

# PRACTICUM

---

## PROTECCIÓN DE DATOS 2018



THOMSON REUTERS

## Sobre el autor

### **Javier Álvarez Hernando**

Licenciado en Derecho por la Universidad de Valladolid. Posteriormente cursó Máster en Derecho de las tecnologías de la información y las comunicaciones en la Universidad Pontificia de Comillas-ICADE en Madrid, en el año 2001, y es diplomado por la Escuela de Práctica Jurídica de Valladolid en el 2007. Junto a su desempeño profesional como abogado, posee amplia experiencia en acciones formativas tanto para empresas como para la Administración Pública. Es autor de más de 100 artículos en revistas de naturaleza jurídica, y cuenta entre sus publicaciones con la monografía «*Guía práctica sobre Protección de datos. Cuestiones y formularios 2011*», Lex Nova; es coautor de la obra «*Comunicación digital eficaz y Legal. Claves jurídicas y de marketing para la empresa del Siglo XXI*» 2012. Thomson Reuters; e igualmente es coautor de la obra «*Practicum Administración de Fincas*» 2014, 2015 y 2016. Thomson Reuters.

Forma parte del equipo de profesores de la Escuela de Administración Pública de Castilla y León (ECLAP) desde 2007 e imparte docencia en el Grado de Derecho en la Universidad Isabel I de Castilla, así como en el Máster de Acceso a la Abogacía de la Universidad de Valladolid. Ha obtenido en los años 2011 y 2013 el primer premio en la I y III Edición del Premio de Artículos Jurídicos de la Agrupación de Abogados Jóvenes de Valladolid organizado por el Ilre. Colegio de Abogados de Valladolid/Fundación Camilo de la Red; e igualmente fue ganador en 2012 de la IV Edición de los Premios Buscando El Norte Digital, en la categoría Mejor Iniciativa Digital, organizado por El Norte de Castilla.

# Sumario

	<u>Página</u>
<b>Abreviaturas</b> .....	41
<b>TEMA 1</b>	
<b>Introducción a la protección de datos personales</b> .....	47
1. Evolución histórica del derecho a la protección de datos .....	48
1.1. <i>Primeros instrumentos normativos</i> .....	48
1.2. <i>El Convenio 108</i> .....	49
1.3. <i>La LORTAD</i> .....	49
1.4. <i>Directiva 95/46/CE</i> .....	50
1.5. <i>La LOPD y su Reglamento</i> .....	50
1.6. <i>Carta de Niza</i> .....	51
1.7. <i>Tratado de Lisboa</i> .....	52
1.8. <i>Reglamento Europeo de Protección de Datos (REPD)</i> .....	52
1.8.1. <i>Publicación y entrada en vigor</i> .....	52
1.8.2. <i>El porqué de una nueva regulación europea</i> .....	53
1.8.3. <i>Novedades del Reglamento europeo</i> .....	54
3. Conceptos y definiciones esenciales en protección de datos .....	58
3.1. <b>Dato personal</b> .....	58
3.2. <i>Dato relacionado con la salud</i> .....	60
3.3. <i>Teléfono y dirección como datos personales</i> .....	60
3.4. <i>La matrícula de vehículos es un dato personal</i> .....	61
3.5. <i>El documento nacional de identidad es un dato de carácter personal</i> .....	62
3.6. <i>La dirección IP es un dato de carácter personal</i> .....	63
3.7. <i>Correo electrónico como dato personal</i> .....	66
3.8. <i>El número de inscripción registral de una finca como dato personal</i> .....	66
3.9. <i>Datos disociados. La anonimización de datos personales</i> .....	67
3.10. <i>Seudonimización</i> .....	67
3.11. <i>Tratamiento de datos personales</i> .....	69
3.12. <i>Fichero como conjunto organizado de datos personales. Ficheros públicos y privados</i> .....	69
3.13. <i>Responsable del fichero y responsable del tratamiento. El titular del fichero</i> .....	71
3.14. <i>Encargado del tratamiento</i> .....	72
3.15. <i>Fuentes accesibles al público</i> .....	72
3.16. <i>Afectado o interesado</i> .....	73
4. Objeto y ámbito de aplicación objetivo de la normativa sobre protección de datos ....	74

	<u>Página</u>
4.1. Objeto y ámbito de aplicación .....	74
4.2. Ficheros excluidos de la aplicación de la LOPD: domésticos, sobre materias clasificadas, terrorismo y delincuencia organizada .....	75
4.3. Tratamientos excluidos del ámbito objetivo de aplicación en el Reglamento Europeo de Protección de Datos .....	76
4.4. Datos de personas jurídicas .....	79
4.5. Datos de contactos de personas jurídicas .....	81
4.6. Empresarios individuales o autónomos .....	82
4.7. Datos de personas fallecidas .....	83
4.8. Ficheros que se rigen por una normativa específica, según establece la LOPD .....	86
5. Ámbito de aplicación territorial .....	87
5.1. Ámbito territorial de aplicación de la Directiva 95/46/CE y en la LOPD .....	87
5.2. Ámbito territorial del Reglamento Europeo de Protección de Datos y definiciones relevantes para el ámbito de aplicación .....	89
5.2.1. Ámbito territorial en el REPD .....	89
5.2.2. Definiciones relevantes en el ámbito de aplicación del Reglamento Europeo de Protección de Datos .....	90

## TEMA 2

<b>Legitimación para el tratamiento: Principios en protección de datos. Régimen jurídico del responsable y el encargado del tratamiento .....</b>	<b>93</b>
1. Bases de legitimación para el tratamiento de datos personales .....	93
2. Principios de protección de datos en la LOPD .....	94
2.1. El consentimiento del afectado en la LOPD y en la Directiva 95/46/CE .....	94
2.1.1. El consentimiento como principio esencial en protección de datos .....	94
2.1.2. Requisitos del consentimiento en la LOPD .....	95
2.1.3. Excepciones a la necesidad de consentimiento para el tratamiento de datos personales .....	98
2.1.4. El consentimiento tácito en el RLOPD .....	102
2.1.5. La prueba del consentimiento .....	103
2.1.6. La revocación del consentimiento prestado .....	105
2.1.7. El consentimiento en los datos especialmente protegidos .....	106
2.1.8. Solicitud del consentimiento para finalidades distintas .....	108
2.1.9. El consentimiento de los menores de edad .....	109
2.1.10. El consentimiento y la transparencia .....	111
2.1.11. Consentimiento del interesado para la publicación de una fotografía suya en una red social: intromisión en el derecho a la propia imagen .....	112
2.1.12. El consentimiento verbal en la contratación de servicios de telecomunicaciones .....	114
2.1.13. Consentimiento y contratación fraudulenta de productos y servicios .....	116
2.2. El interés legítimo como base jurídica para el tratamiento de datos con la Directiva 95/46/CE y la LOPD .....	116
2.3. El principio de calidad de los datos en la LOPD .....	118
2.3.1. Alcance y origen del principio de calidad de los datos .....	118
2.3.2. Finalidades determinadas, explícitas, legítimas y compatibles con aquellas para las que los datos hubieran sido recogidos (principio de finalidad) .....	119
2.3.3. Datos adecuados, pertinentes y no excesivos .....	120

	<u>Página</u>
2.3.4. Adecuación del tratamiento de los datos a la finalidad autorizada («finalidad compatible») .....	123
2.3.5. Exactitud de los datos (veracidad) y puesta al día de los mismos .....	126
2.3.6. La cancelación de los datos .....	130
2.3.7. Conservación y mantenimiento de los datos .....	131
2.3.8. Almacenamiento de la información; la organización del tratamiento ..	135
2.3.9. El principio de calidad en la recogida de datos personales .....	135
2.4. <i>El principio de información en la LOPD</i> .....	136
2.4.1. El principio de información como un derecho del interesado y un deber del responsable del tratamiento .....	136
2.4.2. Contenido del deber de información. Requisitos de «calidad de la información» .....	139
2.4.3. El deber de información como obligación de hacer del responsable del tratamiento .....	139
2.4.4. Exención al deber de informar .....	141
2.4.5. Procedimiento de exención del deber de informar .....	141
2.4.6. Modos de practicar el deber de información con la LOPD .....	143
2.4.7. El deber de información en el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras .....	144
2.4.8. Información a través de una página web cuando se recogen los datos por vía telefónica .....	144
2.4.9. Cumplimiento del deber de información de manera posterior a la recogida de datos .....	145
2.4.10. Excepciones a la obligación de informar al interesado .....	146
2.5. <i>Cesiones o comunicaciones de datos en la LOPD</i> .....	147
2.5.1. Alcance de la cesión o comunicación de datos personales .....	147
2.5.2. Características de la cesión de datos .....	149
2.5.3. Excepciones a la necesidad de consentimiento para ceder datos a terceros .....	150
2.5.4. Cesión de datos especialmente protegidos .....	152
2.5.5. Cesión de datos y grupos de empresas .....	154
2.5.6. Cesiones de datos a entidades financieras .....	156
2.5.7. Cesión de datos de asociados a una federación .....	156
3. Principios de protección de datos en el reglamento europeo .....	157
3.1. <i>Principios relativos al tratamiento de datos y su similitud con el principio de calidad de los datos. Licitud del tratamiento</i> .....	157
3.1.1. Principios relativos al tratamiento .....	157
3.1.2. Licitud del tratamiento .....	159
3.1.3. Tratamiento de categorías especiales de datos personales .....	160
3.1.4. Tratamiento de datos personales relativos a condenas e infracciones penales .....	164
3.1.5. Tratamientos de datos que no requiere identificación .....	164
3.2. <i>El consentimiento del afectado en el Reglamento Europeo de Protección de Datos</i> .....	165
3.2.1. Definición de consentimiento en el REPD y condiciones que legitiman el tratamiento. El consentimiento tácito .....	165
3.2.2. Validez del consentimiento obtenido antes de la entrada en vigor del Reglamento Europeo de Protección de Datos .....	167
3.2.3. Tratamiento de datos y consentimiento de menores de edad .....	168

	<u>Página</u>
3.2.4. Consentimiento para el tratamiento de categorías especiales de datos personales .....	169
3.2.5. Recogida del consentimiento para varias finalidades de tratamiento .	170
3.2.6. El REPD descarta la validez del consentimiento tácito .....	170
3.3. <i>Legitimación basada en el interés legítimo en el Reglamento Europeo de Protección de Datos</i> .....	171
3.4. <i>El principio de información en el Reglamento Europeo de Protección de Datos</i> .....	172
3.4.1. Comparativa entre la LOPD y el REPD .....	172
3.4.2. Excepciones a la necesidad de informar al interesado .....	174
3.4.3. Procedimientos de recogida de datos y forma de informar al interesado .....	175
3.4.4. Información proporcionada por capas o niveles .....	176
4. Acceso a datos por cuenta de terceros. El encargado del tratamiento y su régimen jurídico .....	185
4.1. <i>El responsable del fichero y el encargado del tratamiento en la Directiva 95/46/CE y en la LOPD</i> .....	185
4.1.1. Concepto y aproximación normativa .....	185
4.1.2. Consideración de la existencia de una cesión de datos y no de un acceso a datos por cuenta de terceros .....	186
4.1.3. El contrato de acceso a datos por cuenta de terceros .....	188
4.1.4. Modelo de contrato de acceso a datos por cuenta de terceros en el marco de una prestación de servicios de mantenimiento técnico informático válido hasta la entrada en vigor del Reglamento Europeo de Protección de Datos, en mayo de 2018 .....	191
4.1.5. Implicaciones del responsable y del encargado del tratamiento a lo largo del desarrollo de la prestación de los servicios que implican un acceso a los datos .....	195
4.1.6. Supuestos específicos de acceso a datos por cuenta de terceros .....	200
4.2. <i>La relación entre el responsable y el encargado del tratamiento en el Reglamento Europeo de Protección de Datos</i> .....	203
4.2.1. Conceptos .....	203
4.2.2. Elección y supervisión del encargado del tratamiento. Principio de responsabilidad activa .....	203
4.2.3. Aplicación del Reglamento Europeo a los encargados de tratamiento dentro y fuera de la Unión Europea .....	206
4.2.4. Subcontratación .....	207
4.2.5. El contrato de encargo y su contenido .....	207
4.2.6. Modelo de contrato entre un responsable y un encargado del tratamiento adaptado al Reglamento Europeo de Protección de Datos .....	213

## TEMA 3

<b>Obligaciones formales. Inscripción, modificación y supresión de ficheros en el Registro General de Protección de Datos</b> .....	221
1. Obligaciones formales. Aproximación normativa y obligación a extinguir con la entrada en vigor del Reglamento Europeo de Protección de Datos .....	221
2. Requisitos para la inscripción de ficheros y los sistemas de control .....	225
3. Agrupación de ficheros para la inscripción .....	226
4. Procedimiento de inscripción, modificación o supresión de ficheros de la AEPD .....	227
5. Creación, modificación y supresión de ficheros de titularidad pública .....	229

	<u>Página</u>
6. Forma de realizar las notificaciones de inscripción, modificación y supresión de ficheros: Formulario NOTA .....	230
7. Operativa de cumplimentación del formulario NOTA .....	233
7.1. Cuestiones iniciales .....	233
7.2. Responsable del fichero y encargado del tratamiento .....	235
7.3. Identificación y finalidad del fichero .....	237
7.4. Origen y procedencia de los datos .....	238
7.5. Tipos de datos, estructura y organización del fichero .....	239
7.6. Medidas de seguridad .....	241
7.7. Comunicaciones o cesiones de datos .....	241
7.8. Transferencias internacionales de datos (TID) .....	242
8. Modificación de la inscripción del fichero previamente inscrito en el RGPD .....	243
9. Supresión de los ficheros inscritos en el RGPD .....	244

## TEMA 4

<b>Responsabilidad proactiva o accountability en el Reglamento Europeo de Protección de Datos</b> .....	<b>245</b>
1. Exigencia de responsabilidad activa y demostrable .....	246
1.1. El principio de responsabilidad activa o «accountability»: novedad en el Reglamento Europeo de Protección de Datos .....	246
1.2. Cumplimiento normativo o «compliance» .....	246
1.3. Exigencia de responsabilidad activa y demostrable en el Reglamento Europeo .....	247
2. Medidas de protección de datos desde el diseño .....	249
3. Medidas de protección de datos por defecto .....	251
4. Registro de las actividades de tratamiento de datos .....	251
4.1. Aspectos generales o comunes del Registro de Actividades .....	251
4.2. Registro de actividades del responsable del fichero o tratamiento .....	253
4.3. Registro de actividades del encargado del tratamiento .....	254
5. El delegado de protección de datos .....	255
5.1. Introducción y antecedentes históricos .....	255
5.2. Funciones del delegado de protección de datos .....	257
5.2.1. Función de información y asesoramiento normativo .....	257
5.2.2. Función de supervisión del cumplimiento normativo. Auditoría .....	257
5.2.3. Función de cooperación y enlace con la autoridad de control .....	257
5.2.4. Función de atención a los interesados .....	257
5.3. ¿Cuándo es obligatoria en una organización la existencia de un DPO? .....	258
5.4. Supuestos especiales .....	262
5.5. La figura del delegado de protección de datos .....	262
5.6. Modelo de certificación como Delegado de Protección de Datos .....	268
6. Evaluaciones de impacto .....	269
6.1. Concepto de evaluación de impacto .....	269
6.2. Supuestos tasados en los que se exige una evaluación de impacto .....	271
6.3. Contenido de una evaluación de impacto .....	274
6.4. Solicitud de la opinión del interesado .....	274
6.5. Excepciones a la necesidad de evaluación de impacto previa .....	274
6.6. Códigos de conducta y evaluaciones de impacto .....	275
6.7. Consulta previa a la AEPD .....	275

	<u>Página</u>
6.8. <i>Realización de una Evaluación de Impacto en protección de datos</i> .....	276
6.8.1. <i>Análisis de necesidad. Equipo de trabajo y definición del proyecto</i> ....	276
6.8.2. <i>Descripción del proyecto y de los flujos de información. Detalle de las categorías de datos que se tratan, los usuarios de los mismos, los flujos de información y las tecnologías utilizadas</i> .....	276
6.8.3. <i>Identificación de los riesgos</i> .....	277
6.8.4. <i>Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan y del daño que causarían si se materializaran. Consultas a los afectados</i> .....	280
6.8.5. <i>Gestión de los riesgos identificados</i> .....	281
6.8.6. <i>Análisis de cumplimiento normativo</i> .....	291
6.8.7. <i>Informe final</i> .....	292
6.8.8. <i>Implantación de las recomendaciones</i> .....	293
6.8.9. <i>Revisión y realimentación</i> .....	293
<b>TEMA 5</b>	
<b>Derechos del interesado y su ejercicio en materia de protección de datos personales</b> .....	295
1. <i>Los derechos de acceso, rectificación, cancelación y oposición (ARCO); procedimiento y excepciones a su ejercicio</i> .....	295
1.1. <i>Introducción</i> .....	295
1.2. <i>Poder de disposición y control de los interesados de sus datos personales</i> .....	296
1.3. <i>Los derechos de los interesados no son derechos absolutos</i> .....	297
1.4. <i>Derechos independientes</i> .....	298
1.5. <i>Excepciones generales al ejercicio de derechos ARCO</i> .....	298
1.6. <i>Procedimiento para el ejercicio de los derechos</i> .....	299
1.7. <i>La representación para el ejercicio de los derechos por los interesados</i> .....	302
1.8. <i>El responsable del fichero y encargado del tratamiento ante un ejercicio de derechos</i> ..	303
1.9. <i>Procedimiento y aspectos exigidos en el Reglamento Europeo de Protección de Datos en el ejercicio de derechos del interesado. Limitaciones e infracciones</i> .....	304
1.9.1. <i>Derechos y procedimiento para el ejercicio de derechos en el REPD y en el anteproyecto de reforma de la LOPD</i> .....	304
1.9.2. <i>Limitaciones del alcance de las obligaciones y los derechos de los interesados</i> .....	306
1.9.3. <i>Infracciones en el Reglamento Europeo frente a vulneraciones de los derechos de los interesados</i> .....	307
1.10. <i>Reclamaciones a la AEPD por no atención de los derechos de los interesados</i> .....	308
2. <i>Derechos del interesado: información y acceso; rectificación; cancelación; supresión (olvido); oposición; limitación y portabilidad</i> .....	310
2.1. <i>Derecho a la información y principio de transparencia</i> .....	310
2.2. <i>El derecho de acceso del interesado y su ejercicio</i> .....	314
2.2.1. <i>Derecho de acceso y su regulación en la LOPD y RLOPD</i> .....	314
2.2.2. <i>Derecho de acceso y su regulación en el Reglamento Europeo de Protección de Datos y en el anteproyecto de reforma de la LOPD</i> .....	322
2.3. <i>Derecho a la portabilidad de los datos en el Reglamento Europeo de Protección de Datos y en el anteproyecto de reforma de la LOPD</i> .....	325
2.3.1. <i>Concepto y regulación</i> .....	325
2.3.2. <i>Requisitos y condiciones para el ejercicio del derecho a la portabilidad</i> .....	326



	<u>Página</u>
2.3.3. Elementos de la portabilidad de los datos .....	327
2.3.4. Limitaciones al derecho de portabilidad .....	328
2.3.5. Aplicación de las normas generales al ejercicio de los derechos de los interesados a la portabilidad de los datos .....	329
2.3.6. Derecho a la portabilidad en el anteproyecto de reforma de la LOPD .....	331
2.4. <i>El derecho de rectificación del interesado y su ejercicio</i> .....	332
2.4.1. Derecho de rectificación y su regulación en la LOPD y RLOPD .....	332
2.4.2. Derecho de rectificación en el Reglamento Europeo y en el anteproyecto de reforma de la LOPD .....	334
2.5. <i>El derecho de cancelación, supresión o derecho al olvido, con la LOPD y con el Reglamento Europeo de Protección de Datos</i> .....	335
2.5.1. Derecho de cancelación en la LOPD .....	335
2.5.2. El Derecho al olvido .....	342

## TEMA 6

<b>Seguridad de los datos personales</b> .....	395
1. Obligaciones generales en materia de seguridad de la información .....	397
1.1. <i>Encaje normativo básico. La seguridad en el Reglamento Europeo de Protección de Datos</i> .....	397
1.1.1. Seguridad en la LOPD y en el RLOPD .....	397
1.1.2. Seguridad en el Reglamento Europeo de Protección de Datos .....	398
1.2. <i>Principios de seguridad en la LOPD e interpretación jurisprudencial</i> .....	399
1.3. <i>La seguridad como principio en el Reglamento Europeo de Protección de Datos</i> .....	402
1.4. <i>La seguridad como obligación en el Reglamento Europeo de Protección de Datos (REPD)</i> .....	402
2. Niveles de seguridad .....	404
2.1. <i>Nivel alto. A ficheros o tratamientos con datos (artículo 83.1 RLOPD)</i> .....	405
2.2. <i>Nivel medio. A ficheros o tratamientos con datos</i> .....	406
2.3. <i>Nivel básico</i> .....	408
2.4. <i>Aplicación de medidas de seguridad de distinto nivel a un mismo fichero</i> .....	410
2.5. <i>Derecho de cancelación, bloqueo y medidas de seguridad</i> .....	410
2.6. <i>Cuadro resumen de medidas de seguridad y niveles aplicables, atendiendo al tipo de ficheros o tratamientos</i> .....	411
3. Niveles y medidas de seguridad en ámbitos específicos .....	412
3.1. <i>Nivel de seguridad para tratamientos con datos de menores de edad</i> .....	412
3.2. <i>Medidas de seguridad en una página web que trata datos con fines publicitarios. Redes sociales</i> .....	412
3.3. <i>Medidas de seguridad en medios de comunicación audiovisuales</i> .....	412
3.4. <i>Medidas de seguridad en una asesoría fiscal</i> .....	413
3.5. <i>Quiebras e incidencias de seguridad y su notificación por parte de operadores de comunicaciones; por los prestadores de servicios de confianza de certificados y firma electrónica; y por los operadores de servicios esenciales y proveedores de servicios digitales: La Directiva NIS</i> .....	413
3.5.1. <i>Quiebras de seguridad y su notificación por parte de los operadores de comunicaciones electrónicas</i> .....	413
3.5.2. <i>Notificación de quiebras de seguridad por parte de prestadores de servicios de confianza de certificados y firma electrónica</i> .....	417

	<u>Página</u>
3.5.3. Notificación de incidentes de seguridad, por parte de operadores de servicios esenciales y proveedores de servicios digitales: La Directiva NIS .....	418
3.6. <i>Medidas de seguridad en el «software» de gestión de clientes</i> .....	421
3.7. <i>Declaración de prácticas de certificación y sus implicaciones en materia de seguridad de los datos</i> .....	421
3.8. <i>Medidas de seguridad en el fichero de clientes de hotel que contiene datos de salud</i> ....	422
4. Documento de seguridad y su contenido .....	422
4.1. <i>El documento de seguridad (DS)</i> .....	423
4.2. <i>Actualización del documento de seguridad</i> .....	424
4.3. <i>Documento de seguridad y grupo de empresas</i> .....	425
5. El responsable de seguridad .....	425
6. Las concretas medidas de seguridad exigidas para ficheros automatizados y no automatizados .....	426
6.1. <i>Esquemas de las medidas de seguridad de obligatoria implantación tanto para ficheros automatizados como no automatizados o en soporte papel</i> .....	426
6.2. <i>Delegación de la gestión de la seguridad</i> .....	431
6.3. <i>Funciones y obligaciones del personal en seguridad de la información</i> .....	432
6.4. <i>Deber de secreto y su alcance</i> .....	435
6.4.1. <i>Introducción</i> .....	435
6.4.2. <i>Deber de secreto en la LOPD</i> .....	436
6.4.3. <i>Acceso a datos por cuenta de terceros y prestaciones de servicios sin que impliquen acceso a datos</i> .....	436
6.4.4. <i>Deber de secreto en determinadas profesiones reguladas</i> .....	436
6.4.5. <i>Deber de secreto en el Reglamento Europeo de Protección de Datos (REPD) y en el anteproyecto de reforma de la LOPD</i> .....	437
6.4.6. <i>Directiva de protección de secretos comerciales</i> .....	439
6.4.7. <i>Compromiso de confidencialidad</i> .....	440
6.4.8. <i>Interpretación de deber de secreto en la jurisprudencia y en las Resoluciones de la AEPD</i> .....	440
6.5. <i>Incumplimientos del personal de las medidas de seguridad</i> .....	442
6.6. <i>Medidas de seguridad por parte del prestador de un servicio con acceso a datos personales</i> .....	442
6.7. <i>Medidas de seguridad por parte de un prestador de un servicio de seguridad o de limpieza, que no tiene acceso a datos personales</i> .....	444
6.8. <i>Medidas de seguridad en redes de comunicaciones</i> .....	445
6.9. <i>Seguridad cuando se trabaja fuera de los locales del responsable o se almacenan datos en dispositivos portátiles</i> .....	446
6.10. <i>Medidas de seguridad en ficheros temporales o copias de documentos</i> .....	446
6.11. <i>Identificación y autenticación. Cambio de contraseñas de acceso</i> .....	447
6.12. <i>Control de acceso a los ficheros automatizados</i> .....	449
6.12.1. <i>Control de acceso para el nivel básico de seguridad</i> .....	450
6.12.2. <i>Registro de acceso para el nivel alto de seguridad</i> .....	450
6.12.3. <i>Control de acceso físico</i> .....	452
6.13. <i>Gestión de soportes para un nivel básico de seguridad</i> .....	453
6.14. <i>Registro de entrada y salida de soportes</i> .....	456
6.15. <i>Gestión y distribución de soportes para un nivel alto de seguridad</i> .....	456
6.16. <i>Copias de seguridad o backups</i> .....	457

	<u>Página</u>
6.17. <i>Incidencias en materia de seguridad de la información</i> .....	458
6.18. <i>Registro de incidencias</i> .....	459
6.19. <i>Medidas de seguridad específicas para ficheros en soporte papel</i> .....	462
6.19.1. <i>Criterio de archivo de ficheros manuales</i> .....	462
6.19.2. <i>Dispositivos de almacenamiento</i> .....	462
6.19.3. <i>Custodia de los soportes</i> .....	463
6.19.4. <i>Almacenamiento de la información</i> .....	463
6.19.5. <i>Copias y destrucción de documentos</i> .....	463
6.19.6. <i>Acceso a la documentación por parte del personal autorizado</i> .....	464
6.19.7. <i>Protocolo para el traslado de documentos</i> .....	464
7. <i>Auditoría de seguridad</i> .....	464
7.1. <i>Exigencia de auditoría bienal para niveles medios y altos de seguridad</i> .....	464
7.2. <i>Figura del auditor de seguridad</i> .....	466
7.3. <i>Informe de auditoría y su contenido</i> .....	466
7.4. <i>Listado de comprobación o checklist, para las auditorías de seguridad o para la verificación de cumplimiento normativo</i> .....	467
7.5. <i>¿Qué debe hacer la empresa u organización una vez que disponga de un informe de auditoría de seguridad?</i> .....	475
8. <i>Medidas de seguridad en la evaluación de impacto en materia de protección de datos (EIPD)</i> .....	477
8.1. <i>¿Qué es una evaluación de impacto y cuál es su encaje normativo?</i> .....	477
8.2. <i>Guía de la AEPD para una evaluación del impacto en la protección de datos personales</i> .....	478
9. <i>Notificación de violaciones de seguridad de los datos personales a la autoridad de control y a los afectados, según el Reglamento Europeo de Protección de Datos</i> .....	480
9.1. <i>Distinta obligación de comunicación que la exigida a los proveedores de servicios de comunicaciones electrónicas</i> .....	480
9.2. <i>Obligación de notificación de una violación de seguridad de los datos a la autoridad de control</i> .....	480
9.3. <i>Obligación de notificación de una violación de seguridad de los datos al interesado</i> ...	482
10. <i>Protocolo de seguridad adaptado al Reglamento Europeo de Protección de Datos</i> ...	530
10.1. <i>Objeto</i> .....	531
10.2. <i>Ámbito de aplicación de las medidas de seguridad</i> .....	533
10.3. <i>Registro de las actividades de tratamiento en la organización</i> .....	534
10.4. <i>Seguridad de la información en la Evaluación de Impacto en la Protección de Datos Personales</i> .....	535
10.5. <i>Códigos de conducta en materia de protección de datos</i> .....	537
10.6. <i>Mecanismos de certificación en materia de protección de datos</i> .....	537
10.7. <i>Medidas de seguridad técnicas y organizativas adecuadas al riesgo para los datos objeto de tratamiento en la organización</i> .....	537
10.7.1. <i>Seudonimización</i> .....	537
10.7.2. <i>Cifrado de datos personales</i> .....	538
10.7.3. <i>Medidas de seguridad que garantizan la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento en la entidad</i> .....	538

**TEMA 7**

<b>Transferencias internacionales de datos</b> .....	551
1. Los movimientos internacionales de datos y su marco regulador .....	552
1.1. Régimen normativo de las transferencias internacionales de datos .....	552
1.2. Decisiones de la Comisión Europea .....	555
1.3. Figuras que operan en una transferencia internacional de datos: el exportador y el importador de datos .....	555
1.4. Estándares internacionales de privacidad .....	556
2. Cuando se considera que se produce una transferencia internacional de datos (TID) .....	557
3. Requisitos para realizar una transferencia internacional de datos .....	558
4. Excepciones a la norma general para las transferencias internacionales de datos .....	561
5. Estados con nivel adecuado de protección .....	564
5.1. Los Estados miembros de la Unión Europea, además de Islandia, Liechtenstein y Noruega (que conforman el Espacio Económico Europeo) .....	564
5.2. Estados que la Comisión Europea ha declarado que garantizan un nivel de protección adecuado .....	564
5.3. Canadá, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos .....	565
5.4. Entidades estadounidenses certificadas en el marco del Escudo de Privacidad UE-EE.UU. La norma habilitante es la Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016 .....	565
5.4.1. Antecedentes de la TID a Estados Unidos: el Acuerdo de Puerto Seguro o Safe Harbour .....	565
5.4.2. Escudo de la privacidad UE-EE. UU .....	566
5.5. Australia, Canadá y Estados Unidos de América, respecto a los datos personales (Passenger Name Records –PNR–) incluidos en los registros de nombres de los pasajeros que se transfieren al servicio de aduanas de estos países .....	573
5.6. Los Estados Unidos de América respecto al tratamiento y la transferencia de datos de mensajería financiera de la UE a los EE.UU. a efectos del Programa de Seguimiento de la Financiación del Terrorismo (Decisión del Consejo 2010/412/UE, de 13 de julio de 2010). Acuerdos SWIFT .....	578
5.7. Los Estados Unidos respecto a los datos a efectos policiales y judiciales en materia penal .....	579
6. Suspensión temporal de las transferencias internacionales de datos .....	580
7. Transferencias internacionales de datos a estados que no proporcionen un nivel adecuado de protección .....	581
8. Notificación de las transferencias internacionales de datos al registro general de protección de datos .....	585
9. Normas corporativas vinculantes (NCV) .....	587
9.1. Qué son las normas corporativas vinculantes (NCV) .....	587
9.2. Antecedentes normativos y disposiciones actuales que dan soporte a las NCV .....	587
9.3. Contenido de las NCV .....	588
9.4. Procedimiento de elaboración de una NCV .....	589
9.5. Ventajas de las normas corporativas vinculantes .....	590
9.6. Normas corporativas vinculantes (NCV) en el Reglamento Europeo de Protección de Datos .....	591
9.6.1. Definición .....	591
9.6.2. Contenido mínimo de las NCV .....	591
9.6.3. Aprobación por la autoridad de control de una NCV .....	593

	<u>Página</u>
9.6.4. Formato y procedimiento para el intercambio de información en una NCV .....	593
10. Cloud computing y transferencias internacionales de datos .....	593
11. Transferencias internacionales de datos, encargados del tratamiento y subcontrataciones .....	594
11.1. <i>Obligaciones del responsable del fichero que quiera contar con un encargado del tratamiento para la prestación de un servicio, que implique transferir internacionalmente datos</i> .....	594
11.2. <i>Subcontrataciones por parte del encargado del tratamiento y transferencias internacionales de datos</i> .....	595
11.3. <i>Ubicación de la página web y la base de datos de una empresa en un servidor de estados unidos</i> .....	596
12. Sanciones por irregularidades en transferencias internacionales de datos .....	596
13. Modelos de contratos de TID entre un responsable y un encargado del tratamiento, de conformidad a lo establecido en la decisión de la comisión europea de 5 de febrero de 2010 [2010/87/UE] .....	596
14. Modelo de contrato para la transferencia de datos personales a los subencargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos .....	605
15. Las TID en el Reglamento Europeo de Protección de Datos .....	614
15.1. <i>Introducción</i> .....	614
15.2. <i>Principio general y supuestos en los que cabe una TID</i> .....	616
15.3. <i>Transferencias basadas en una decisión de adecuación de la Comisión Europea</i> .....	619
15.4. <i>Transferencias mediante garantías adecuadas</i> .....	621
15.5. <i>Transferencias no autorizadas por el Derecho de la UE</i> .....	623
15.6. <i>Normas corporativas vinculantes</i> .....	623
15.7. <i>Régimen sancionador ante infracciones relativas a TID</i> .....	623
<b>TEMA 8</b>	
<b>Códigos de conducta y certificación en materia de protección de datos</b> .....	625
1. Los códigos de conducta (o códigos tipo) en la LOPD y en su reglamento de desarrollo .....	625
1.1. <i>Objeto y naturaleza de los códigos de conducta (o códigos tipo). Aproximación normativa</i> .....	625
1.2. <i>Contenido de los códigos tipo, según la vigente LOPD</i> .....	627
1.3. <i>Garantías del cumplimiento de los códigos de conducta</i> .....	630
1.4. <i>Inscripción de un código tipo (hasta mayo de 2018)</i> .....	630
1.5. <i>Códigos tipo inscritos en España</i> .....	633
1.6. <i>Códigos tipo de ámbito europeo atendiendo a la regulación de la Directiva 95/46/CE</i> .....	634
2. Los códigos de conducta en el Reglamento Europeo de Protección de Datos y en el anteproyecto de reforma de la LOPD .....	636
3. La certificación en el Reglamento Europeo de Protección de Datos .....	639
3.1. <i>Introducción</i> .....	639
3.2. <i>Certificación en protección de datos</i> .....	640
3.3. <i>El organismo de certificación</i> .....	641

**TEMA 9**

<b>Infracciones y sanciones en protección de datos</b> .....	643
1. Introducción al régimen sancionador .....	643
1.1. <i>En la LOPD</i> .....	643
1.2. <i>En el Reglamento Europeo de Protección de Datos</i> .....	645
2. Infracciones y sanciones .....	646
2.1. <i>Infracciones y sanciones en la LOPD</i> .....	646
2.2. <i>Infracciones y sanciones en el Reglamento Europeo de Protección de Datos y en el anteproyecto de reforma de la LOPD</i> .....	653
3. Graduación y atenuación de las sanciones en la LOPD y en el Reglamento Europeo de Protección de Datos .....	665
3.1. <i>Graduación y atenuación de las sanciones en la LOPD</i> .....	665
3.1.1. <i>Graduación de las sanciones en la LOPD</i> .....	665
3.1.2. <i>Atenuación de las sanciones en la LOPD</i> .....	667
3.2. <i>Graduación y atenuación de las sanciones en el Reglamento Europeo de Protección de Datos y en el anteproyecto de reforma de la LOPD</i> .....	671
4. Terminación por reconocimiento de la responsabilidad o pronto pago .....	674
5. El apercibimiento (y la advertencia), según la LOPD y el Reglamento Europeo de Protección de Datos .....	675
5.1. <i>El apercibimiento en la LOPD</i> .....	675
5.2. <i>El apercibimiento y la advertencia en el Reglamento Europeo de Protección de Datos</i> .....	678
6. Presunción de inocencia .....	678
7. Prescripción de las infracciones y sanciones .....	679
8. Régimen de responsabilidad en la LOPD y en el REPD .....	680
8.1. <i>Régimen de responsabilidad en la LOPD</i> .....	680
8.2. <i>Régimen de responsabilidad en el Reglamento Europeo de Protección de Datos</i> .....	681

**TEMA 10**

<b>Procedimientos tramitados por la Agencia Española de Protección de Datos</b> .....	683
1. Introducción y encaje normativo de los procedimientos tramitados por la AEPD .....	684
1.1. <i>Procedimientos en la LOPD, su Reglamento de desarrollo, y en el anteproyecto de reforma de la LOPD</i> .....	684
1.2. <i>El derecho a presentar reclamaciones ante la autoridad de control en el Reglamento Europeo de Protección de Datos</i> .....	688
1.3. <i>El derecho a la tutela judicial efectiva contra una autoridad de control en el Reglamento Europeo de Protección de Datos. Competencias</i> .....	688
1.4. <i>El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento en el Reglamento Europeo de Protección de Datos</i> .....	689
2. Representación .....	690
2.1. <i>La representación en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común</i> .....	690
2.2. <i>La representación en el Reglamento Europeo de Protección de Datos</i> .....	690
2.3. <i>Suspensión de procedimientos judiciales, según el Reglamento Europeo</i> .....	692
3. Publicidad de las resoluciones de la AEPD .....	692
4. Procedimiento de tutela de derechos de acceso, rectificación, cancelación u oposición .....	693
5. Procedimientos relativos al ejercicio de la potestad sancionadora .....	695

	<u>Página</u>
5.1. Actuaciones previas de los inspectores de la AEPD .....	695
5.2. Archivo de denuncias y sus causas más frecuentes .....	697
5.3. Valor de las actas de inspección de los inspectores de la AEPD .....	699
5.4. Procedimiento sancionador .....	700
5.5. Inmovilización de ficheros .....	705
6. Legitimación para recurrir en vía jurisdiccional resoluciones de la AEPD e indefensión por defectos procedimentales .....	706
6.1. Legitimación para recurrir en vía jurisdiccional .....	706
6.2. Indefensión por defectos procedimentales .....	706
7. Procedimiento de exención del deber de información al interesado .....	707
8. Procedimiento para la conservación de datos con fines históricos, estadísticos o científicos .....	708

## TEMA 11

<b>Autoridades de control en protección de datos .....</b>	<b>711</b>
1. Autoridades de control en la Directiva 95/46/CE y en el Reglamento Europeo de Protección de Datos .....	712
1.1. Competencia de la autoridad de control .....	716
1.2. Funciones de la autoridad de control .....	719
1.3. Poderes de la autoridad de control .....	721
1.4. Informe de actividad. Memoria anual .....	723
2. Procedimientos de cooperación y coherencia en el reglamento europeo de protección de datos .....	724
2.1. Cooperación .....	724
2.2. Coherencia .....	727
3. La Agencia Española de Protección de Datos como autoridad de control .....	730
3.1. La Agencia Española de Protección de Datos (AEPD) .....	730
3.2. ¿Tiene la Agencia Española de Protección de Datos competencia para restringir la publicidad de una sentencia del Tribunal Constitucional? .....	737
3.3. ¿Es competente la AEPD para resolver una reclamación de tutela del derecho de cancelación y oposición a la publicidad de las resoluciones del Tribunal Constitucional? ...	739
3.4. El/de la Director/a de la Agencia Española de Protección de Datos .....	739
3.5. Consejo Consultivo de la Agencia Española de Protección de Datos .....	742
3.6. El Registro General de Protección de Datos (RGPD) .....	743
3.7. Subdirección General de Inspección de Datos (SGI) –la inspección de datos .....	743
3.8. Secretaría General de la Agencia .....	744
3.9. Régimen económico, patrimonial y de personal de la Agencia Española de Protección de Datos .....	744
4. El Consejo General del Poder Judicial (CGPJ) y su competencia sobre datos jurisdiccionales .....	744
5. Agencias autonómicas de protección de datos .....	746
5.1. Autoritat Catalana de Protecció de Dades –Autoridad Catalana de Protección de Datos (APDCAT) .....	747
5.2. Datuak Babesteko Euskal Bulegoa – Agencia Vasca de Protección de Datos (AVPD) .....	748
5.3. Agencias autonómicas en el anteproyecto de reforma de la LOPD .....	749
6. Supervisor europeo de protección de datos (SEPD) .....	751
7. Comité consultivo del convenio nº 108 .....	752
8. Grupo de Trabajo del Artículo 29 (GT29) .....	752

	<u>Página</u>
9. El Comité Europeo de Protección de Datos (CEPD) .....	754
10. La Europol .....	757
11. Autoridad Común de Control de Schengen .....	759
12. Autoridad común de control en el sistema de información aduanero .....	761
13. Autoridad Común de Control Eurojust .....	762
14. Red Global de Control de la Privacidad (Global Privacy Enforcement Network-GPEN) .....	762

## TEMA 12

<b>Ficheros de «solventia patrimonial y crédito» y «de cumplimiento o incumplimiento de obligaciones dinerarias» .....</b>	<b>765</b>
1. Regulación de los ficheros de solventia patrimonial y crédito .....	766
2. Los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias o ficheros de morosos .....	767
2.1. <i>Introducción y encaje normativo</i> .....	767
2.2. <i>Ficheros de cumplimiento o incumplimiento de obligaciones dinerarias en España con mayor número de incidencias registradas</i> .....	769
2.3. <i>Requisitos de inclusión en un fichero de cumplimiento o incumplimiento de obligaciones dinerarias</i> .....	770
2.4. <i>Notificación a los interesados de los datos registrados en el fichero común</i> .....	780
2.5. <i>Supuestos que habilitan la consulta al fichero común de morosidad</i> .....	783
2.6. <i>Responsabilidad frente a inexactitudes de registro en el fichero común</i> .....	786
2.7. <i>Derechos de acceso, rectificación, cancelación u oposición (arco) frente a un fichero relativo al cumplimiento o incumplimiento de obligaciones dinerarias</i> .....	789
2.8. <i>Cancelación inmediata de la deuda tras el pago de la misma. El saldo cero</i> .....	798
2.9. <i>Regímenes matrimoniales y ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias</i> .....	800
3. Vulneración del derecho al honor por inclusión indebida o no veraz en un fichero relativo al cumplimiento o incumplimiento de obligaciones dinerarias .....	802
4. Fichero de morosos inmobiliarios y listas negras .....	807
4.1. <i>Registro de sentencias firmes de impagos de rentas de alquiler</i> .....	807
4.2. <i>Ficheros de morosos inmobiliarios y listas negras de naturaleza privada</i> .....	807
5. Inclusión de datos personales, por parte de empresas de recobro, en un fichero de solventia patrimonial y crédito .....	809
6. Central de Información de Riesgos del Banco de España (CIRBE) .....	810

## TEMA 13

<b>Videovigilancia .....</b>	<b>819</b>
1. Introducción .....	820
2. La imagen como dato de carácter personal y ámbito de aplicación de la LOPD a los sistemas de videovigilancia .....	820
2.1. <i>La imagen como dato personal</i> .....	820
2.2. <i>Ámbito de aplicación de la normativa de protección de datos a los tratamientos derivados de videovigilancia</i> .....	821
2.3. <i>Tratamientos con fines de videovigilancia en el anteproyecto de reforma de la LOPD</i> .....	823
3. Requisitos que habilitan la instalación de un sistema de videovigilancia .....	824
3.1. <i>Principio de proporcionalidad</i> .....	824
3.2. <i>Interés legítimo del responsable del tratamiento de videovigilancia</i> .....	827



	<u>Página</u>
4. Responsables del fichero y encargados del tratamiento en los sistemas de videovigilancia .....	828
5. Requisitos para la instalación de un sistema de videovigilancia, respecto a la captación de imágenes, cartel e impreso informativo y finalidad de los tratamientos .....	829
6. Inscripción en el registro de protección de datos de un sistema de videovigilancia ...	833
7. Conservación de las imágenes grabadas .....	833
8. Derechos que pueden ejercitar las personas cuyas imágenes han sido captadas por un sistema de videovigilancia .....	834
9. Cesión a la compañía aseguradora de las imágenes de un accidente captadas con las cámaras de videovigilancia instaladas en el interior de un establecimiento .....	835
10. Nivel de seguridad de ficheros de videovigilancia .....	836
11. Videovigilancia en actividades y servicios de seguridad privada .....	836
12. Cámaras de videovigilancia instaladas por las fuerzas y cuerpos de seguridad del estado .....	837
13. Control de acceso a edificios a través de videovigilancia .....	839
14. Video grabado a efectos probatorios .....	840
15. Videocámaras “on board” instaladas en el exterior de vehículos .....	840

## TEMA 14

### Publicidad, comunicaciones comerciales electrónicas y protección de datos .....

1. Introducción y aproximación normativa .....	844
2. Tratamiento de datos con fines comerciales o publicitarios en la LOPD. Las fuentes accesibles al público .....	845
2.1. <i>Planteamiento general</i> .....	845
2.2. <i>Las fuentes accesibles al público (FAP)</i> .....	845
2.2.1. Consideración de fuente de acceso público .....	845
2.2.2. Derecho de información al afectado .....	849
2.2.3. Caducidad de las fuentes accesibles al público .....	850
3. El reglamento europeo y los tratamientos de datos con fines comerciales o publicitarios .....	850
4. Ejercicio de derechos ante tratamientos con fines publicitarios o de prospección comercial .....	851
5. Utilización de bases de datos propias para realizar una campaña publicitaria .....	853
6. Adquisición de bases de datos de potenciales clientes en el mercado .....	853
6.1. <i>Declaración de legalidad de la BD y cláusulas de exoneración de responsabilidad</i> .....	854
6.2. <i>Plazos de caducidad y actualización de la base de datos</i> .....	854
6.3. <i>Informar en cada comunicación a los destinatarios</i> .....	854
6.4. <i>Consulta previa a una Lista Robinson (de exclusión)</i> .....	855
6.5. <i>Atender el ejercicio de derechos de los interesados</i> .....	855
7. Encomendar a un tercero la realización de una campaña publicitaria o comercial .....	858
7.1. <i>Fijación de responsabilidad en protección de datos</i> .....	858
7.2. <i>Encargo de una campaña a un tercero pero utilizando la base de datos de la propia entidad</i> .....	859
7.3. <i>Inscripción de ficheros en la AEPD</i> .....	863
8. Ficheros de exclusión del envío de comunicaciones comerciales. Las listas robinson .....	863
9. Medidas de seguridad a aplicar a un fichero con fines publicitarios o de prospección comercial .....	866

	<u>Página</u>
10. Llamadas telefónicas no solicitadas con fines de venta directa .....	866
11. Prácticas comerciales desleales .....	869
12. Comunicaciones comerciales por vía electrónica .....	870
12.1. Régimen jurídico de las comunicaciones comerciales electrónicas .....	870
12.2. Comunicación electrónica comercial de naturaleza viral .....	873
12.3. Régimen sancionador por infracciones en relación con las comunicaciones comerciales electrónicas .....	874
12.3.1. Según el artículo 38.3.c), d) e i) se consideran infracciones graves, cuya sanción prevista es de multa de 30.001 € hasta 150.000 €, las siguientes conductas .....	874
12.3.2. Se consideran como infracciones leves, según el artículo 38.4.d), g) y h) de la LSSICE, cuya sanción es de multa de hasta 30.000 €, las siguientes conductas .....	875
13. La regulación del uso de dispositivos de almacenamiento y recuperación de información en los equipos terminales de los usuarios (las «cookies») .....	876
13.1. Concepto y alcance de «cookies» .....	876
13.2. Aproximación a la normativa europea en materia de «cookies» y dictámenes de las autoridades europeas de protección de datos .....	876
13.3. Regulación en España del uso de las «cookies» .....	878
13.4. Guía de la AEPD sobre el uso de las «cookies» .....	879
13.5. Las «cookies» y la autorregulación de la publicidad online en Europa .....	880
14. Propuesta de reglamento sobre la privacidad y las comunicaciones electrónicas (reglamento e-privacy) .....	881

## TEMA 15

<b>Las relaciones laborales y la protección de datos</b> .....	<b>883</b>
1. Las relaciones laborales y la protección de datos. Regulación en el Reglamento Europeo de Protección de Datos .....	884
2. Procesos de selección de personal y su implicación en protección de datos .....	886
2.1. Información y consentimiento del solicitante de empleo para el tratamiento y cesión de sus datos personales contenidos en un curriculum .....	886
2.2. Solicitud de datos que resulten discriminatorios en un proceso de selección .....	888
2.3. Antecedentes penales del candidato. Certificado de delitos de naturaleza sexual .....	888
2.4. Listas negras de trabajadores .....	888
3. Portales de empleo a través de internet .....	889
4. Contratos de trabajo y cláusulas de protección de datos. Información y consentimiento del trabajador. Cláusulas de confidencialidad .....	890
4.1. Principio de información y consentimiento para el tratamiento de datos del trabajador en los contratos laborales .....	890
4.2. Cláusula de confidencialidad y normas de uso del correo electrónico .....	892
5. Fichero de control sobre el absentismo laboral con datos de salud de los trabajadores .....	897
6. Prevención de riesgos laborales y protección de datos .....	898
6.1. Tratamientos de datos personales en la función de prevención de riesgos laborales .....	898
6.2. Servicios de prevención de riesgos laborales .....	899
6.3. Consideración de datos de salud y medidas de seguridad .....	900
6.4. Acceso de los delegados de prevención a datos de salud .....	900
7. Función de las organizaciones sindicales y sus implicaciones en materia de protección de datos .....	901

	<u>Página</u>
7.1. Cesión de datos personales de trabajadores a organizaciones sindicales .....	901
7.2. Remisión de información sindical por correo electrónico a los trabajadores .....	902
7.3. Publicación de información sindical que incorpore datos personales de trabajadores en los tablones de anuncios o en la intranet corporativa .....	904
8. Comunicación de datos de trabajadores al comité de empresa .....	905
9. Cesión de datos de los trabajadores con el fin de suscribir seguros de vida y planes de pensiones .....	906
10. Cesión de datos de trabajadores a contratistas .....	907
11. Agencias de colocación y tratamiento de datos de los trabajadores .....	908
12. Derecho a la intimidad y al secreto a las comunicaciones en la intervención empresarial de los medios informáticos .....	908
12.1. Control de los medios informáticos puestos a disposición de los trabajadores .....	908
Resumen de los criterios seguidos por la jurisprudencia y la AEPD para el control de los medios informáticos puestos a disposición de los trabajadores .....	915
12.2. La intervención del correo electrónico en la Jurisdicción penal requiere contar con autorización judicial .....	916
12.3. El control biométrico de los trabajadores .....	917
12.3.1. Concepto y control biométrico en la jurisprudencia .....	917
12.3.2. Control biométrico en el Reglamento Europeo de Protección de Datos .....	919
13. Utilización de pruebas obtenidas de redes sociales para justificar un despido disciplinario .....	920
14. Videovigilancia en el centro de trabajo .....	921
14.1. Consentimiento o no del trabajador para la instalación de sistemas de videovigilancia .....	921
14.2. Comunicación de la instalación de videovigilancia a los representantes de los trabajadores y comité de empresa .....	926
14.3. Aspectos a tener en cuenta por la empresa para instalar sistemas de videovigilancia ..	927
14.4. Acceso por parte de los representantes de los trabajadores a las grabaciones realizadas por los sistemas de videovigilancia en el centro de trabajo .....	930
14.5. Grabaciones del trabajador al empleador en el ámbito laboral y posibles intromisiones ilegítimas en el derecho a la intimidad, secreto en las comunicaciones y protección de datos .....	930
15. Sistemas de geolocalización de los trabajadores .....	932
15.1. Estudio general de los requisitos, en materia de protección de datos, sobre sistemas de geolocalización de los trabajadores .....	932
15.2. Geolocalización de escoltas mediante localizador GPS .....	934
15.3. Utilización en los vehículos de policía de sistemas de geolocalización a través de GPS .....	934
16. Sistema de denuncias internas en el sector privado «whistleblowing» y la figura del «compliance officer» o director de cumplimiento normativo .....	936
<b>TEMA 16</b>	
<b>Abogados, procuradores y mediadores y las implicaciones en materia de protección de datos .....</b>	<b>941</b>
1. Cambio de paradigma en los despachos de abogados y procuradores .....	942
2. Determinación del responsable del fichero y/o tratamiento en las distintas formas de ejercicio de la abogacía .....	943
3. Obligaciones formales para profesionales del derecho .....	944

	<u>Página</u>
4. Principios de consentimiento e información respecto a los clientes de un abogado/ procurador y de la contraparte en un proceso judicial .....	945
4.1. <i>Tratamientos de datos de los propios clientes</i> .....	945
4.1.1. Regla general: principio de información en la LOPD .....	945
4.1.2. Legitimación del abogado/procurador para el tratamiento de los da- tos especialmente protegidos de sus clientes. Designaciones en turno de oficio .....	945
4.1.3. Turno de oficio y legitimación del tratamiento .....	946
4.1.4. Reglamento Europeo y tratamientos de datos por parte de abogados y procuradores .....	947
4.1.5. Derecho de información y principio de transparencia que debe prestar el abogado o procurador a su cliente, según el Reglamento Europeo de Protección de Datos .....	947
4.2. <i>Tratamientos de datos de la contraparte en un proceso</i> .....	949
4.3. <i>Responsabilidad penal del abogado por aportación de documentos, obtenidos irregular- mente por su cliente, en procedimientos judiciales</i> .....	951
5. Ejercicio de derechos ante un abogado o procurador .....	952
6. Medidas de seguridad en un despacho de abogados o procuradores .....	953
6.1. <i>Introducción</i> .....	954
6.2. <i>Clasificación de las medidas de seguridad con la LOPD</i> .....	955
6.3. <i>Aspectos a considerar derivados de la Ley de Blanqueo de Capitales</i> .....	957
7. Acceso del abogado a datos por cuenta de terceros .....	959
8. Cesión de datos del turno de oficio a los colegios de abogados .....	959
9. Comunicación de datos de los colegios de abogados y procuradores al Consejo General del Poder Judicial .....	960
10. Cesión de datos de letrados, por parte de los colegios de abogados, a la Agencia Estatad de Administración Tributaria (AEAT) con ocasión de los dictámenes emitidos ante la impugnación de costas judiciales .....	960
10.1. <i>Informe jurídico de la AEPD</i> .....	960
10.2. <i>Informe de la Comisión Jurídica del Consejo General de la Abogacía Española</i> .....	961
11. «Cloud computing» o servicios en la nube para abogados .....	962
12. Publicación de sentencias íntegras con inclusión de los nombres de los profesionales intervinientes en repertorios de jurisprudencia y en publicaciones jurídicas .....	963
13. Guías de abogados y procuradores como fuentes accesibles al público .....	964
14. Publicidad y comunicaciones comerciales por medios electrónicos por parte de los abogados .....	965
15. Uso de «WhatsApp» como medio de comunicación entre abogados y procuradores y sus clientes .....	968
16. Reclamaciones entre abogados con el trasfondo de la LOPD .....	969
17. Ficheros ilegales de abogados sospechosos por razón de las defensas asumidas .....	969
18. Publicidad del Registro de la Propiedad versus protección de datos .....	970
18.1. <i>Acreditación del interés legítimo</i> .....	971
18.2. <i>Límites de la normativa de protección de datos</i> .....	971
18.3. <i>Actuación del registrador a la hora de calificar</i> .....	972
19. La mediación y las obligaciones en materia de protección de datos .....	973
19.1. <i>Introducción y aproximación normativa</i> .....	973
19.2. <i>La confidencialidad en la mediación</i> .....	974

**TEMA 17**

<b>Tratamientos de datos personales relacionados con la salud</b> .....	977
1. Consideración de datos de carácter personal relacionados con la salud .....	978
1.1. <i>Los datos de salud en la Directiva 95/46/CE; y en la LOPD y RLOPD</i> .....	978
1.2. <i>La historia clínica</i> .....	979
1.3. <i>Los datos de salud en el Reglamento Europeo de Protección de Datos</i> .....	980
1.3.1. <i>Definiciones</i> .....	980
1.3.2. <i>Legitimación para el tratamiento de categorías de datos especiales: datos de salud, genéticos, o biométricos</i> .....	982
1.3.3. <i>Tratamientos de salud a "gran escala"</i> .....	986
1.3.4. <i>Registro de actividades de tratamiento</i> .....	986
2. <i>Legitimación para el tratamiento de datos de salud en la LOPD: El consentimiento</i> ..	987
3. <i>Ejercicios de derechos de los afectados frente a tratamientos de datos relacionados con su salud</i> .....	987
3.1. <i>Aspectos generales del derecho de acceso a la historia clínica</i> .....	987
3.2. <i>Alcance del derecho de acceso a la historia clínica</i> .....	990
3.3. <i>Historia clínica de los pacientes fallecidos</i> .....	991
3.4. <i>Acceso a la historia clínica de un menor por uno de los padres</i> .....	991
3.5. <i>Acceso a la historia clínica de pacientes por parte del personal sanitario</i> .....	992
3.6. <i>Derecho de acceso a los informes periciales de salud o valoración corporal, por parte del interesado</i> .....	994
3.7. <i>Información a familiares por parte de los servicios de urgencias</i> .....	994
3.8. <i>Rectificación de datos identificativos en la historia clínica por cambio de sexo</i> .....	994
3.9. <i>Acceso al contrato de seguro incorporado supuestamente a una historia clínica</i> .....	995
4. <i>Conservación y cancelación del historial clínico</i> .....	996
5. <i>Medidas de seguridad en ficheros con datos personales relacionados con la salud</i> ...	998
5.1. <i>Introducción</i> .....	998
5.2. <i>Nivel de seguridad, custodia y conservación de la historia clínica</i> .....	998
5.3. <i>Ejemplos de vulneración de medidas de seguridad en ficheros relacionados con la salud</i> .....	1000
5.4. <i>Medidas de seguridad en un fichero de implantes de productos sanitarios</i> .....	1000
6. <i>Herramientas informáticas de prescripción de medicamentos genéricos</i> .....	1001
7. <i>Implicaciones en materia de protección de datos de las actividades relacionadas con la utilización de células y tejidos humanos</i> .....	1001
8. <i>Facultativos que tienen alquilada una consulta en un centro de salud</i> .....	1002
9. <i>Traspaso de consulta médica o farmacia</i> .....	1002
10. <i>Utilización de datos de salud en los contratos de seguro</i> .....	1003
10.1. <i>El caso de que, con motivo de la contratación de un nuevo seguro, o por cualquier circunstancia equivalente, se conocieran datos «preexistentes» al primer contrato celebrado</i> .....	1003
10.2. <i>Con motivo de la celebración de un segundo contrato o por otros motivos, se conocieran datos relevantes para un contrato ya celebrado, pero posteriores a su celebración</i> .....	1004
10.3. <i>Situaciones relativas a un segundo contrato de seguro aún no concertado, respecto de las cuales el asegurador tenga conocimiento de datos de salud trascendentes en la valoración del riesgo, con motivo de un contrato anterior</i> .....	1004
11. <i>Cesión de datos de salud por los centros sanitarios a la compañía aseguradora</i> .....	1004
12. <i>Cesión de la historia clínica a un Tribunal eclesiástico</i> .....	1004

13. Comunicación a Tráfico de los datos relativos a personas a las que se ha declarado en situación de incapacidad, pero mantienen su permiso de conducir .....	1005
14. Recetas médicas, órdenes de dispensación y sus implicaciones en materia de protección de datos .....	1006
15. Tratamiento de datos de análisis de sangre para controles antidopaje .....	1007
16. Recomendaciones e informes a centros sanitarios .....	1008
16.1. <i>Recomendaciones resultantes del informe de cumplimiento de la LOPD en hospitales, de la AEPD, de octubre de 2010</i> .....	1008
16.2. <i>Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español del INTECO y la (extinta) APD de la Comunidad de Madrid</i> .....	1009

## TEMA 18

<b>Protección de datos en colegios y centros de formación</b> .....	1011
1. La protección de datos en los centros educativos. Menores y datos personales .....	1012
1.1. <i>Introducción</i> .....	1012
1.2. <i>Tratamiento de datos de menores de edad</i> .....	1013
1.3. <i>Trabajo habitual con menores y necesidad de contar con un “Certificado de delitos de naturaleza sexual”</i> .....	1013
2. Centros de educación reglada (no universitaria) y tratamiento de datos personales ..	1014
3. Inscripción de ficheros en el Registro General de Protección de Datos .....	1014
4. El tratamiento de datos por los centros educativos .....	1015
4.1. <i>Con la actual LOPD</i> .....	1015
4.2. <i>Tratamiento de datos a partir del Reglamento Europeo, en mayo de 2018</i> .....	1017
5. Medidas de seguridad. Algunos supuestos especiales .....	1018
5.1. <i>Deber de información y medidas de seguridad</i> .....	1018
5.2. <i>Fichero con datos personales de los alumnos</i> .....	1018
5.3. <i>Fichero de alumnos matriculados en la asignatura de religión</i> .....	1018
5.4. <i>Nivel de seguridad exigible a los ficheros de alumnos de una universidad</i> .....	1019
5.5. <i>Medidas de seguridad aplicables al campus virtual de un centro educativo</i> .....	1019
6. Derechos de los interesados .....	1021
6.1. <i>Acceso por parte de los padres a las calificaciones de sus hijos menores de edad</i> .....	1021
6.2. <i>Acceso de los progenitores a las calificaciones de sus hijos mayores de edad en el ámbito universitario y en centros docentes</i> .....	1022
6.2.1. <i>En el ámbito universitario</i> .....	1022
6.2.2. <i>Supuesto de centros docentes no universitarios</i> .....	1023
6.3. <i>Derecho de acceso a documentos e informes sobre la evolución de un menor en una escuela infantil</i> .....	1024
6.4. <i>Ejercicio de derechos ante un colegio público por parte de un alumno menor de edad</i> .	1025
6.5. <i>Puesto que existe una relación contractual entre el colegio y los padres que no puede ser asumida por el menor, ¿es lícito facilitar dichas calificaciones a los padres como resultado de los servicios contratados?</i> .....	1026
7. Publicación de datos personales en la web de un centro educativo .....	1026
7.1. <i>Eliminación de fotos de menores de la web de un colegio</i> .....	1026
7.2. <i>Publicación de datos personales de profesores en el sitio web de una universidad o centro de formación. Denegación del ejercicio del derecho de oposición</i> .....	1028
8. El sector educativo (no universitario), las plataformas de teleformación y el «cloud computing» .....	1028
9. Videovigilancia en los colegios .....	1032

	<u>Página</u>
10. Cámaras en centros infantiles .....	1033
11. Prevención y concienciación sobre privacidad entre menores de edad .....	1034

## TEMA 19

<b>Tratamientos de datos personales en la Administración Pública .....</b>	<b>1037</b>
1. Los ficheros de naturaleza pública y ámbito de aplicación de la LOPD .....	1039
2. Impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones públicas .....	1041
3. Creación, modificación y supresión de ficheros de titularidad pública y su notificación al Registro General de Protección de Datos .....	1046
3.1. <i>Ejemplo de inscripción: Orden JUS/746/2014, de 7 de mayo, por la que se desarrollan los artículos 14 y 21 del Real Decreto 980/2013, de 13 de diciembre y se crea el fichero de mediadores e instituciones de mediación .....</i>	<i>1047</i>
3.2. <i>Formulario NOTA para la notificación de la inscripción de ficheros públicos .....</i>	<i>1051</i>
3.3. <i>Formulario NOTA para la modificación de la inscripción de ficheros públicos .....</i>	<i>1055</i>
3.4. <i>Formulario NOTA para la supresión de ficheros públicos .....</i>	<i>1056</i>
4. Cesiones o comunicaciones de datos en el ámbito de la Administración Pública .....	1056
4.1. <i>Aspectos generales sobre las comunicaciones de datos entre Administraciones públicas y su encaje normativo .....</i>	<i>1056</i>
4.2. <i>Comunicaciones de datos, por medios electrónicos, en la Administración Pública .....</i>	<i>1059</i>
4.3. <i>Cesión de datos a la Administración Tributaria y deber de colaboración con la AEPD .....</i>	<i>1060</i>
4.4. <i>Cesión de datos de personas hospedadas a las Fuerzas y Cuerpos de Seguridad del Estado .....</i>	<i>1061</i>
<i>Modelo de parte de entrada de viajeros en un establecimiento hotelero .....</i>	<i>1062</i>
4.5. <i>Cesión de datos del Padrón a las Administraciones públicas y a las Fuerzas y Cuerpos de Seguridad del Estado .....</i>	<i>1063</i>
4.6. <i>Cesión de datos del Registro de Vehículos a las Fuerzas y Cuerpos de Seguridad del Estado .....</i>	<i>1064</i>
4.7. <i>Conservación y cesión de datos, por parte de los operadores de comunicaciones, a la Policía Judicial y Centro Nacional de Inteligencia .....</i>	<i>1065</i>
4.8. <i>Cesiones de datos personales en un expediente de contratación .....</i>	<i>1068</i>
4.9. <i>Publicación en Internet de los datos de personas que han resultado elegidas presidentes y vocales de las mesas electorales .....</i>	<i>1068</i>
4.10. <i>Cesiones de datos a empresas portuguesas .....</i>	<i>1069</i>
4.11. <i>Cesión de datos de un atestado a una compañía aseguradora .....</i>	<i>1069</i>
4.12. <i>Comunicación de datos de un atestado a los interesados o a sus representantes legales .....</i>	<i>1071</i>
4.13. <i>Cesiones de datos a las entidades gestoras de prestaciones de la Seguridad Social .....</i>	<i>1072</i>
5. Supuestos específicos en la Administración pública y principios de protección de datos .....	1074
5.1. <i>Administración de Justicia y protección de datos .....</i>	<i>1074</i>
5.2. <i>Orden de conservación de datos por el Ministerio Fiscal o Policía Judicial .....</i>	<i>1079</i>
5.3. <i>Subastas electrónicas y protección de datos .....</i>	<i>1079</i>
5.4. <i>Estatuto de la víctima de delitos y protección de datos .....</i>	<i>1080</i>
5.5. <i>¿Se requiere el consentimiento de las personas que aparecen en fotografías en un concurso organizado por un Ayuntamiento? ¿Sería necesario recabar su consentimiento para publicar la foto ganadora en una revista? .....</i>	<i>1080</i>



	<u>Página</u>
5.6. <i>Consentimiento de los interesados presentes en un pleno de un Ayuntamiento para poder grabar el mismo para posteriormente publicarlo en una página web en Internet ..</i>	1081
5.7. <i>Información contenida en el Catastro y datos personales .....</i>	1082
5.8. <i>¿Están las Fuerzas y Cuerpos de Seguridad del Estado autorizadas legalmente para acceder a un aparcamiento y proceder a registrar las matrículas de los vehículos estacionados? .....</i>	1084
5.9. <i>Tratamiento y acceso del público a documentos oficiales en el Reglamento Europeo de Protección de Datos .....</i>	1085
6. <i>Transparencia, acceso a la información pública y protección de datos en España .....</i>	1086
7. <i>Ejercicio de derechos y supuestos concretos en el ámbito de la Administración Pública .....</i>	1097
7.1. <i>Acceso a datos personales de empleados públicos y puesto que ocupan a la luz de la Ley de Transparencia .....</i>	1097
7.2. <i>Derecho de acceso a informe psicológico por parte de un interno en un centro penitenciario .....</i>	1098
7.3. <i>Derecho de cancelación frente a la Dirección General de Instituciones Penitenciarias .....</i>	1099
7.4. <i>Derecho de acceso a un atestado de la Policía .....</i>	1099
7.5. <i>Derecho de cancelación de datos frente al Registro de Conductores e Infractores .....</i>	1100
7.6. <i>Impugnación de valoraciones en procesos de adopción .....</i>	1100
7.7. <i>Derecho de los ciudadanos en la Administración Electrónica .....</i>	1101
7.8. <i>Derecho de cancelación de datos ante los Registros Administrativos de Apoyo a la Administración de Justicia .....</i>	1101
8. <i>Acceso a datos por cuenta de terceros en la Administración pública .....</i>	1106
8.1. <i>Contrato escrito de acceso a datos por cuenta de terceros en el ámbito de la contratación pública .....</i>	1106
8.2. <i>Encargados del tratamiento y Administración Pública en el Reglamento Europeo de Protección de Datos .....</i>	1107
8.3. <i>Entidad adjudicataria de la prestación de un servicio de atención telefónica a mujeres víctimas de violencia de género .....</i>	1108
8.4. <i>Entidades colaboradoras en la función de intermediación en la adopción internacional como encargadas del tratamiento .....</i>	1109
8.5. <i>Acceso a datos personales del Padrón por parte de una empresa pública, por cuenta del Ayuntamiento .....</i>	1109
8.6. <i>Acceso a datos personales en una plataforma de depósito de documentos electrónicos por parte de una Administración autonómica .....</i>	1110
9. <i>Medidas de seguridad en ficheros públicos .....</i>	1111
9.1. <i>Medidas de seguridad en un fichero de titularidad pública .....</i>	1111
9.2. <i>Medidas de seguridad en la Administración electrónica .....</i>	1113
9.3. <i>Medidas de seguridad en el sistema de Registros administrativos de apoyo a la Administración de Justicia .....</i>	1114
9.4. <i>Esquema Nacional de Seguridad .....</i>	1115
10. <i>El «cloud computing» en las Administraciones públicas .....</i>	1116
11. <i>Entidades locales y ficheros de solvencia patrimonial y crédito .....</i>	1118
12. <i>La Base de Datos Nacional de Subvenciones .....</i>	1118
13. <i>Registro Nacional de Víctimas de Accidentes de Tráfico .....</i>	1120
14. <i>Base de Datos Policial sobre identificadores obtenidos a partir del ADN .....</i>	1121
14.1. <i>La intimidad genética .....</i>	1121
14.2. <i>Antecedentes normativos .....</i>	1121
14.3. <i>Base de Datos Policial sobre identificadores obtenidos del ADN .....</i>	1122



	<u>Página</u>
14.4. <i>Las muestras de ADN son datos personales</i> .....	1123
14.5. <i>Operadores que tienen acceso a los datos de ADN</i> .....	1125
14.6. <i>Plazo de conservación de las muestras de ADN</i> .....	1125
14.7. <i>Comisión Nacional para el uso forense del ADN</i> .....	1125
14.8. <i>Documento de consentimiento informado de detenido o imputado para la obtención de muestras de ADN en asunto criminal</i> .....	1126
15. Ejercicio de derechos ante ficheros policiales de investigación .....	1128
16. Sistema Integrado de Gestión Operativa, Análisis y Seguridad Ciudadana (SIGO) de la Guardia Civil .....	1134
17. Registro Central de Delinquentes Sexuales .....	1136
18. Publicación de datos de infractores tributarios por parte de la Agencia Tributaria ....	1137
18.1. <i>Regulación</i> .....	1137
18.2. <i>Procedimiento de inclusión en el listado de morosos tributarios</i> .....	1138
19. Reutilización de la información del sector público .....	1138
19.1. <i>Regulación</i> .....	1138
19.2. <i>Ámbito objetivo de aplicación de la Ley sobre Reutilización de Información en el Sector Público</i> .....	1140
19.3. <i>Reutilización y protección de datos</i> .....	1141
19.4. <i>Conexión con la Ley de Transparencia y Acceso a la Información Pública</i> .....	1142
19.5. <i>Orientaciones sobre protección de datos en la reutilización de la información del sector público</i> .....	1143
20. Armonización en el intercambio de datos policiales y judiciales: la Directiva (UE) 2016/680 .....	1144
21. Remisión de mensajes SMS y MMS por parte de una fundación del sector público ...	1145
22. Infracciones en materia de protección de datos en ficheros de titularidad pública .....	1146

## TEMA 20

<b>Comunidades de propietarios, administradores de fincas y sus obligaciones en materia de protección de datos</b> .....	1149
1. Aproximación normativa .....	1150
1.1. <i>Ficheros y comunidades de propietarios</i> .....	1151
1.2. <i>La comunidad de propietarios como «responsable del fichero» y el administrador de fincas como «encargado del tratamiento»</i> .....	1151
2. Obligación formal de las comunidades de propietarios: Inscripción de sus ficheros ..	1155
3. Principios de consentimiento, información y calidad de los datos de los propietarios ..	1156
4. Entrega a los propietarios de documentación relativa a la gestión y administración del inmueble. Cesión de datos a entidades financieras .....	1158
4.1. <i>Acceso y obtención de copias de la documentación de la comunidad por parte de los propietarios de viviendas</i> .....	1158
4.2. <i>Exhibición del libro de actas de la comunidad de propietarios a entidades financieras</i> .....	1160
5. Ejercicio de derechos de acceso, rectificación, cancelación u oposición frente a la comunidad .....	1161
6. Medidas de seguridad sobre los ficheros de la comunidad de propietarios .....	1161
7. Deber de secreto de la comunidad de propietarios y del administrador de la finca en el tratamiento de datos personales .....	1163
8. Comunicaciones, tablones de anuncios y protección de datos .....	1164
8.1. <i>Publicación en tablones de anuncios de impagos de los recibos de la comunidad</i> .....	1164

	<u>Página</u>
8.2. <i>Publicación periódica de la relación de propietarios con cuotas vencidas y pendientes de pago</i> .....	1166
8.3. <i>Sanción de apercibimiento</i> .....	1167
8.4. <i>Principio de calidad de los datos tratados por la comunidad en las comunicaciones en el tablón de anuncios</i> .....	1167
8.5. <i>Exposición pública de comunicaciones recibidas por el presidente de la comunidad</i> ....	1168
8.6. <i>Derecho al honor y exposición pública de datos de propietarios morosos</i> .....	1168
9. <i>Videovigilancia en las comunidades de propietarios</i> .....	1169
9.1. <i>Normativa de aplicación en la videovigilancia en comunidades de vecinos</i> .....	1169
9.2. <i>Quórum necesario para la aprobación en junta general de la instalación de un sistema de videovigilancia</i> .....	1170
9.3. <i>Requisitos jurisprudenciales que habilitan la instalación de sistemas de videovigilancia (también en una comunidad de vecinos)</i> .....	1171
9.4. <i>Requisitos para instalar en una comunidad de propietarios un sistema de videovigilancia</i> .....	1172
9.5. <i>Aspectos a tener en cuenta cuando se pretenda instalar un sistema de videovigilancia en una comunidad de propietarios, respecto a la captación de imágenes, cartel e impreso informativo y finalidad de los tratamientos</i> .....	1173
9.5.1. <i>Captación de imágenes</i> .....	1173
9.5.2. <i>Cartel informativo</i> .....	1173
9.5.3. <i>Impresos informativos</i> .....	1173
9.5.4. <i>Principio de finalidad</i> .....	1174
9.6. <i>Inscripción en el Registro General de Protección de Datos de un sistema de videovigilancia</i> .....	1174
9.7. <i>Nivel de seguridad a ficheros de videovigilancia</i> .....	1175
9.8. <i>Videovigilancia en plazas de garaje</i> .....	1175
9.9. <i>Cesión a la compañía aseguradora de las imágenes de un accidente captadas con las cámaras de videovigilancia instaladas en el interior de una comunidad de vecinos</i> ....	1176
10. <i>El administrador de fincas y la protección de datos</i> .....	1176
10.1. <i>El administrador de fincas en el régimen de propiedad horizontal</i> .....	1176
10.2. <i>El administrador de fincas y el régimen de propiedad vertical</i> .....	1178

## TEMA 21

<b>Internet, redes sociales y protección de datos</b> .....	1179
1. <i>Riesgos para la privacidad en las redes sociales</i> .....	1180
2. <i>Redes sociales como responsables del tratamiento. Jurisdicción aplicable y ámbito de aplicación</i> .....	1181
3. <i>Usuarios de las redes sociales y su condición desde la perspectiva de la protección de datos</i> .....	1183
4. <i>Legitimación para el tratamiento y cumplimiento del principio de información por parte de las redes sociales</i> .....	1185
5. <i>Menores de edad y el tratamiento de sus datos en Internet y, especialmente, en las redes sociales</i> .....	1186
6. <i>Derechos de acceso, rectificación, cancelación u oposición ante la red social</i> .....	1189
7. <i>Conservación de los datos por la red social</i> .....	1189
8. <i>Medidas de seguridad en redes sociales</i> .....	1189
9. <i>La instalación de «cookies» en una red social y el consentimiento del usuario</i> .....	1190
10. <i>Redes sociales como plataformas para el envío de correos electrónicos no deseados</i> .....	1191

	<u>Página</u>
11. Datos personales de fallecidos en las redes sociales .....	1192
12. Protección civil y penal de la violación de los derechos al honor, la intimidad y la propia imagen a través de Internet y las redes sociales .....	1193
12.1. Suplantación de identidad en las redes sociales .....	1195
12.2. Descubrimiento y revelación de secretos .....	1196
12.3. Delitos contra el honor .....	1199
12.4. Extorsión y amenazas .....	1200
12.5. Delito de humillación a víctimas de delitos de terrorismo .....	1201
12.6. Delitos de acoso a través de Internet .....	1203
12.7. Delitos de injurias a la corona .....	1203
13. Pulsar «me gusta» en Facebook no es causa de abstención o recusación de un Juez ..	1204
14. Internet no se considera como una fuente accesible al público .....	1205
15. Privacidad en las aplicaciones móviles .....	1206
16. Actuaciones más destacadas de la Agencia Española de Protección de Datos en el ámbito de Internet .....	1208
16.1. Suplantación de identidad .....	1208
16.2. Administración pública .....	1209
16.3. Menores de edad .....	1209
16.4. Correos electrónicos .....	1210
16.5. Redes «peer to peer» .....	1210
16.6. Redes sociales .....	1210
16.7. Publicación en Internet de datos de forma indebida .....	1211

## TEMA 22

<b>Tratamientos específicos y su vinculación con protección de datos .....</b>	<b>1213</b>
1. Aeronaves no tripuladas (DRONES) y sus implicaciones en protección de datos .....	1213
1.1. Concepto y regulación .....	1213
1.2. Principio de información y ejercicio de los derechos frente a tratamientos de datos realizados por drones .....	1216
1.3. Conveniencia de la realización de una «evaluación de impacto en la protección de datos (EIPD)» en los tratamientos de imágenes captadas con drones .....	1218
1.4. Dictamen de las Autoridades Europeas de protección de datos sobre drones .....	1219
2. Tecnología RFID y privacidad .....	1220
2.1. Concepto y usos de la tecnología RFID .....	1220
2.2. Funcionamiento y estandarización de la tecnología rfid .....	1221
2.3. Riesgos para la privacidad y seguridad .....	1222
2.4. Recomendaciones y buenas prácticas .....	1223
3. El «cloud computing» y sus implicaciones en materia de protección de datos .....	1223
3.1. Antecedentes históricos de la computación en nube y perspectivas .....	1223
3.2. Concepto y características definidoras del «cloud computing» .....	1224
3.3. Tipos y modalidades de servicios de computación en nube .....	1225
3.4. Problemas y riesgos del «cloud computing» .....	1226
3.5. «Cloud computing» y tratamientos de datos personales. El responsable del tratamiento y el encargado del mismo .....	1227
3.6. Servicios de computación en nube en supuestos en los que el proveedor del mismo tiene su sede o domicilio en los Estados Unidos .....	1233
3.7. Estrategias para el cliente de servicios de computación en la nube .....	1233

	<u>Página</u>
4. Internet de las cosas (IOT) .....	1239
5. Big data .....	1241
<b>I</b>	
<b>Índice Analítico</b> .....	1243