

Incluye



Práctica del ejercicio de la abogacía y Derecho Internacional Privado de la Unión Europea

Volumen III. Parte especial:
Derecho de los negocios internacionales

ALFONSO ORTEGA GIMÉNEZ
(DIRECTOR)

LERDYS SARAY HEREDIA SÁNCHEZ
(COORDINADORA)

© Alfonso Ortega Giménez (Director), 2026
© ARANZADI LA LEY, S.A.U.

ARANZADI LA LEY, S.A.U.

C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es

Atención al cliente: <https://areacliente.aranzadilaley.es/publicaciones>

Primera edición: enero 2026

Depósito Legal: M-631-2026

ISBN versión impresa con complemento electrónico: 978-84-1085-579-3

ISBN versión electrónica: 978-84-1085-580-9

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.

Printed in Spain

© **ARANZADI LA LEY, S.A.U.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, ARANZADI LA LEY, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

ARANZADI LA LEY no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, o cualesquiera otras herramientas de participación. Igualmente, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

ARANZADI LA LEY queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

ARANZADI LA LEY se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **ARANZADI LA LEY, S.A.U.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Índice general

	<i><u>Página</u></i>
PRÓLOGO	25
PRESENTACIÓN	27
CAPÍTULO 1	
TELETRABAJO TRANSFRONTERIZO Y PROTECCIÓN DE DATOS PERSONALES	
ALFONSO ORTEGA GIMÉNEZ	31
I. El teletrabajo transfronterizo como tendencia global y sus repercusiones jurídicas	31
II. Teletrabajo transfronterizo y aplicación extraterritorial del Reglamento General de Protección de Datos de la UE	40
III. Teletrabajo transfronterizo y mecanismos adecuados para legitimar transferencias internacionales de datos	45
IV. La aplicación extraterritorial del Reglamento General de Protección de Datos y supuestos de teletrabajo transfronterizo ..	53
V. Referencias bibliográficas	62
CAPÍTULO 2	
LA DETERMINACIÓN DE LA LEY APLICABLE A LA CONTRATACIÓN AUTOMATIZADA, IA Y RESPONSABILIDAD TRANSFRONTERIZA	
ANTONIO MERCHÁN MURILLO	67
I. Introducción	67

	<u>Página</u>
II. Tipología funcional de la contratación automatizada	69
III. Formación, ejecución y errores sistémicos: problemas estructurales para la determinación de la ley aplicable	70
IV. Criterios de conexión en entornos automatizados y transfronterizos	79
1. <i>Régimen contractual: aplicación del Reglamento Roma I y la identidad electrónica como punto de conexión</i>	82
2. <i>Régimen extracontractual: productos digitales con IA y reinterpretación funcional del Convenio de La Haya de 1973</i>	88
V. Conclusiones	94
VI. Bibliografía	95

CAPÍTULO 3

CONTRATOS INTERNACIONALES DE *TIME-SHARING*

AURORA HERNÁNDEZ RODRÍGUEZ	99
i. Introducción	99
II. Los contratos internacionales de <i>Time-sharing</i>	100
1. <i>Aspectos generales</i>	100
2. <i>El Time-sharing en el Derecho español</i>	102
3. <i>Los contratos internacionales de time-sharing en la jurisprudencia española</i>	105
III. Competencia judicial internacional y contratos de <i>Time-sharing</i>	109
1. <i>Pluralidad normativa</i>	109
2. <i>Rbi-bis: el foro exclusivo del art. 24.1</i>	111
3. <i>Rbi-bis y protección del consumidor</i>	112
3.1. <i>Aspectos generales</i>	112
3.2. <i>Foros de protección</i>	115
4. <i>El foro de la sucursal (art. 7. 5 rbi-bis)</i>	121

	<u>Página</u>
4.1. Aspectos generales	121
4.2. Foro de la sucursal y contratos de <i>Time-sharing</i>	122
IV. Determinación del Derecho aplicable y contratos de <i>time-sharing</i>	127
1. Aspectos generales	127
2. Ley aplicable al contrato de <i>time-sharing</i> : el art. 6 RR-I	128
2.1. Art. 6 RR-I: Condiciones de aplicación	129
2.2. Art. 6 RR-I: Ley aplicable	130

CAPÍTULO 4

CONTRATOS E-COMMERCE CON CONSUMIDORES A TRAVÉS DE PLATAFORMAS DIGITALES: MARCO JURÍDICO OPERATIVO DESDE LA PERSPECTIVA DEL DERECHO EUROPEO EN UNA APROXIMACIÓN DE LEY APLICABLE

CLARA ISABEL CORDERO ÁLVAREZ	133
I. Introducción	134
II. Delimitación conceptual del objeto de estudio	139
1. Plataformas digitales B2C como prestadores de servicios de la sociedad de la información en el Derecho de la Unión	140
2. Modelos de negocio a través de plataformas en línea y su naturaleza jurídica: condicionante del marco jurídico y régimen de responsabilidad	145
3. Concurrencia necesaria de la condición de consumidor del usuario final y de contrato celebrado entre las partes para la aplicación del régimen tuitivo europeo	150
III. Marco jurídico europeo aplicable	160
1. Derecho Europeo sobre E-commerce: la DCE y el RSD para la regulación de los servicios en línea	160
2. Régimen de los contratos de consumo a través de plataformas B2C	167

	<u>Página</u>
2.1. Aspectos generales	170
2.2. Incidencia de la normativa imperativa europea sobre el contrato de consumo intermediado: Directivas de consumo y condiciones generales	172
2.3. Nuevas obligaciones sustantivas para las plataformas B2C en el RSD	176
IV. Conclusiones	185

CAPÍTULO 5

CLÁUSULAS CONTRACTUALES DE ELECCIÓN DE FORO: REGULACIÓN Y EFECTOS DE LA ADHESIÓN DE LA CONFEDERACIÓN SUIZA AL CONVENIO DE LA HAYA SOBRE ACUERDOS DE ELECCIÓN DEL FORO

GUAYASÉN MARRERO GONZÁLEZ	187
I. Introducción	187
II. La relevancia de los acuerdos de elección de foro en las relaciones comerciales internacionales	189
III. El convenio de La Haya sobre acuerdos de elección de foro ..	191
1. <i>Nulidad del acuerdo de elección de foro</i>	<i>202</i>
2. <i>Incapacidad de las partes</i>	<i>202</i>
3. <i>Falta de notificación adecuada</i>	<i>202</i>
4. <i>Fraude procesal</i>	<i>203</i>
5. <i>Orden público</i>	<i>203</i>
6. <i>Resoluciones incompatibles dictadas por el Estado requerido</i>	<i>203</i>
7. <i>Resoluciones incompatibles dictadas por tribunales extranjeros .</i>	<i>204</i>
IV. La articulación de las relaciones entre el Reino Unido y la confederación Suiza a través del convenio de La Haya sobre acuerdos de elección de foro	204
V. Conclusiones	208

CAPÍTULO 6

TUTELA TRANSFRONTERIZA DE DERECHOS DE PROPIEDAD INTELECTUAL UNITARIOS EN EUROPA: MARCA Y DISEÑO DE LA UNIÓN EUROPEA Y PATENTE EUROPEA CON EFECTO UNITARIO

GUILLERMO PALAO MORENO	213
I. Introducción	214
II. Mercado único y derechos de propiedad industrial: superación de derechos nacionales por medio de títulos con efecto unitario	215
1. <i>Derechos de propiedad industrial nacionales y mercado interior</i> .	215
2. <i>La creación de derechos con un alcance unitario</i>	217
III. Tutela judicial internacional de marcas y diseños de la Unión Europea	223
1. <i>Bases para su protección jurisdiccional transfronteriza y coordinación entre instrumentos europeos</i>	224
2. <i>Reglas de competencia judicial internacional aplicables</i>	228
IV. Litigación internacional en materia de patentes europeas con efecto unitario	235
1. <i>El tribunal unificado de patentes</i>	235
2. <i>La determinación de la competencia judicial en la materia</i>	236
V. Valoración	241

CAPÍTULO 7

CONTRATOS DE TRABAJO INTERNACIONAL EN EL SECTOR TECNOLÓGICO: ANÁLISIS DE SUS PRINCIPALES CLÁUSULAS

JOSÉ LUIS IRIARTE ÁNGEL y MARTA CASADO ABARQUERO	243
I. Desafíos jurídicos de la tecnologización de las relaciones laborales	244

	<u>Página</u>
II. La contratación laboral en la industria tecnológica: cláusulas y particularidades	247
III. Cláusulas de confidencialidad y secreto empresarial	248
1. <i>Marco jurídico y conceptual de las cláusulas de confidencialidad y secreto empresarial</i>	248
2. <i>Estructura y contenido habitual de las cláusulas de confidencialidad en el ámbito laboral transnacional</i>	250
IV. Cláusulas de propiedad intelectual e industrial	252
1. <i>Marco jurídico y conceptual de la propiedad intelectual e industrial en el contexto laboral transnacional</i>	252
2. <i>Estructura y contenido habitual de las cláusulas sobre titularidad, cesión y compensación económica</i>	254
V. Cláusulas sobre teletrabajo y derecho a la desconexión	256
1. <i>El marco jurídico transnacional del teletrabajo: pluralidad normativa y lagunas de regulación</i>	256
2. <i>Estructura y contenido habitual de las cláusulas contractuales en el teletrabajo transnacional</i>	258
VI. Cláusulas de uso de dispositivos y control empresarial en los contratos de trabajo internacionales	261
1. <i>El marco jurídico internacional del control empresarial sobre los dispositivos laborales</i>	261
VII. Cláusulas de no competencia y permanencia en los contratos de trabajo internacionales	262
1. <i>Concepto y fundamento jurídico</i>	262
2. <i>Marcos normativos de nuestro entorno y problemas de acomodo entre ellos</i>	263
3. <i>Contenido habitual y criterios de validez</i>	265
VIII. Algunas reflexiones desde el punto de vista del derecho internacional privado	266

CAPÍTULO 8

LA SUCESIÓN *MORTIS CAUSA* DE BIENES DIGITALES: LA RELEVANCIA DE LA LEY APLICABLE A LA SUCESIÓN

ISABEL ANTÓN JUÁREZ	269
I. Aproximación inicial	269
II. El impacto de la vida digital en la sucesión <i>mortis causa</i>: ¿Toda sucesión es internacional?	271
1. <i>Aproximación inicial</i>	271
2. <i>La calificación de la sucesión mortis causa como internacional por la existencia de bienes digitales</i>	272
3. <i>Las normas que regulan la sucesión mortis causa transfronteriza de bienes digitales</i>	275
III. La categorización de los bienes digitales	277
IV. La determinación de la competencia judicial internacional y el derecho aplicable de la sucesión <i>mortis causa</i> de bienes digitales	279
1. <i>El punto de partida</i>	279
2. <i>Los diferentes escenarios</i>	281
3. <i>La determinación del Derecho aplicable bienes personales y mixtos</i>	283
4. <i>Los litigios derivados de la sucesión mortis causa de bienes digi- tales y la determinación del tribunal competente</i>	287
V. Conclusiones	292

CAPÍTULO 9

ARBITRAJE COMERCIAL INTERNACIONAL EN CHILE A MÁS DE VEINTE AÑOS DE APLICACIÓN DE LA LEY MODELO SOBRE LA MATERIA DE LA COMISIÓN DE NACIONES UNIDAS SOBRE EL DERECHO MERCANTIL, ¿VIENTOS DE CAMBIO?

JAIME GALLEGOS ZÚÑIGA	295
I. Consideraciones preliminares	295

	<u>Página</u>
II. La decisión de la Corte Suprema que rompe una tendencia . .	296
III. Orden público y control judicial de lo decidido	307
IV. Orden público en el Derecho Internacional Privado de Chile .	309
V. Contravención del orden público de la sede como causal de anulación del laudo, o del lugar en que se solicita su reconocimiento o ejecución	312
VI. Reflexiones finales	313

CAPÍTULO 10

LOS CONTRATOS DE TRANSPORTE INTERNACIONAL DE MERCANCÍAS. ESPECIAL REFERENCIA A LAS VÍAS AÉREA, MARÍTIMA Y POR CARRETERA

JUAN JOSÉ ÁLVAREZ RUBIO y UNAI BELINTXON MARTÍN	315
I. Consideraciones preliminares	316
II. Rasgos característicos del contrato de transporte internacional de mercancías	319
1. <i>Definición de contrato de transporte internacional</i>	319
2. <i>Los conceptos de remuneración y transportista profesional</i>	320
3. <i>Elementos esenciales del contrato de transporte internacional de mercancías</i>	320
III. El transporte internacional de mercancías por carretera	321
1. <i>Consideración inicial</i>	321
2. <i>Marco jurídico internacional aplicable</i>	322
2.1. El Convenio de Ginebra de 1956 sobre contrato de transporte internacional de mercancías por carretera (CMR)	322
2.2. Ámbito de aplicación del CMR (art. 1)	324
2.3. Competencia judicial internacional y transporte de mercancías por carretera	325

	<i>Página</i>
2.4. La aplicación subsidiaria del RBI bis para determinar la competencia judicial internacional en los contratos internacionales de transporte de mercancías por carretera y la aplicación prioritaria del propio RBI bis para concretar la competencia judicial internacional en los contratos de transporte de viajeros por carretera.	330
IV. El transporte internacional de mercancías aéreo	335
1. <i>Competencia judicial internacional en el convenio de montreal</i> ..	335
1.1. Consideración previa	335
1.2. Los foros objetivos alternativos recogidos en el Convenio de Montreal	338
1.3. Autonomía de la voluntad: el pacto atributivo de jurisdicción y arbitraje	339
V. El transporte internacional de mercancías por mar	341
1. <i>Derecho uniforme y derecho marítimo internacional</i>	341
2. <i>Un problema concreto: los acuerdos atributivos de jurisdicción en el ordenamiento jurídico español</i>	343
VI. Ley aplicable y contratos de transporte internacional de mercancías	355
VII. Bibliografía	366

CAPÍTULO 11

ASPECTOS LEGALES PRÁCTICOS DE LA PUBLICIDAD EMPRESARIAL A TRAVÉS DE INFLUENCERS, A PROPÓSITO DE LA ENTRADA EN VIGOR DEL NUEVO CÓDIGO DE CONDUCTA EN OCTUBRE DE 2025

LERDYS SARAY HEREDIA SÁNCHEZ	373
I. Planteamiento del tema a modo de introducción	374
II. Diferencias entre influencers de las redes sociales (personas físicas) e influencers digitales creados por IA	377
1. <i>¿Quiénes son considerados influencers? Una aproximación conceptual</i>	377

2. <i>El rol de los influencers virtuales en la publicidad empresarial</i> ..	379
III. Respaldo legal de la actividad de los influencers a favor de las empresas en España	383
1. <i>Ley 13/2022, General de Comunicación Audiovisual</i>	386
2. <i>Ley 34/2002, de Servicios de la Sociedad de la Información y de comercio electrónico</i>	390
3. <i>Ley 3/1991, de competencia desleal</i>	392
4. <i>Ley General de Publicidad de 1988</i>	393
5. <i>Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual</i>	395
IV. Papel de la autorregulación de la actividad publicitaria a través de influencers: código de conducta sobre el uso de influencers por parte de las empresas en la publicidad	399
1. <i>La Asociación Autocontrol en España</i>	401
V. La lectura del sistema desde el derecho internacional privado español	403
VI. Ideas finales a modo de conclusiones	405
VII. Bibliografía consultada	407

CAPÍTULO 12

LAS RENOVADAS NECESIDADES DE PROTECCIÓN DE LOS CONSUMIDORES EN EL DERECHO EUROPEO EN LA ACTUAL ERA DIGITAL

LUCAS ANDRÉS PÉREZ MARTÍN y ADA LUCÍA MARISCAL GONZÁLEZ	413
I. Introducción: la evolución futura del derecho de consumidores europeos	414
II. Protección general del consumidor en el derecho internacional privado europeo	416

	<u>Página</u>
1. <i>La protección de los consumidores europeos en la determinación de la competencia judicial internacional</i>	423
2. <i>La protección de los consumidores en la ley aplicable</i>	425
3. <i>Protección de derechos de los consumidores en el lustro 2020-2025</i>	428
III. La protección de los consumidores 2025-2030 en la era digital .	430
IV. La digitalización del comercio de productos financieros y la protección del inversor	435
V. Conclusiones: hacia un nuevo derecho de consumidores europeo	440

CAPÍTULO 13

RESOLUCIÓN DE CONFLICTOS COMERCIALES INTERNACIONALES A TRAVÉS DEL ARBITRAJE, LA MEDIACIÓN Y OTROS MASC EN EL ENTORNO DIGITAL

LYDIA ESTEVE GONZÁLEZ y RICHARD A. MAC BRIDE	443
I. Introducción: los MASC y sus combinaciones ARB-MED, MED-ARB en el comercio internacional del siglo XXI	444
II. Los MASC a la luz de «la Ley 1/2025 de eficiencia procesal» y su aplicación en el ámbito comercial internacional	448
1. <i>Origen contemporáneo del impulso de los MASC: hacia métodos adecuados y eficaces de solución de controversias</i>	448
2. <i>Métodos Adecuados de Solución de Controversias y el requisito de procedibilidad en asuntos comerciales internacionales</i>	449
3. <i>Repercusión de la Ley Orgánica 1/2025 en los conflictos comerciales internacionales</i>	451
III. La práctica del arbitraje comercial internacional	454
1. <i>Planteamiento: Caracteres y clases de arbitraje</i>	454
2. <i>Fuentes reguladoras del arbitraje comercial internacional: características y ventajas</i>	456
3. <i>El convenio arbitral. Efectos, requisitos para su validez e impugnación de la validez del convenio arbitral</i>	460

	<i>Página</i>
4. <i>Procedimiento arbitral y laudo arbitral: Derecho aplicable</i>	461
5. <i>Anulación del laudo arbitral internacional y reconocimiento y ejecución de laudos extranjeros: procedimiento</i>	462
IV. La práctica de la mediación comercial internacional	465
1. <i>Regulación de la mediación internacional/transfronteriza y su significado</i>	465
2. <i>Caracteres, ventajas y clases de la mediación</i>	468
3. <i>La persona mediadora en asuntos de comercio internacional</i>	470
4. <i>Acuerdo de mediación en controversias internacionales. Requisitos de validez y efectos</i>	473
5. <i>Procedimiento de mediación en controversias de comercio internacional. Normativa aplicable y fases del procedimiento</i>	475
6. <i>Acuerdo de resolución de conflictos comerciales internacionales: Derecho aplicable, requisitos y su ejecución extraterritorial</i>	477
V. Resolución alternativa de controversias en línea: on line/ai Dispute Resolution (ODR-AIDR)	479
1. <i>Planteamiento: aumento de transacciones digitales y métodos de solución de conflictos en el entorno digital</i>	479
2. <i>Métodos de ODR/ AIDR más frecuentes en el ámbito del comercio internacional</i>	482
3. <i>Principios rectores de los ODR/ AIDR</i>	484
VI. Conclusión	486

CAPÍTULO 14

LA REGULACIÓN DE LOS CONTRATOS INTERNACIONALES EN ARGENTINA A 10 AÑOS DE LA ENTRADA EN VIGOR DEL CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN

PAULA MARÍA ALL	489
I. Introducción	490
II. La calificación de contrato internacional y su reglamentación .	495

	<i>Página</i>
III. La determinación de la jurisdicción internacional en materia contractual	498
1. <i>El sistema de DIPr de fuente interna argentina</i>	500
IV. La determinación del derecho aplicable	520
1. <i>El rol de la autonomía de la voluntad en el sistema de DIPr de fuente interna</i>	520
2. <i>Los contratos entre ausentes</i>	542
3. <i>El punto de inflexión a la autonomía de la voluntad: los contratos de consumo</i>	543
V. A modo de conclusión	543

CAPÍTULO 15

LOS PROBLEMAS DE Oponibilidad DE LOS Pactos DE SOCIOS EN EL SISTEMA JURÍDICO INTERNACIONAL. COMPARATIVA Y ANÁLISIS DE LOS SISTEMAS ANGLOSAJONES Y DE DERECHO COMPARADO CONTINENTAL

RAQUEL CAYOTOPA, MAX BERRE y RICHARD EDO GÓMEZ	549
I. Introducción	550
II. Naturaleza jurídica de los pactos de socios	552
1. <i>Fundamento normativo y autonomía de la voluntad</i>	552
2. <i>El principio de relatividad contractual y sus límites</i>	552
3. <i>La tensión entre contrato y estatutos</i>	553
4. <i>Pactos como contratos plurilaterales de duración</i>	554
III. España y la regla de la inoponibilidad	555
1. <i>Génesis normativa de la regla en el ordenamiento español</i>	555
2. <i>Doctrina administrativa: la posición de la DGRN/DGSJyFP</i> ...	556
3. <i>Debate doctrinal: pactos omnilaterales, eficacia frente a terceros y flexibilidad</i>	557
IV. Derecho comparado continental	558
1. <i>Italia: pionera en la positivización de los pactos parasociales</i>	558

	<u>Página</u>
2. <i>Francia: prevalencia de la inoponibilidad inter partes</i>	559
3. <i>Portugal: regulación expresa pero conservadora</i>	559
4. <i>Alemania: el reconocimiento jurisprudencial de los contratos de sindicación de voto</i>	560
5. <i>Síntesis comparada: convergencias y divergencias</i>	561
V. El sistema anglosajón	561
1. <i>Estados Unidos</i>	562
2. <i>Reino Unido</i>	563
3. <i>Impacto en el Derecho internacional privado</i>	564
3.1. <i>Reconocimiento y ejecución internacional. Los arbitrajes</i>	565
VI. Discusión comparativa e implicaciones internacionales	569
1. <i>Dos concepciones opuestas de la eficacia contractual</i>	569
2. <i>Implicaciones en operaciones de M&A. La inversión extranjera y el venture capital</i>	569
3. <i>Implicaciones en la valoración de empresas</i>	571
VII. Cuantificación del riesgo y valoración empresarial	571
1. <i>Introducción: el riesgo jurídico como riesgo financiero</i>	571
2. <i>La prima de riesgo contractual</i>	572
3. <i>Impacto en métodos de valoración</i>	572
4. <i>Casos prácticos: impacto en venture capital y M&A</i>	574
5. <i>Interacción con el riesgo país y el riesgo regulatorio</i>	575
VIII. Conclusiones y propuestas de armonización internacional	576
IX. Bibliografía	578

CAPÍTULO 16

CONTRATOS DE ESTADO Y ARBITRAJE DE INVERSIÓN

HUGO CARDONA-CÁRDENAS	581
I. Introducción	581

	<i><u>Página</u></i>
II. Los contratos de inversión como fuente de obligaciones bilaterales	583
III. Evolución y tipos de contratos de inversión	584
1. <i>Concesiones sobre recursos naturales</i>	587
2. <i>Concesiones sobre servicios públicos</i>	588
3. <i>Contratos de construcción, operación y transferencia</i>	589
4. <i>Asociaciones público-privadas</i>	590
IV. Matices del arbitraje transnacional emergente de contratos de inversión	591
V. ¿Responsabilidad internacional del estado por el incumplimiento de contratos de inversión?	593
1. <i>Distinción entre la responsabilidad internacional en base a tratados y a contratos</i>	594
2. <i>Vulneración de cláusulas de estabilización y cláusulas paraguas</i> .	596
3. <i>Aplicabilidad del estándar mínimo de trato a los contratos de inversión</i>	597
VI. Conclusión	598

Ahora bien, a pesar de estos beneficios, el teletrabajo transfronterizo también presenta desafíos, especialmente en términos de cumplimiento normativo y protección de datos. Las empresas deben navegar por un complejo panorama legal, asegurando que cumplen con las regulaciones locales e internacionales para la protección de datos personales. Esto es particularmente relevante en el contexto del RGPD, que tiene implicaciones extraterritoriales y requiere que las empresas implementen medidas robustas para proteger los datos de los ciudadanos de la UE.

II. TELETRABAJO TRANSFRONTERIZO Y APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE

Se considera «teletrabajo transfronterizo» toda actividad que pueda ejercerse desde cualquier lugar y que podría realizarse en los locales o en el domicilio del empleador y que se lleva a cabo en uno o varios Estados miembros distintos de aquel en el que están situados los locales o el domicilio del empresario, y se basa en las tecnologías de la información para permanecer conectado con el entorno de trabajo del empleador o de la empresa, así como con los interesados/clientes, a fin de cumplir las tareas que el empleador o los clientes asignen al trabajador, en el caso de los trabajadores por cuenta propia⁶. Este tipo de teletrabajo no solo redefi-

-
6. *Vid.* Artículo 1.c del Acuerdo marco relativo a la aplicación del apartado 1 del artículo 16 del Reglamento (CE) n.º 883/2004 en los casos de teletrabajo transfronterizo habitual.

Este Acuerdo Marco, firmado por Alemania, Suiza, Liechtenstein, República Checa, Austria, Países Bajos, Eslovaquia, Bélgica, Luxemburgo, Finlandia, Noruega, Portugal, Suecia, Polonia, Croacia, Malta, España y Francia, entró en vigor el 1 de julio de 2023. El Reglamento (CE) n.º 883/2004 se adoptó en un momento en que el teletrabajo no era tan habitual. Sin embargo, dado el incremento del teletrabajo transfronterizo a raíz de la pandemia de Covid-19, el teletrabajo ha pasado a ser, para muchos trabajadores, una forma estructural de trabajo. Por ello se quiere mitigar el efecto del teletrabajo transfronterizo en la legislación aplicable en materia de seguridad social a corto plazo. En relación con su ámbito de aplicación, este Acuerdo Marco abarca a todas las personas a las que pueda aplicarse el artículo 16.1 del Reglamento 883/2004, siempre que su residencia se encuentre en un Estado signatario y la sede o el domicilio de la empresa o empleador esté situado en otro Estado signatario. El Acuerdo se refiere a las personas a las que sería aplicable la legislación del Estado de residencia como consecuencia del teletrabajo transfronterizo habitual en aplicación del artículo 13.1.a) del Reglamento 883/2004 en concordancia con los apartados 8 y 10 de su artículo 14 del Reglamento (CE) n.º 987/2009 y que estén empleadas por una o más empresas o empleadores que tengan su sede o domicilio en un único Estado signata-

ne la relación laboral tradicional, sino que también promueve una mayor integración económica entre países, permitiendo a los trabajadores y las empresas superar barreras geográficas. Por ejemplo, en sectores como la tecnología, el teletrabajo transfronterizo facilita la contratación de profesionales especializados que, de otra forma, no estarían disponibles localmente. Este tipo de trabajo no solo optimiza la productividad y eficiencia, sino que también presenta desafíos significativos en términos de cumplimiento normativo, especialmente en relación con la protección de datos personales. El Reglamento General de Protección de Datos (RGPD) de la UE se aplica extraterritorialmente, lo que significa que las empresas fuera de la UE que procesan datos de ciudadanos de la UE también deben cumplir con sus estrictas regulaciones. Esto incluye la obligación de garantizar que los datos personales transferidos internacionalmente sean protegidos de manera adecuada, utilizando mecanismos como las cláusulas contractuales tipo, las normas corporativas vinculantes o las decisiones de adecuación por parte de la Comisión Europea. Las empresas deben realizar evaluaciones de impacto sobre la protección de datos y establecer políticas claras para manejar los datos personales en el contexto del teletrabajo transfronterizo. La aplicación extraterritorial del RGPD establece un precedente en la gobernanza de datos globales. Este marco normativo obliga a las empresas de países terceros a adoptar medidas de cumplimiento que incluyen la designación de representantes en la UE y la implementación de auditorías periódicas para asegurar que se respeten los derechos de privacidad de los interesados europeos. Además, la creciente demanda de cumplimiento está impulsando el desarrollo de tecnologías de protección de datos, como plataformas automatizadas que monitorean la conformidad en tiempo real.

Las ventajas del teletrabajo (también denominado «trabajo remoto», «trabajo móvil» o «e-trabajo»)⁷ transfronterizo son de sobra conocidas: las

rio distinto (véase el art. 2). Por lo que se refiere a la legislación aplicable, el artículo 3 establece que, previa solicitud, las personas que realicen teletrabajo transfronterizo habitual y estén amparadas por el artículo 2, estarán sujetas, conforme al artículo 16.1 del Reglamento 883/2004, a la legislación del Estado en el que el empresario tenga su sede o su domicilio, siempre que el teletrabajo transfronterizo realizado en el Estado de residencia sea inferior al 50 % del tiempo de trabajo total.

7. Vid. Crawford, J. O., Maccalman, L. & Jackson, C. A. (2011). The health and well-being of remote and mobile workers. *Occupational Medicine*, 61(6), 385-394. La OIT, por su parte, define al teletrabajo como «un nuevo esquema de labor, en un lugar alejado de una oficina central o instalaciones de producción, comercio, servicios, etc., separando al trabajador del contacto personal con colegas y líderes que estén en esa oficina, planta o área comercial». Esto no es más que el teletrabajo integrado con la tecnología,

personas que realizan teletrabajo se esfuerzan más por ver cumplidos sus objetivos y se produce un aumento en el desempeño personal, debido a la presencia de elementos como la flexibilidad de horarios y la autonomía para realizar las actividades⁸. Además, el teletrabajo transfronterizo permite a las empresas acceder a un talento global, lo que puede mejorar la diversidad y la innovación dentro de la organización. Esta diversidad no solo enriquece el entorno laboral con una variedad de perspectivas culturales y experiencias, sino que también puede conducir a soluciones más creativas y efectivas a los problemas empresariales. Las empresas pueden contratar a los mejores talentos sin las limitaciones geográficas tradicionales, lo que es particularmente beneficioso en sectores altamente especializados donde la demanda de habilidades específicas es alta. El acceso al talento global también está transformando las dinámicas salariales. Las empresas pueden optimizar costes al contratar en regiones donde los niveles salariales son más competitivos, mientras que los empleados se benefician de oportunidades laborales que no habrían estado disponibles localmente. Esto crea un equilibrio económico que promueve la equidad y la diversificación en el mercado laboral global.

Sin embargo, esta modalidad también exige a las empresas que se aseguren de que sus empleados tengan acceso a las herramientas tecnológicas adecuadas y a un soporte técnico continuo para mantener la productividad y la seguridad de la información. La inversión en infraestructura tecnológica es fundamental. Esto incluye proporcionar hardware y *software* adecuados, así como garantizar conexiones de internet seguras y confiables. Es crucial que las empresas implementen políticas de ciberseguridad robustas para proteger la información sensible contra posibles amenazas y brechas de seguridad. La formación en ciberseguridad para los empleados es igualmente importante, ya que ellos son la primera línea de defensa contra los ciberataques. Además de proporcionar soporte técnico, las empresas deben desarrollar estrategias de recuperación ante incidentes que incluyan planes de continuidad del negocio y sistemas de respaldo de datos. Estas medidas son esenciales para mitigar el impacto de posibles ciberataques y garantizar que las operaciones puedan continuar sin interrupciones significativas.

lo que hace posible la separación laboral, facilitando así la comunicación entre los diferentes niveles de una compañía, de una empresa o de una institución u organismo de la administración.

8. Vid. Hamilton, E. (2002). *Bringing Work Home: Advantages and Challenges of Telecommuting* (pp. 1-32). Boston College.

La implementación de prácticas efectivas de gestión de equipos virtuales es esencial para maximizar los beneficios del teletrabajo y minimizar sus posibles desventajas. Esto incluye la realización de reuniones regulares, que no solo ayudan a mantener a todos informados y alineados con los objetivos de la empresa, sino que también fomentan un sentido de comunidad y colaboración entre los empleados. Las plataformas colaborativas como *Google Meet*, *Microsoft Teams*, *Slack* o *Zoom* pueden jugar un papel crucial en este aspecto, facilitando la comunicación y el intercambio de información en tiempo real. Asimismo, la integración de herramientas avanzadas de análisis y gestión de proyectos, como *Asana* o *Monday.com*, permite a los equipos monitorear el progreso de las tareas de manera eficiente. Estas plataformas ofrecen transparencia en tiempo real y fomentan una mayor responsabilidad entre los miembros del equipo.

La formación continua es otro componente crítico. En un entorno de trabajo en constante cambio, es vital que los empleados mantengan sus habilidades actualizadas. Las empresas deben ofrecer programas de desarrollo profesional que incluyan capacitación en nuevas tecnologías, habilidades de gestión del tiempo y estrategias de comunicación efectiva. Esto no solo mejora la competencia y eficiencia de los empleados, sino que también aumenta su satisfacción y lealtad hacia la empresa.

Además, es importante que las empresas desarrollen una cultura de confianza y responsabilidad. En el teletrabajo, los empleados disfrutan de una mayor autonomía, pero esto debe ir acompañado de un claro entendimiento de las expectativas y objetivos. La fijación de metas claras y la evaluación regular del desempeño ayudan a asegurar que todos estén trabajando hacia los mismos fines. Una cultura de confianza también se refuerza mediante políticas de reconocimiento y recompensas para aquellos empleados que destacan en entornos remotos. Estas prácticas no solo motivan a los equipos, sino que también fomentan un sentido de pertenencia y compromiso organizacional.

El bienestar de los empleados también debe ser una prioridad. El teletrabajo puede difuminar las líneas entre la vida laboral y personal, lo que puede llevar al agotamiento.

Siendo conscientes de que el marco normativo es generalista y, además, es imposible que se ofrezcan respuestas concretas a la multitud de casos particulares que se plantean, dada la velocidad a la que se producen los cambios y la evolución de las nuevas tecnologías, es necesario crear un acervo de conocimientos que recoja los retos a los que se enfrentan los

operadores jurídicos y ofrecer soluciones prácticas a los operadores de distintos ámbitos en esta materia. Estos retos incluyen la necesidad de adaptarse rápidamente a los avances tecnológicos, la complejidad de coordinar múltiples jurisdicciones con diferentes normativas y la implementación efectiva de medidas de seguridad para proteger los datos personales. Este marco generalista, aunque esencial para proporcionar una base común, a menudo genera lagunas normativas que dificultan la aplicación uniforme en contextos específicos. Por ejemplo, en situaciones de teletrabajo transfronterizo, las empresas deben coordinar el cumplimiento de normativas contradictorias entre jurisdicciones. Esto exige un enfoque colaborativo entre reguladores nacionales e internacionales para garantizar que las leyes evolucionen al ritmo de los avances tecnológicos. Además, se debe considerar el impacto del teletrabajo en la privacidad de los empleados y la responsabilidad de las empresas en garantizar un entorno seguro para la gestión de información sensible. El objetivo principal que persigue este trabajo es arrojar luz sobre algunas de las cuestiones jurídicas que se observan por las circunstancias excepcionales actuales, en particular, el teletrabajo transfronterizo y la aplicación extraterritorial del RGPD⁹. La privacidad de los empleados es una preocupación creciente, especialmente en un entorno de teletrabajo donde las herramientas digitales pueden monitorear actividades laborales. Esto requiere un equilibrio cuidadoso entre la supervisión empresarial y el respeto a la privacidad individual, garantizando que cualquier monitorización sea proporcional, transparente y conforme a las normativas aplicables. Esto requiere un enfoque flexible y adaptable por parte de los legisladores y reguladores, quienes deben considerar la creación de marcos normativos que no solo protejan los derechos de los individuos, sino que también permitan a las empresas innovar y operar eficientemente en un mercado global. La flexibilidad normativa es crucial para responder adecuadamente a los desafíos emergentes y proporcionar un entorno legal que apoye el crecimiento y la competitividad empresarial. Un ejemplo de esta flexibilidad puede observarse en el reciente marco de cooperación entre la Unión Europea y Japón para la transferencia de datos personales, que combina estrictas salvaguardias de privacidad con procedimientos simplificados para las empresas que cumplen con estándares mutuamente reconocidos. Este tipo de iniciativas demuestra cómo los marcos adaptativos pueden facilitar el comercio global sin comprometer los derechos

9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 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 (Reglamento General de Protección de Datos).

fundamentales. Sin embargo, para maximizar estos beneficios, es crucial que las empresas comprendan y cumplan con el RGPD, que establece estándares rigurosos para la protección de datos personales. La aplicación extraterritorial del RGPD asegura que los derechos de los individuos estén protegidos, sin importar dónde se procesen sus datos. El cumplimiento del RGPD también refuerza la confianza del consumidor, que es un factor clave en la economía digital actual. Los estudios han demostrado que las empresas que implementan medidas estrictas de privacidad y seguridad tienden a atraer más clientes, destacándose frente a competidores que priorizan menos estos aspectos. Para lograr esto, las empresas deben implementar herramientas y estrategias de cumplimiento, como las cláusulas contractuales tipo, las normas corporativas vinculantes y la adopción de tecnologías de cifrado y anonimización de datos. También es fundamental realizar auditorías regulares y formaciones continuas para los empleados sobre la gestión de datos y las mejores prácticas de ciberseguridad, con el objeto de legitimar las transferencias internacionales de datos entre miembros de un mismo grupo empresarial. Además, la implementación de sistemas automatizados de gestión de datos puede simplificar el monitoreo del cumplimiento normativo, identificando rápidamente posibles brechas o riesgos. Estos sistemas pueden integrarse con tecnologías de inteligencia artificial para analizar grandes volúmenes de datos en tiempo real, ayudando a las empresas a responder con mayor rapidez a cambios regulatorios o incidentes de seguridad.

III. TELETRABAJO TRANSFRONTERIZO Y MECANISMOS ADECUADOS PARA LEGITIMAR TRANSFERENCIAS INTERNACIONALES DE DATOS

El aumento de las transferencias internacionales de datos personales en áreas tales como la de los recursos humanos, los servicios financieros, la banca, la educación, el comercio electrónico, el auxilio judicial internacional o la investigación en el área de la salud son ahora una parte integral de la economía globalizada¹⁰. Estas transferencias han transformado las dinámicas operativas de las empresas, permitiéndoles optimizar sus operaciones a nivel global. Sin embargo, también han planteado interrogantes

10. *Vid.*, en particular, García del Poyo, R. & Gari, F. (2007). Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales. *Revista Española de Protección de Datos*, (2), 239-266; y Fernández López, J.M. (2007). Movimiento internacional de datos y buen gobierno corporativo. *Boletín del Ilustre Colegio de Abogados de Madrid*, (35), 3.ª ép., p. 177.

significativos en materia de cumplimiento normativo y protección de los derechos de los interesados. Este fenómeno exige una atención especial por parte de las empresas y reguladores para evitar brechas de seguridad y garantizar la legitimidad de los flujos de datos.

El crecimiento de los flujos internacionales de información ha multiplicado las solicitudes de autorización de transferencias internacionales de datos de carácter personal: comunicaciones de datos personales entre las filiales de una empresa multinacional, utilización de herramientas multiacceso, prestación de servicios desde distintos países, o la gestión integral de los procesos de recursos humanos de una multinacional, están a la orden del día. Las solicitudes de transferencia no solo han aumentado en volumen, sino también en complejidad, debido a la proliferación de tecnologías avanzadas como la inteligencia artificial y el análisis de grandes volúmenes de datos. Estas tecnologías requieren un tratamiento masivo y continuo de datos personales, lo que amplifica los riesgos asociados y refuerza la necesidad de garantías legales robustas.

Los principales sectores de actividad en que operan las entidades exportadoras de datos son telecomunicaciones, energía, servicios informáticos, banca, industria química y farmacéutica, y publicidad directa. El conjunto de estos factores pone de manifiesto que se están produciendo decisiones empresariales autónomas que llevan consigo un fenómeno de deslocalización de actividades empresariales en estos sectores y países, para las que la obtención de una autorización de transferencia internacional de datos es un elemento instrumental necesario desde el punto de vista legal¹¹. La deslocalización de actividades, impulsada por la búsqueda de optimización de costes y acceso a mercados especializados, ha hecho que las empresas dependan aún más de las transferencias internacionales de datos. En este contexto, garantizar la seguridad y la legalidad

-
11. Las transferencias internacionales de datos responden a diversos objetivos que se pueden diferenciar entre: *a)* Aquellas relacionadas con la gestión empresarial en un contexto global. Las empresas multinacionales requieren la realización de transferencias internacionales de datos para finalidades tales como la gestión, mantenimiento y soporte técnico de los sistemas de información (sobre todo en relación con la gestión eficiente de los recursos humanos, los clientes y los proveedores, así como la prestación de servicios de apoyo administrativo en relación con estos); y *b)* Aquellas relacionadas con la atención telefónica a los clientes y otras acciones de marketing telefónico dirigidas a mejorar el grado de satisfacción de los mismos, como la gestión centralizada de los servicios de atención al cliente. En este grupo destacan principalmente las prestaciones de servicios de atención al cliente o *telemarketing*.

de estas transferencias es fundamental para mantener la confianza de los clientes y socios comerciales, así como para cumplir con los requisitos regulatorios.

En efecto, atendiendo a la modalidad, objeto y destino de las transferencias internacionales de datos autorizadas, destacan tres fenómenos interrelacionados donde debemos extremar la protección tuitiva del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: 1) que la principal modalidad de transferencia es la que se lleva a cabo entre un responsable ubicado en España, principalmente dedicado a servicios de telecomunicaciones, y una empresa prestadora de servicios en un tercer país (= encargado del tratamiento de datos), al amparo de las cláusulas contractuales tipo previstas en el RGPD, 2) la diversificación de las áreas geográficas a las que se transfiere los datos personales: los EE.UU. siguen siendo el primer importador de datos desde España y los países latinoamericanos se consolidan en segunda posición (principalmente, México, Argentina, Chile, Colombia, Perú, Paraguay y Uruguay). Pero han aparecido nuevos países de destino de las transferencias en Asia, destacando India, que en los últimos años ha triplicado el número de expedientes tramitados y tiende a convertirse en uno de los principales importadores de datos personales. También ha aumentado el número de autorizaciones con destino a Marruecos; y, 3) que las transferencias autorizadas corresponden, en un alto porcentaje, a prestaciones de servicios que se realizan en terceros países, lo que es indicativo de la importancia que va adquiriendo la deslocalización de actividades que se externalizan en dichos países¹². La diversificación de los destinos geográficos plantea nuevos desafíos en términos de armonización normativa y adaptación a marcos regulatorios locales. Por ejemplo, mientras que los países de América Latina han avanzado en la adopción de normativas de protección de datos similares al RGPD, regiones como Asia presentan una heterogeneidad significativa, desde legislaciones avanzadas como la

12. Desde la perspectiva española, las categorías de transferencias internacionales de datos de carácter personal son, en la práctica, de tres tipos: *a)* Transferencias de datos personales derivadas de la optimización de la gestión de recursos por una empresa, cuya matriz, española o central, se halla en un país extranjero; *b)* Transferencias de datos personales ligadas a la naturaleza de la actividad o producto (p. ej., reservas de billetes de avión o de plazas hoteleras en el extranjero contratadas a través de agencias de viajes en España); y, *c)* Transferencias de datos personales destinadas a mejorar el servicio al cliente (p. ej., en los casos en los que se encarga el tratamiento de datos a un tercero en el extranjero, cuya gestión permitirá que el servicio que se presta al cliente sea más eficaz).

de Japón hasta marcos legales menos definidos como los de algunos países del sudeste asiático.

Y en este contexto es donde debemos observar los diferentes mecanismos que el RGPD proporciona para la realización de las transferencias de datos desde el Espacio Económico Europeo (EEE) a países terceros. Nos referimos, en particular, a los siguientes:

- A) Mediante una decisión de adecuación de la Comisión Europea se puede declarar que un Estado no perteneciente al EEE ofrece un nivel de protección de datos adecuado, lo cual significa que se pueden transferir datos a una entidad de ese Estado no perteneciente al EEE sin que el exportador de los datos deba ofrecer más garantías o esté sujeto a condiciones adicionales. En otras palabras, las transferencias a ese tercer país se asimilarán a una transmisión de datos dentro del EEE. Estas decisiones de adecuación son fundamentales para establecer un marco de confianza entre las partes implicadas en la transferencia de datos. Actualmente, países como Japón, Suiza y Nueva Zelanda han obtenido esta designación, lo que ha facilitado enormemente el comercio y la cooperación internacional. Sin embargo, el proceso para obtener dicha decisión es riguroso y requiere que el país candidato demuestre que su legislación garantiza un nivel de protección de datos equivalente al del RGPD.
- B) A falta de una decisión de adecuación, la transferencia puede hacerse mediante el establecimiento de garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Tales garantías adecuadas incluyen, entre otras:
 - a) En el caso de los grupos empresariales o la unión de empresas dedicadas a una actividad económica conjunta, las empresas pueden transferir los datos personales basándose en las denominadas «Normas Corporativas Vinculantes».
 - b) Acuerdos contractuales con el destinatario de los datos personales que utilizan, por ejemplo, las cláusulas contractuales tipo aprobadas por la Comisión Europea.
 - c) La adhesión a un código de conducta o un mecanismo de certificación junto con compromisos vinculantes y exigibles asumidos por el destinatario en relación con la aplicación de las garantías adecuadas para la protección de los datos transferidos.

Entre estas garantías, las Normas Corporativas Vinculantes (BCR) destacan por su aplicabilidad en empresas multinacionales. Estas normas no solo permiten transferencias fluidas dentro del mismo grupo empresarial, sino que también refuerzan la confianza interna al establecer directrices claras para el manejo de datos personales. Por otro lado, las cláusulas contractuales tipo se han convertido en una herramienta ampliamente adoptada para relaciones comerciales externas, ya que proporcionan una base legal uniforme para las transferencias de datos.

Asimismo, los códigos de conducta y los mecanismos de certificación representan un enfoque innovador para garantizar el cumplimiento normativo. Estas herramientas permiten a las empresas demostrar de manera proactiva su compromiso con la protección de datos, facilitando las relaciones con socios internacionales y reduciendo los riesgos regulatorios.

- C) Por último, si se prevé realizar una transferencia de datos personales a un tercer país que no está sujeto a una decisión de adecuación y en ausencia de garantías adecuadas, se puede realizar la transferencia basándose en varias excepciones para situaciones específicas, por ejemplo, cuando una persona haya consentido explícitamente a la transferencia propuesta tras haber recibido toda la información necesaria sobre los riesgos relacionados con dicha transferencia.

Las excepciones contempladas en el RGPD son esenciales para casos donde las transferencias son inevitables, pero los mecanismos formales no pueden aplicarse. Sin embargo, estas excepciones deben usarse con precaución y solo en situaciones claramente justificadas. Por ejemplo, el consentimiento explícito del interesado debe ser informado y documentado de manera exhaustiva, dejando constancia de que la persona comprende plenamente los riesgos asociados.

Además del consentimiento, otras excepciones incluyen transferencias necesarias para la ejecución de un contrato entre el interesado y el responsable del tratamiento, o por razones importantes de interés público, como investigaciones científicas internacionales o cooperación en justicia penal. Estas excepciones permiten cierta flexibilidad, pero exigen que las empresas implementen medidas adicionales para minimizar los riesgos inherentes a estas transferencias.

De los mecanismos mencionados, las Normas Corporativas Vinculantes constituyen el mecanismo frecuentemente utilizado por las empresas para legitimar las transmisiones de datos entre miembros de un mismo grupo empresarial, dado que se encuentran diseñadas para ser una solución global para empresas multinacionales al garantizar que las transferencias intragrupo se realicen en cumplimiento de las normas respectivas. Las NCV ofrecen una herramienta versátil y adaptable para abordar los desafíos inherentes al tratamiento de datos en múltiples jurisdicciones. No obstante, su implementación requiere un compromiso significativo por parte de las empresas, dado que estas deben demostrar ante las autoridades de control que han adoptado medidas exhaustivas para proteger los derechos de los interesados. Esto incluye garantizar la transparencia, establecer procedimientos de resolución de disputas accesibles y proporcionar garantías contractuales para todas las partes implicadas en la transferencia de datos.

Suponiendo que un grupo empresarial cuenta con Normas Corporativas Vinculantes aprobadas por una Autoridad de Control de un Estado miembro, no existen dudas de que se encuentra habilitado para transferir datos de los titulares residentes en el Espacio Económico Europeo a empresas/filiales del mismo grupo en países terceros; pero, no podrá transferir datos de residentes en países fuera del EEE basándose en las mismas Normas Corporativas Vinculantes, puesto que este mecanismo es considerado válido tan sólo en países donde el RGPD resulta de aplicación y alguno otro país cuya legislación local también así lo considere (por ejemplo, Argentina¹³). En este sentido, la falta de armonización global en materia de protección de datos sigue siendo un obstáculo significativo para las empresas multinacionales. Incluso en países con normativas avanzadas, como Argentina o Japón, las NCV pueden ser insuficientes si no se ajustan a las particularidades locales. Este desajuste subraya la necesidad de un enfoque global coordinado para abordar las discrepancias normativas y facilitar flujos de datos internacionales seguros. En estos casos, el Delegado de Protección de Datos del grupo deberá, antes de realizar la transferencia, hacer una evaluación de la normativa local para saber qué requisitos existen para la realización de transferencias internacionales. Los requisitos pueden ser bastante dispares dependiendo del país al que queremos realizar la transferencia. A título de ejemplo, en China —a partir de un determinado umbral— se necesita no sólo una autorización de la Autoridad de Control, también se exige además que los datos se encuentren alojados localmente

13. Vid. Resolución n.º 159/2018 de la Agencia de Acceso a la Información Pública.

antes de ser transferidos. En Botsuana la Autoridad de Control acaba de publicar una lista de 45 países para los cuales se pueden transferir datos y queda prohibido realizar transferencias a países que no estén en dicha lista. En definitiva, la casuística es muy amplia y necesariamente hay que consultar la normativa local. Este proceso de evaluación no solo incrementa la carga administrativa para las empresas, sino que también puede ralentizar significativamente las operaciones comerciales internacionales. Además, la creciente tendencia de algunos países a requerir almacenamiento local de datos plantea desafíos logísticos y económicos. Las empresas deben decidir si establecer centros de datos locales o buscar soluciones tecnológicas que les permitan operar dentro de estas restricciones sin comprometer la eficiencia operativa.

Para un grupo empresarial con filiales y teletrabajadores dispersos por todo el mundo, esta realidad puede traer algunos problemas. Creo que caben pocas dudas de que el acceso por un teletrabajador residente en Rusia a datos de clientes o empleados de otra entidad del grupo, con el propósito de realizar sus funciones de control financiero supone una transferencia internacional de datos. El *European Data Protection Board* —Comité Europeo de Protección de Datos— (EDPB) considera, sin embargo, que si el acceso es realizado por parte de un teletrabajador que se encuentra en el país de forma temporal, en un viaje de negocios, no constituye una transferencia internacional¹⁴. Esta distinción entre acceso temporal y permanente subraya la necesidad de criterios claros para definir lo que constituye una transferencia internacional de datos en el contexto del teletrabajo. Las empresas deben establecer políticas internas que detallen las condiciones bajo las cuales se permite el acceso a datos desde ubicaciones internacionales, y asegurarse de que estas políticas sean consistentes con las normativas locales e internacionales aplicables.

14. *Vid.* Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, page 6, Example 5: Employee of a controller in the EU travels to a third country on a business trip. George, employee of A, a company based in Poland, travels to India for a meeting. During his stay in India, George turns on his computer and accesses remotely personal data on his company's databases to finish a memo. This remote access of personal data from a third country, does not qualify as a transfer of personal data, since George is not another controller, but an employee, and thus an integral part of the controller (company A). Therefore, the disclosure is carried out within the same controller (A). The processing, including the remote access and the processing activities carried out by George after the access, are performed by the Polish company, i.e. a controller established in the Union subject to Article 3(1) of the GDPR.

Si los clientes/teletrabajadores residen en el EEE, las Normas Corporativas Vinculantes son un mecanismo válido. Pero ¿qué ocurre en el caso de que los clientes/empleados sean residentes en un país que no permite la transferencia de datos a Rusia por considerar que el país no ofrece garantías suficientes? En ese caso no se podrá realizar la transferencia y el trabajador en Rusia no podrá acceder a datos para realizar sus funciones. Estas limitaciones pueden obstaculizar significativamente las operaciones diarias de las empresas multinacionales. En sectores críticos como el financiero o el sanitario, donde los datos son esenciales para la toma de decisiones en tiempo real, estas restricciones pueden generar ineficiencias operativas y aumentar los costes asociados con el cumplimiento normativo.

Las Normas Corporativas Vinculantes no son un mecanismo válido en países donde no las reconocen como tal y, por lo tanto, para legitimar la transferencia de datos personales de residentes en países fuera del EEE, tenemos que analizar cómo se encuentran reguladas las transferencias internacionales en la ley local. En estos casos, la capacidad de las empresas para operar de manera efectiva en mercados globales dependerá de su capacidad para adaptarse rápidamente a las normativas locales. Esto incluye no solo cumplir con los requisitos legales existentes, sino también anticiparse a cambios regulatorios que puedan impactar sus operaciones. Es innegable que las Normas Corporativas Vinculantes no son un mecanismo válido en países donde no las reconocen como tal y, por lo tanto, cuando hablamos de datos personales de residentes en países fuera del EEE, si queremos legitimar la transferencia, tenemos que analizar cómo se encuentran reguladas las transferencias internacionales en la ley local. Y es bastante difícil que determinados países permitan la transferencia a países en los que los Gobiernos no ofrezcan garantías suficientes, tales como China o Rusia. Esto puede afectar la actividad del grupo empresarial y, en definitiva, la forma en que algunas empresas facilitan a los llamados nómadas digitales trabajar desde cualquier punto del mundo. Una práctica que, sobre el papel, es sin duda tentadora, sobre todo para los jóvenes, pero que en la práctica no está exenta de riesgos de diversa índole que no se deben ni minimizar ni, por supuesto, obviar. Hacerlo es colocarse en el punto de mira de las Autoridades de Control, con todo lo que eso conlleva.

En definitiva, así las cosas, una multinacional, en un contexto de teletrabajo transfronterizo, con clientes y teletrabajadores dispersos por el mundo, necesitará contar con un equipo dinámico que sea capaz de mantener un programa de privacidad robusto que garantice el cumplimiento

normativo en todos los países donde tiene actividad¹⁵. Este equipo debe estar compuesto por expertos legales, técnicos y operativos que trabajen de manera conjunta para implementar soluciones innovadoras que permitan gestionar eficazmente las transferencias internacionales de datos. Además, es fundamental establecer mecanismos internos de auditoría y formación continua para garantizar que todos los empleados comprendan y cumplan con las políticas de privacidad de datos aplicables.

IV. LA APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y SUPUESTOS DE TELETRABAJO TRANSFRONTERIZO

Siendo conscientes de la aplicación del RGPD a entornos de teletrabajo transfronterizo, con transferencias internacionales de datos personales y clientes y teletrabajadores dispersos de por medio. En estos contextos transfronterizos el RGPD se convierte en «ley de policía», desde la perspectiva de la UE, tanto en aquellos supuestos en que el teletrabajador trabaja en la UE, como en aquellos casos en los que el teletrabajador se encuentra en un tercer Estado, pero el empleador tiene su centro de trabajo en la UE. Y esto es así por la introducción de reglas específicas de extraterritorialidad en la aplicación del RGPD. Estas reglas, que se encuentran en el apartado 2 del artículo 3 del RGPD, establecen una serie de supuestos en los que responsables o encargados del tratamiento de datos personales que estén ubicados fuera de la UE pueden quedar sujetos a las reglas establecidas en el RGPD, a la monitorización de los tratamientos por parte de las autoridades de los Estados miembros de la UE y a su régimen sancionador. Esta aplicación extraterritorial del RGPD no solo busca proteger los derechos fundamentales de los interesados residentes en la UE, sino también garantizar una competencia justa entre empresas europeas y extranjeras. Al requerir que todas las entidades que operan con datos de ciudadanos de la UE cumplan con las mismas normas, se evita que empresas no comunitarias puedan beneficiarse de un marco regulatorio más laxo en su país de origen. Esto es especialmente relevante en sectores donde la digitalización ha eliminado las barreras tradicionales de entrada al mercado, permitiendo que empresas de cualquier lugar del mundo ofrezcan bienes y servicios a clientes europeos sin necesidad de tener presencia física en la región.

15. Vid. Yañez, S. (2022). El teletrabajo y las transferencias internacionales de datos. *LA LEY Privacidad*, (13), 1-5.

El artículo 3 del RGPD señala lo siguiente respecto de su ámbito de aplicación territorial: «1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. 3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público». La introducción de estas reglas de aplicación extraterritorial en el RGPD confirma una tendencia que ya se estaba consolidando en la UE y que implicaba una creciente exigibilidad del cumplimiento de las normas de protección de datos europeas a aquellas entidades que, con independencia de su ubicación y nacionalidad, llevaban a cabo actividades empresariales en la UE con acceso a, y tratamiento de, datos personales de ciudadanos de la UE. Esta tendencia interpretativa trae su causa en la digitalización cada vez más evidente de muchos sectores y negocios, lo que facilita enormemente el acceso al mercado de usuarios finales europeos a entidades extracomunitarias sin que tengan necesidad de ubicarse en la UE. Tendencia que ya puso de manifiesto el propio TJUE, en el caso *Google vs. Costeja*, cuando amplió, *de facto*, el ámbito de aplicación territorial de las normas europeas a entidades ubicadas fuera de la UE.

La formulación de esa norma implica, a la luz de la jurisprudencia del TJUE en los asuntos *Google Spain* y *Weltimmo*, que «*with a view to fulfilling the objective of ensuring effective and complete protection, the meaning of “in the context of the activities of an establishment” cannot be interpreted restrictively*» (*Guidelines*, p. 6), lo que implica que la entidad no establecida deba cumplir con el RGPD siempre que exista «*an inextricable link between the activities of an EU establishment and the processing of data carried out by a non-EU controller*» (*Guidelines*, p. 7)¹⁶.

16. Vid. De Miguel Asensio, P. (2019). Ámbito de aplicación territorial del Reglamento UE sobre protección de datos: casos difíciles. Pedro de Miguel Asensio. <https://pedrode-miguelasensio.blogspot.com/2019/04/ambito-de-aplicacion-territorial-del.html>.

El ámbito de aplicación territorial «natural» del RGPD, en virtud de su artículo 3.1, es claro: el RGPD será de aplicación a aquellos tratamientos de datos personales que se realicen «en el contexto de las actividades de un establecimiento» del responsable o del encargado en la UE. No se exige, por tanto, la existencia de una u otra entidad con una forma jurídica concreta, sino de un «establecimiento» en la UE; entendiendo por el mismo el ejercicio de manera efectiva y real (aunque sea de forma mínima) de una actividad «a través de modalidades estables», con independencia de que el tratamiento de los datos —su recogida, almacenamiento, etc.— tenga lugar en la UE o no.

Esta interpretación extensiva del concepto de «establecimiento» ha sido confirmada tanto por el TJUE (p. ej., en el caso C-230/14, *Weltimmo vs. NAIH*) como por el Comité Europeo de Protección de Datos (*European Data Protection Board* o «EDPB»), en su Guía 3/2018 sobre la aplicación territorial del RGPD. Por ello, no es posible excluir de la aplicación del RGPD aquellos tratamientos de datos que responsables o encargados europeos, con teletrabajadores transfronterizos, realicen fuera de la UE, bien porque la actividad empresarial o profesional se ejecute y tenga lugar fuera de la UE, o bien porque los datos se ubiquen y almacenen fuera de la UE.

Analizado el ámbito de aplicación territorial «natural» del RGPD, conviene analizar las reglas propiamente de aplicación extraterritorial, que buscan de forma expresa la aplicación de la norma europea —que exigirá a dicha organización una adaptación significativa de procedimientos y sistemas que conllevará la dedicación, esfuerzos y recursos organizativos y económicos— a responsables o encargados no nacionales de Estados miembros de la UE. Nos encontramos entonces ante la posible aplicación del RGPD a organizaciones no europeas, incluso en el caso de que estas organizaciones no cuenten con establecimiento alguno en la UE. Además, esta interpretación amplia permite al RGPD proteger no solo los derechos fundamentales de los interesados, sino también garantizar un marco de competencia equitativo entre las empresas establecidas dentro y fuera del territorio europeo. La existencia de modalidades estables de actividad empresarial en la UE se convierte en un criterio determinante, incluso si las operaciones relacionadas con el tratamiento de datos tienen lugar fuera de las fronteras europeas. Así, un caso típico podría ser el de una sucursal o representante comercial que opera en Europa pero cuyas operaciones de tratamiento de datos, como el análisis de comportamiento de clientes o la gestión de inventarios, se efectúan en servidores ubicados en un tercer país. En tales situaciones, el RGPD asegura que las normas europeas sobre

privacidad prevalezcan independientemente de la ubicación física de los datos o los procesos.

Esta interpretación extensiva del concepto de «establecimiento» ha sido confirmada tanto por el TJUE (p. ej., en el caso C-230/14, *Weltimmo vs. NAIH*) como por el Comité Europeo de Protección de Datos (European Data Protection Board o «EDPB»), en su Guía 3/2018 sobre la aplicación territorial del RGPD. Por ello, no es posible excluir de la aplicación del RGPD aquellos tratamientos de datos que responsables o encargados europeos, con teletrabajadores transfronterizos, realicen fuera de la UE, bien porque la actividad empresarial o profesional se ejecute y tenga lugar fuera de la UE, o bien porque los datos se ubiquen y almacenen fuera de la UE. Estas reglas extraterritoriales, contenidas principalmente en el artículo 3.2 del RGPD, imponen obligaciones específicas a cualquier organización no establecida en la Unión Europea pero que ofrezca bienes o servicios a residentes de la UE, o monitorice su comportamiento dentro del territorio europeo. Este enfoque es particularmente relevante en el contexto del comercio digital y el teletrabajo transfronterizo, donde las interacciones entre empresas y consumidores a menudo trascienden las fronteras nacionales. Por ejemplo, una plataforma de comercio electrónico con sede en Asia que ofrece productos a consumidores europeos, o una consultora estadounidense que utiliza análisis de datos para monitorizar tendencias en el mercado europeo, quedarían sujetas al RGPD bajo estas disposiciones.

Los casos en los que el apartado 2 del artículo 3 del RGPD determina que será de aplicación el RGPD de manera extraterritorial a tratamientos de datos personales de interesados que residan en la UE por parte de cualquier responsable o encargado no establecido en la UE son los siguientes: a) cuando el tratamiento de los datos esté relacionado con la oferta de bienes o servicios a interesados en la UE, independientemente de si a estos se les requiere su pago —esto es, cuando el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la UE—; o b) cuando el tratamiento de los datos esté relacionado con el control del comportamiento de los interesados, en la medida en que este tenga lugar en la UE.

En este sentido, el considerando 23 del RGPD aporta un interesante criterio interpretativo cuando señala que la mera accesibilidad del sitio web del responsable o encargado (o de un intermediario), de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable, no

bastarían para determinar esa intención de la organización no europea de ofrecer los bienes y servicios en la UE. Sin embargo, el propio considerando 23 apunta que hay factores, considerados solos o conjuntamente, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la UE, que pueden revelar que el responsable del tratamiento sí proyecta y tiene la intención de ofrecer bienes o servicios a interesados en la UE. La Guía del EDPB proporciona criterios interpretativos adicionales y ejemplos concretos respecto a qué se entiende por oferta de bienes y servicios en el sentido del artículo 3.2.a) del RGPD.

No cabe duda de que la jurisprudencia del TJUE en relación con el uso del criterio de las actividades dirigidas en el actual artículo 17.1.c) del Reglamento 1215/2012 (Reglamento «Bruselas I bis») y en el artículo 6 del Reglamento «Roma I», en especial, por el momento, su conocida sentencia en los asuntos *Hotel Alpenhof* y *Pammer*, es relevante a estos efectos. En todo caso, conviene no perder de vista que la aplicación de estas normas requiere la presencia de ciertas circunstancias a las que, en principio, no se subordina la aplicación del RGPD en virtud del artículo 3.2. Basta tener en cuenta que esas normas del Reglamento «Bruselas I bis» y del Reglamento «Roma I» exigen la previa celebración de un contrato entre el consumidor y el profesional, así como que, por ejemplo, el régimen de protección del artículo 6 RRI no es aplicable cuando se trate de contratos de prestación de servicios en los que los servicios deban prestarse al consumidor exclusivamente en un país distinto al de su residencia habitual¹⁷.

Una pregunta recurrente al analizar estas cuestiones es a qué se refiere el artículo 3 del RGPD al referirse a «interesados en la Unión» como sujetos respecto de los que el tratamiento de sus datos personales activaría la aplicabilidad del RGPD. La duda más recurrente sobre este aspecto es si el RGPD se refiere a ciudadanos nacionales de Estados miembros de la UE, si basta con que tengan estatus jurídico de residentes en el territorio de la UE con independencia de su nacionalidad o si basta con que los interesados se encuentren localizados «en» la UE con independencia de su estatus jurídico. En este sentido, el RGPD parece referirse a ciudadanos localizados en la UE, puesto que no sujeta la aplicación de la norma a un

17. Vid. De Miguel Asensio, P. (2019). Ámbito de aplicación territorial del Reglamento UE sobre protección de datos: casos difíciles. Pedro de Miguel Asensio. <https://pedrode-miguelasensio.blogspot.com/2019/04/ambito-de-aplicacion-territorial-del.html>.

requisito de nacionalidad o residencia legal. Esta interpretación amplia ha sido confirmada en la Guía. Esta precisión adquiere relevancia en contextos donde el flujo transfronterizo de datos personales puede implicar a personas que no cumplen con un estatus tradicional de residencia o ciudadanía, pero cuya actividad o presencia en el territorio europeo genera la aplicación del RGPD. Por ejemplo, en casos de turistas o viajeros de negocios que se encuentren temporalmente en la UE y cuyos datos personales sean tratados por organizaciones locales o extranjeras que operan en la Unión, el RGPD será aplicable debido a su localización física en el territorio europeo. La precisión es relevante, por ejemplo, en la medida que existen ciudadanos nacionales de un Estado miembro que residen fuera de la UE y, en muchos casos, organizaciones no europeas se plantean si el tratamiento de los datos de esos nacionales europeos residentes en el país de origen del propio responsable (p. ej., porque se abran una cuenta en una entidad de crédito en el país no UE) activaría la aplicación del RGPD. En estos supuestos, la Guía aclara expresamente que no sería de aplicación el RGPD.

Más complejo aún se hace determinar el alcance concreto del supuesto de extraterritorialidad previsto en el artículo 3.2.b) del RGPD («el control de su comportamiento, en la medida en que este tenga lugar en la Unión»). El concepto de «control de comportamiento» es complejo, indeterminado y sujeto a muy diversas interpretaciones. El considerando 24 del RGPD señala que este supuesto debe entenderse aplicable «cuando esté relacionado con la observación del comportamiento de dichos interesados» en la medida en que este comportamiento tenga lugar en la UE. Por tanto, como el propio EDPB aclara en la Guía, el requisito para este supuesto es doble: debe referirse a interesados ubicados en la UE y el comportamiento monitorizado debe tener lugar y desarrollarse por dicho interesado también en el territorio de la UE. Este doble requisito genera un marco interpretativo que va más allá de la ubicación de la organización que realiza el tratamiento, centrando el foco en las actividades específicas del interesado dentro de la UE. Un ejemplo práctico sería el seguimiento a través de dispositivos móviles de los hábitos de consumo de un turista japonés durante su estancia en la UE, por parte de una empresa de análisis de datos con sede fuera de Europa. En este caso, la monitorización del comportamiento del interesado dentro de las fronteras europeas activaría la aplicabilidad del RGPD, aunque la empresa no tenga presencia física en la Unión.

Para determinar si se puede considerar que un tratamiento «controla» el comportamiento de los interesados, el considerando 24 señala que debe

tenerse en consideración si las personas físicas son objeto de un seguimiento en Internet, «inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes». En este sentido, el control del comportamiento no se limita a actividades comerciales, sino que puede extenderse a otros ámbitos, como la supervisión de actividades académicas o laborales en plataformas digitales que recopilen datos sobre patrones de estudio o productividad de usuarios en la UE. Este enfoque más amplio busca cubrir la diversidad de contextos en los que el control del comportamiento puede influir en la privacidad del interesado. Sin embargo, y a pesar de la expresa referencia del considerando 24 al seguimiento de comportamientos a través de Internet, el EDPB ha manifestado en la Guía que no debe darse una interpretación estricta al artículo y deberían considerarse también monitorizaciones realizadas por redes y tecnologías distintas a Internet. Esto amplía el alcance del RGPD a tecnologías emergentes como dispositivos IoT (Internet de las cosas), sistemas de seguimiento mediante inteligencia artificial o drones utilizados para capturar datos en tiempo real, asegurando que la protección de datos evolucione al mismo ritmo que las innovaciones tecnológicas.

Una última regla extraterritorial adicional es la que se prevé en el apartado 3 del artículo 3 del RGPD, por la que se establece que el RGPD se aplicará al tratamiento de datos personales por parte de responsables no establecidos en la UE si se ubican en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público. Esto podría incluir, por ejemplo, embajadas, consulados u oficinas de representación de la UE en terceros países, donde el tratamiento de datos personales se lleva a cabo en el marco de las actividades relacionadas con dichas representaciones. Este enfoque garantiza que la normativa europea sobre protección de datos se extienda a contextos específicos, incluso fuera de las fronteras de la UE, reforzando la protección de los derechos de los interesados.

Con este panorama normativo de aplicación extraterritorial existe el riesgo de una interpretación expansiva del mencionado supuesto del artículo 3.2.b) del RGPD, consistente en que cualquier recogida de datos personales por medios *online* y su posterior análisis, a través, por ejemplo, de cualquier sitio web o *app*, implique la aplicación del RGPD a entidades no europeas. Este riesgo aumenta en un entorno digital globalizado donde



Esta obra colectiva, editado bajo el paraguas de la Cátedra de Relaciones Privadas Internacionales de la Universidad Miguel Hernández de Elche (UMH)-Ilustre Colegio de Abogados de Orihuela (ICAO), reúne diferentes estudios jurídicos que abordan, elaborados por más de veinte profesionales, desde una perspectiva internacional, comparada y multidisciplinar, los desafíos emergentes que enfrenta el Derecho de los Negocios Internacionales en un contexto marcado por la digitalización, la globalización y la evolución normativa. Los autores, provenientes de diversas universidades e instituciones, ofrecen un análisis riguroso y actualizado sobre fenómenos jurídicos que afectan la contratación transfronteriza, la resolución de conflictos, la protección de consumidores, la propiedad intelectual y la regulación de nuevas formas de comunicación comercial.

El hilo conductor de esta obra es la transformación del comercio internacional en la era digital, la irrupción de tecnologías como la inteligencia artificial, el comercio electrónico, las plataformas digitales y los *influencers* todo lo cual ha modificado profundamente las dinámicas contractuales, los modelos de negocio y las exigencias regulatorias. En este nuevo escenario, el Derecho se ve interpelado a ofrecer respuestas ágiles, coherentes y eficaces, que garanticen la seguridad jurídica sin obstaculizar la innovación.

Uno de los méritos de esta obra radica en su capacidad para integrar enfoques diversos sin perder coherencia temática. La pluralidad de voces y perspectivas permite al lector comprender la complejidad del Derecho de los Negocios Internacionales en su dimensión más dinámica y global. A través de un enfoque crítico y propositivo, los autores invitan a reflexionar sobre el papel del Derecho en la configuración de un comercio internacional más justo, transparente y sostenible; es más, no sólo describen el estado actual de la normativa aplicable, sino que también plantean interrogantes, proponen soluciones y anticipan tendencias. Desde el análisis de los contratos automatizados y la determinación de la ley aplicable, hasta la regulación de la publicidad empresarial en redes sociales, cada contribución aporta una mirada especializada que enriquece el debate jurídico contemporáneo. Asimismo, se abordan cuestiones de gran relevancia práctica como el teletrabajo transfronterizo, la sucesión de bienes digitales, los contratos laborales internacionales en el sector tecnológico, y los problemas de oponibilidad de pactos de socios en sistemas jurídicos comparados. La obra también dedica especial atención a la evolución del arbitraje comercial internacional, tanto en Europa como en América Latina, y a la revalorización de los contratos de Estado en el sistema de arbitraje de inversión.

ISBN: 978-84-1085-579-3

