

ÍNDICE GENERAL

<i>Acerca de la guía</i>	VII
<i>Orientación</i>	XI
<i>Terminología</i>	XIII
<i>Panorama actual</i>	XV
<i>Abreviaturas</i>	XXXVII

CAPÍTULO PRIMERO

DERECHO DE LA INTELIGENCIA ARTIFICIAL

§ 1.	Leyes que regulan a la IA	1
	a) Ley de Colorado sobre IA	3
	b) Ley de la IA de la UE	4
§ 2.	Seguridad de los productos, responsabilidad civil y legislación penal	4
§ 3.	Leyes que regulan la propiedad	8
	a) Propiedad de la IA, entrada y salida	9
	b) Infracciones	11
	c) Términos de la licencia de código abierto	13
	d) Injerencia informática y allanamiento de morada	16
	e) Derechos sobre los datos	17
§ 4.	Secretos industriales, confidencialidad y seguridad de la información	19
§ 5.	Lucha contra la discriminación	21
§ 6.	Privacidad y difamación	22
§ 7.	Publicidad	24

§ 8.	Reglamento General de Protección de Datos y otras normativas sobre tratamiento de datos	24
a)	Datos personales	25
b)	Desidentificación y datos sintéticos	25
c)	Datos disponibles públicamente	27
d)	Tratamiento	27
e)	Restricciones al tratamiento de datos personales	28
f)	Minimización de datos, limitación de la finalidad, equidad	28
g)	Derechos de los titulares de datos	29
h)	Evaluaciones de impacto de la protección de datos	29
i)	Aplicabilidad territorial del RGPD	30
j)	Medidas de cumplimiento del RGPD	30
§ 9.	Residencia y conservación de datos	32
§ 10.	Contratos y estándares de la industria	34

CAPÍTULO II

PUESTA EN MARCHA DE UN PROGRAMA DE CUMPLIMIENTO DE LA LEGISLACIÓN SOBRE IA

§ 11.	Hazte cargo	35
a)	Los responsables de protección de datos y los profesionales de la privacidad	36
b)	Abogados	36
c)	Profesionales de las tecnologías de la información	36
d)	Desarrolladores de producto	36
e)	Audidores y responsables de cumplimiento	37
f)	Usuarios de la IA	37
g)	Nuevo departamento o nuevos funcionarios	37
§ 12.	Gobernanza	38
§ 13.	Asignación de responsabilidades	39
§ 14.	Colaborar eficazmente con las partes interesadas internas y los asesores externos	40
§ 15.	Herramientas de monitoreo y automatización	41
§ 16.	Preparar una lista de tareas	43
§ 17.	Hacer balance de la IA y las leyes	45

§ 18.	Priorizar	47
§ 19.	Identificar los principales requisitos legales	50
	a) ¿Qué leyes son especialmente relevantes para la IA y su empresa?	50
	b) ¿Qué leyes se aplican a su empresa en función de las limitaciones por razón de la materia?	51
	c) ¿Qué leyes se aplican a la empresa en función de las limitaciones territoriales?	51
	d) ¿Qué leyes pueden aplicarse contra la empresa?	53
§ 20.	Ejecutar	55

CAPÍTULO III

REDACCIÓN DE LA DOCUMENTACIÓN

§ 21.	¿Por qué se crea el documento?	57
	a) Fines jurídicos	58
	b) Fines comerciales	60
	c) Objetivos organizacionales	61
§ 22.	¿Cuál es el público?	62
§ 23.	Diferenciar las categorías de documentación	63
§ 24.	Asesoramiento jurídico, riesgos y cumplimiento de la normativa	70
	a) Privilegio abogado-cliente	70
	b) Documentación para demostrar la conformidad	71
§ 25.	Avisos	74
§ 26.	Advertencias	75
§ 27.	Consentimiento	76
	a) Consentimiento necesario, útil y facultativo	76
	b) Cómo obtener un consentimiento válido	79
	c) Aceptación, exclusión e intermedios	81
	1) Ejemplos de mecanismos de consentimiento	81
	2) Antes o después de la formación del contrato	83
	3) Visibilidad	83
	4) El silencio como consentimiento	84
	5) Consentimiento afirmativo y expreso	84
	6) Consentimiento combinado	85

d) Más allá del consentimiento expreso	85
e) Otras consideraciones para la redacción del consentimiento	87
1) Incorporación de avisos a las declaraciones de consentimiento	87
2) Expresar un consentimiento específico	87
3) Colocación del mecanismo y la declaración de consentimiento	88
§ 28. Registros de actividades de tratamiento (RoPA), mapas de datos y diagramas de flujo	88
§ 29. Contratos	90
§ 30. Protocolos	90

CAPÍTULO IV

EVALUACIÓN DE IMPACTO Y MITIGACIÓN DE RIESGOS

§ 31. Impacto, daño y riesgo	91
§ 32. Cuantificar y calificar el riesgo y el daño	92
§ 33. Razones para evaluar los impactos y riesgos de la IA	92
§ 34. Riesgos por daños y responsabilidad	93
§ 35. Seguros	94
§ 36. Riesgos de sanciones y recursos particulares	94
§ 37. Proteger el secreto profesional y la confidencialidad al redactar las evaluaciones de impacto	99
§ 38. Evaluaciones de impacto y de riesgo específicamente requeridas	100
a) Auditorías parciales conforme con la ley de Nueva York ..	100
b) Evaluaciones de impacto de la protección de datos con arreglo al RGPD	100
c) Diseños adaptados a la edad	101
§ 39. Riesgos de la IA de la A a la Z	102
a) Toma de decisiones automatizada	102
b) Sesgo	104
c) Control	105

d) “Deepfakes”, difamación y desinformación	106
e) Ética y ESG	108
f) Reconocimiento facial y tratamiento de datos biométricos ..	109
g) Condiciones de contratación pública e impuestos	110
h) Alucinaciones	111
i) Derechos de propiedad intelectual, infracción e interfe- rencia informática	112
j) “Jailbreaking”	116
k) Contratos	116
l) Trabajo y empleo	117
m) Manipulación	118
n) Obligaciones de confidencialidad	119
ñ) Cumplimiento de la licencia del código fuente abierto ...	120
o) Privacidad y publicidad	120
p) Control de calidad	122
q) Conservación y residencia de los datos	122
r) Seguridad y protección	123
s) Transparencia	124
t) Comunicaciones no solicitadas (“spam”)	125
u) Vendedores	126
v) Armamento, control de las exportaciones, embargos co- merciales	129
w) Contenido X	129
x) Protección de la juventud	130
y) Amenazas de hora cero	132
§ 40. Riesgos de no desarrollar, proporcionar y utilizar la IA	132

CAPÍTULO V

CONTRATOS DE IA

§ 41. Organización de los contratos, cláusulas y anexos.	135
§ 42. ¿Qué ofrece un proveedor de este tipo de servicios?	138
§ 43. ¿Cuáles son las principales obligaciones del comprador?	139
§ 44. ¿Qué obligaciones secundarias asume cada parte o ambas? ...	143

§ 45.	¿Quién debe ser propietario de qué cosas?	144
§ 46.	¿Qué información es confidencial y cómo debe protegerla cada parte?	145
§ 47.	¿Qué debe hacer cada una de las partes, si las cosas salen mal?	146
§ 48.	¿Cómo debe responder cada una de las partes? ¿Qué límites deben aplicarse?	154
§ 49.	Legislación aplicable y jurisdicción	156
§ 50.	Fuerza mayor	156

CAPÍTULO VI

PROTOCOLOS

§ 51.	Ejemplo de protocolo sobre el uso aceptable de la IA generativa	158
§ 52.	Ejemplo de protocolo sobre el uso de código fuente abierto y generado por IA	159
§ 53.	Ejemplo de protocolo de adquisición y utilización de datos para el desarrollo de la IA	166

CAPÍTULO VII

MANTENIMIENTO Y AUDITORÍA DEL CUMPLIMIENTO

§ 54.	Obligaciones recurrentes y gestión de cambios	169
§ 55.	Retirar y caducar la documentación y los procesos	170
§ 56.	Asumir o auditar un programa de cumplimiento existente	171
§ 57.	Desarrollo de controles de auditoría	172
§ 58.	Controles técnicos de rendimiento, calidad y seguridad de la IA	173
§ 59.	Herramientas de cumplimiento y automatización	173
§ 60.	Debida diligencia en las fusiones y adquisiciones	174

§ 61. Debida diligencia respecto de los proveedores	176
§ 62. Formación continua de los trabajadores	176
§ 63. Seguimiento de nuevos desarrollos	177
<i>Lista de control</i>	179
<i>Recursos</i>	183

ABREVIATURAS

AEDT	Herramienta automatizada de decisión para el empleo.
API	Interfaz del programa de aplicación.
BIPA	<i>Biometric Information Privacy Act</i> (ley de privacidad de la información biométrica de Illinois).
CAADCA	<i>California Age-Appropriate Design Code Act</i> (ley del código de diseño adecuado a la edad de California).
CalOPPA	<i>California Online Privacy Protection Act</i> (ley de protección de la privacidad en línea de California).
CAPTCHA	Prueba de Turing pública y completamente automatizada para distinguir entre ordenadores y humanos; prueba automatizada de desafío-respuesta para confirmar que la respuesta ha sido generada por una persona.
CCPA	<i>California Consumer Privacy Act</i> (ley de protección de la privacidad de los consumidores de California de 2018).
CCS	Cláusulas contractuales tipo promulgadas por la Comisión Europea para las Transferencias Internacionales de Datos.
CDA	<i>Communications Decency Act</i> (ley de decencia en las comunicaciones –ley federal de Estados Unidos de América con privilegios de responsabilidad contributiva para los proveedores de servicios de internet–).
CFAA	<i>Computer Fraud and Abuse Act</i> (ley de fraude y abuso informático –ley federal estadounidense que prohíbe el acceso a ordenadores sin autorización–).
COPPA	<i>Children’s Online Privacy Protection Rule</i> (norma de protección de la privacidad infantil en línea).
CRM	Gestión de las relaciones con los clientes.
Dirección IP	Dirección de protocolo de internet; número asignado a cada dispositivo (p.ej., ordenador, <i>router</i> , servidor) de una red informática.
DMCA	<i>Digital Millennium Copyright Act</i> (ley de derechos de autor para el milenio digital).

DPA	Contrato de tratamiento de datos.
EDPB	Consejo Europeo de Protección de Datos (organismo de la Unión Europea creado en virtud del art. 68 del RGPD, compuesto por el director de la autoridad de protección de datos de cada Estado miembro de la UE y el supervisor europeo de protección de datos).
EEE	Espacio económico europeo (Estados miembros de la UE, más Islandia, Liechtenstein y Noruega).
EEE+	Estados miembros del EEE, más Suiza y el Reino Unido.
EEOC	Comisión para la Igualdad de Oportunidades en el Empleo de Estados Unidos de América.
EIPD	Evaluación de impacto de la protección de datos.
ERP	Planificación de recursos empresariales.
ESG	Gobernanza medioambiental y social.
FCRA	<i>Fair Credit Reporting Act</i> (ley de información crediticia equitativa de los Estados Unidos de América).
FTC	Comisión Federal de Comercio (autoridad estadounidense encargada de la protección de los consumidores y la intimidad).
HIPAA	<i>Health Insurance Portability and Accountability Act</i> (ley federal estadounidense de 1996, en su versión modificada).
IA	Inteligencia artificial.
IAG	IA general.
IAPP	Asociación Internacional de Profesionales de la Privacidad.
IAS	Infraestructura como servicio.
Informe SOC	Informe de controles de la organización de servicios, según SSAE 16.
ISO	Organización Internacional de Normalización (organización no gubernamental en la que representantes de institutos nacionales de normalización –algunas entidades gubernamentales y otras del sector privado– de 163 países coordinan la elaboración de normas internacionales).
LLM	Gran modelo lingüístico.
NDA	<i>Non-disclosure agreements</i> (contrato de confidencialidad, por sus siglas en inglés).
NIST	National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología, por sus siglas en inglés).
NSA	Agencia de Seguridad Nacional de los Estados Unidos de América.
ONG	Organización no gubernamental.
OSS	<i>Software</i> de código abierto.

PCI	El estándar PCI DSS (<i>payment card industry data security standard</i> o estándar de seguridad de datos de la industria de tarjetas de pago) se refiere a un conjunto de requisitos que son obligatorios para garantizar la seguridad de la información privada de los usuarios de tarjetas de crédito y débito.
PSI	Proveedor de servicios de internet.
RGPD	Reglamento general de protección de datos (UE) 2016/679, de 27/4/2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (en vigor desde el 25/5/2018).
RoPA	Registros de actividades de tratamiento.
RPD	Responsable de protección de datos.
SaaS	<i>Software</i> como servicio.
SAS 70	Norma de auditoría, sustituida por la SSAE 16.
SLA	<i>Service level agreements</i> (acuerdo de nivel de servicio, por sus siglas en inglés).
SSAE	<i>Statement on Standards for Attestation Engagements</i> (Declaración de Normas para los Encargos de Atestiguación, elaborada por el Instituto Americano de Contables Públicos Certificados).
TI	Tecnologías de la información.
TOM	Medidas técnicas, administrativas y organizacionales de seguridad de los datos.
UE	Unión Europea.

