O REVELACIÓN PÚBLICA DE INFORMACIÓN OBTENIDA EN EL MARCO DE CONTEXTOS LABORALES: ANÁLISIS DE LA RESPONSABILIDAD PENAL DEL ALERTADOR

NATALIA PÉREZ RIVAS .....	471
<b>1. Introducción</b> .....	472

<b>2. La responsabilidad penal del alertador por comunicar o revelar públicamente información</b>	<b>475</b>
2.1. <i>La comunicación o revelación pública de información: condiciones para la protección del alertador</i>	475
2.1.1. Requisito objetivo	476
2.1.2. Requisito intelectual	479
2.1.3. Requisito procedimental	481
2.2. <i>La protección penal del alertador por comunicar o revelar información: el diferente tratamiento del legislador europeo y del legislador español</i>	485
2.3. <i>Mapa de riesgos penales del informante: delimitación de los posibles supuestos de responsabilidad</i>	489
2.3.1. La protección penal del secreto	489
2.3.1.1. Los delitos de descubrimiento y revelación de secretos	489
2.3.1.2. El delito de revelación de secretos de empresa	491
2.3.1.3. El delito de revelación de secretos por autoridad o funcionario público	493
2.3.2. La protección penal del honor	496
2.3.2.1. El delito de calumnias	496
<b>3. Causas de exclusión de responsabilidad penal del alertador en casos de comunicación o revelación pública de información</b>	<b>497</b>
3.1. <i>El efecto directo de las Directivas y el principio de primacía del Derecho de la Unión Europea</i>	497
3.2. <i>El deber de denunciar como causa de justificación o atenuación de la responsabilidad penal</i>	498
3.3. <i>Límites jurídico-penales a la protección del secreto: exclusión en casos de ilicitud</i>	500
3.4. <i>La revelación pública de infracciones a los medios de comunicación como manifestación legítima de la libertad de información</i>	503
3.4.1. La revelación pública y la libertad de información del trabajador según la doctrina del Tribunal Europeo de Derechos Humanos: el caso Halet v. Luxemburgo	505

	<i><u>Página</u></i>
3.4.1.1. La existencia de canales alternativos a la divulgación pública para comunicar los hechos .....	506
3.4.1.2. El interés público de los hechos divulgados ..	507
3.4.1.3. La autenticidad de la información divulgada .....	507
3.4.1.4. La concurrencia de buena fe en el informante .....	508
3.4.1.5. La ponderación entre el perjuicio causado y el interés público de la información divulgada .....	509
3.4.1.6. La gravedad de la sanción impuesta al informante .....	510
3.4.2. La prevalencia del derecho a la libertad de información del informante: doctrina constitucional .....	511
<b>4. A modo de conclusión: propuestas de <i>lege lata</i> y de <i>lege ferenda</i> ..</b>	<b>516</b>
<b>5. Bibliografía .....</b>	<b>518</b>

## **LA PRIVATIZACIÓN DE LA SEGURIDAD EN LA NUEVA ERA DIGITAL**

FRANCISCO SALVADOR GIL GARCÍA .....	523
<b>1. La sociedad de control en la era digital .....</b>	<b>523</b>
<b>2. De la era post-industrial a la modernidad .....</b>	<b>525</b>
<b>3. Conservación de datos en la Unión Europea .....</b>	<b>549</b>
<b>4. Transferencia y puesta a disposición de datos personales .....</b>	<b>553</b>
<b>5. Conclusión .....</b>	<b>560</b>

## **INFORMACIÓN FINANCIERA, DATOS PERSONALES Y BLANQUEO DE CAPITAL**

CLARA COLOMER LÓPEZ .....	563
<b>1. Planteamiento de la cuestión .....</b>	<b>563</b>
<b>2. Delimitación del blanqueo .....</b>	<b>566</b>
<b>3. Impacto social y económico del blanqueo .....</b>	<b>570</b>

<b>4. Fases del blanqueo de capitales y acceso a la información financiera</b>	572
<b>5. La tecnología y los nuevos métodos para el blanqueo de capitales</b>	576
<b>6. La dimensión internacional del blanqueo de capitales</b>	579
6.1. <i>Grupo de Acción Financiera Internacional (GAFI) y sus recomendaciones</i>	580
6.2. <i>Otra normativa relevante a nivel internacional</i>	582
<b>7. La dimensión europea del blanqueo</b>	584
7.1. <i>Los artículos 83 y 114 del Tratado de Funcionamiento de la Unión Europea</i>	584
7.2. <i>Las directivas relativas al blanqueo de capitales</i>	586
<b>8. El blanqueo de capitales en el Código Penal</b>	590
8.1. <i>El bien jurídico protegido en el blanqueo</i>	591
8.2. <i>La actividad delictiva previa o determinante</i>	592
8.3. <i>La conducta típica</i>	595
8.4. <i>El objeto material del delito de blanqueo</i>	600
<b>9. Acceso a la información financiera y protección de datos personales en la investigación del blanqueo de capitales</b>	601
<b>10. Conclusiones</b>	605

## CUARTA PARTE

### INFORMACIÓN Y DATOS EN PROCESOS NO PENALES

#### INFORMACIÓN, DATOS Y PERICIAL ALGORÍTMICA EN LOS PROCESOS

IGNACIO COLOMER HERNÁNDEZ	611
<b>1. Delimitación de la cuestión a analizar</b>	611
<b>2. La pericial algorítmica</b>	613
<b>3. Pericial algorítmica, transparencia y valoración de la prueba</b>	617
<b>4. A modo de conclusión</b>	633

## LA NECESIDAD DE DISEÑAR UN PROCESO ORIENTADO AL DATO

VICENTE PÉREZ DAUDÍ .....	635
<b>1. Introducción .....</b>	<b>635</b>
<b>2. La aplicación de los principios del proceso a la ciberjusticia ..</b>	<b>637</b>
2.1. <i>El principio de dualidad de posiciones .....</i>	<i>638</i>
2.2. <i>El principio de audiencia .....</i>	<i>640</i>
2.3. <i>El principio de igualdad .....</i>	<i>641</i>
<b>3. La incidencia de las TICs en la tramitación del proceso declarativo .....</b>	<b>643</b>
3.1. <i>La adopción de decisiones no jurisdiccionales automatizadas ...</i>	<i>643</i>
3.2. <i>Obstáculos estructurales y déficit de integración digital .....</i>	<i>645</i>
3.3. <i>Los actos procesales de parte y el proceso digital. Hacia una integración garantista .....</i>	<i>646</i>
3.4. <i>Comparecencia electrónica, representación y notificaciones ....</i>	<i>647</i>
3.4.1. <i>La articulación digital de las alegaciones. El uso de formularios normalizados. ....</i>	<i>647</i>
3.4.2. <i>El diseño estructurado de las alegaciones en formato digital .....</i>	<i>649</i>
3.4.3. <i>Configuración normativa de los formularios .....</i>	<i>650</i>
3.4.4. <i>La subsanación de los defectos en los formularios .</i>	<i>651</i>
3.4.5. <i>Los actos orales y el formato virtual .....</i>	<i>652</i>
<b>4. A modo de conclusión: la necesidad de diseñar un proceso judicial en formato digital .....</b>	<b>653</b>
<b>5. Bibliografía .....</b>	<b>655</b>

## LA PROBLEMÁTICA DE LA INFORMACIÓN Y DE LOS DOCUMENTOS DECLARADOS CONFIDENCIALES EN EL ÁMBITO DE LA CONTRATACIÓN ADMINISTRATIVA

ALBERTO PALOMAR OLMEDA .....	657
<b>1. Planteamiento inicial .....</b>	<b>657</b>
<b>2. La regulación .....</b>	<b>659</b>
2.1. <i>En el ámbito del derecho comunitario .....</i>	<i>659</i>

	<i>Página</i>
2.2. <i>En el ámbito nacional</i> .....	661
<b>3. Algunos elementos en la interpretación: en concreto, el concepto de secretos comerciales</b> .....	<b>669</b>
3.1. <i>Doctrina general</i> .....	669
3.2. <i>Algunas pautas aplicativas en el ámbito específico de la LCSP</i> ..	673
<b>4. El planteamiento de la jurisprudencia comunitaria</b> .....	<b>675</b>
<b>5. Algunas incógnitas por resolver</b> .....	<b>677</b>

## **INFRACCIONES MASIVAS DE DATOS PERSONALES: HACIA UN SISTEMA DE PRIVATE ENFORCEMENT EFICAZ**

MARÍA JESÚS SANDE MAYO .....	679
<b>1. Introducción</b> .....	<b>680</b>
<b>2. Las acciones de representación «en defensa de los intereses colectivos de los consumidores»</b> .....	<b>684</b>
2.1. <i>La tipología de representación en defensa de los intereses colectivos de los consumidores que alberga la DAR</i> .....	684
2.1.1. Las acciones de representación de cesación .....	687
2.1.2. Las acciones de representación resarcitorias .....	689
2.2. <i>Ámbito de aplicación de las acciones colectivas</i> .....	692
2.2.1. El concepto de consumidor: una noción compleja y en constante construcción .....	692
2.3. <i>Los aspectos más críticos de la transposición al ordenamiento español de la directiva</i> .....	698
2.3.1. El régimen de legitimación .....	699
2.3.2. La vinculación de los consumidores a la acción colectiva .....	703
2.3.2. La financiación .....	706
<b>3. Relación de las acciones de representación de la DAR con las acciones de representación reguladas en el artículo 80 RGPD</b> ..	<b>709</b>
3.1. <i>El alcance del artículo 80.1 RGPD</i> .....	710
3.2. <i>El alcance del artículo 80.2 RGPD</i> .....	713
<b>4. La competencia judicial internacional</b> .....	<b>715</b>

	<i>Página</i>
4.1. <i>La aplicación de los fueros del RBI bis</i> .....	718
4.2. <i>La aplicabilidad del foro especial regulado en el artículo 79.2 RGPD</i> .....	721
<b>5. Conclusiones</b> .....	722
<b>6. Bibliografía</b> .....	723

## **LA INFLUENCIA DE LA EMPRESA COMÚN EUROPEA DE ALTO RENDIMIENTO (EUROHPC) EN EL TRATAMIENTO DE LA INFORMACIÓN PARA LOS PROCESOS DE IA**

ANTONIO VASCO GÓMEZ .....	727
<b>1. Introducción</b> .....	727
<b>2. Competencias de la EuroHPC</b> .....	730
<b>3. Regulación en el reglamento IA</b> .....	734
<b>4. El Reglamento 2024/1732</b> .....	737
<b>5. La EuroHPC y el tratamiento de información en los procesos</b> ..	743
<b>6. Conclusiones</b> .....	755
<b>7. Bibliografía</b> .....	756

## **EL ARQUITECTO Y LOS ALGORITMOS. CUESTIONES JURÍDICAS RELATIVAS A LA RESPONSABILIDAD CIVIL EN EL PROCESO DE EDIFICACIÓN**

LUCÍA AGUADO PEÑAS .....	759
<b>1. Introducción</b> .....	759
<b>2. Breve referencia a la conceptualización de la IA en base al Reglamento de la Unión Europea y demás contextos normativos</b> ....	763
<b>3. La responsabilidad por el uso de la IA</b> .....	769
3.1. <i>Naturaleza de la responsabilidad de la IA</i> .....	772
3.2. <i>Tipos de responsabilidad civil</i> .....	773
3.2.1. Responsabilidad civil del productor .....	773
3.2.2. Responsabilidad del desarrollador del <i>software</i> ....	775
3.2.3. Responsabilidad civil del operador .....	777
<b>4. El factor del riesgo en el uso de sistemas de IA</b> .....	778
<b>5. Clases de defectos</b> .....	780

	<u>Página</u>
<b>6. Relación de causalidad y la carga de la prueba</b> .....	784
6.1. <i>La carga de la prueba</i> .....	786
<b>7. Plazo de garantía y de prescripción</b> .....	789
<b>8. En cuanto a los seguros de responsabilidad civil</b> .....	789
<b>9. Conclusiones</b> .....	793
<b>10. Bibliografía</b> .....	795