ESTUDIOS

# NUEVOS RETOS EN EL USO DE LA INFORMACIÓN Y LOS DATOS EN LOS PROCESOS Y EN LOS PROCEDIMIENTOS SANCIONADORES

**IGNACIO COLOMER HERNÁNDEZ**
DIRECTOR
**JUAN ALEJANDRO MONTORO SÁNCHEZ**
COORDINADOR

**Si quieres adquirir esta obra haz click aquí**

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Cofinanciado por la Unión Europea
AGENCIA ESTATAL DE INVESTIGACIÓN
DATER
ARANZADI

© **Ignacio Colomer Hernández (Dir.) y Juan Alejandro Montoro Sánchez (Coord.),** 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:** Febrero 2026

**Depósito Legal:** M-1308-2026
**ISBN versión impresa:** 978-84-1085-636-3
**ISBN versión electrónica:** 978-84-1085-637-0

Esta publicación es parte del Proyecto «*Datos personales e información en la era digital: desafíos en su obtención y uso en los procesos judiciales y en los procedimientos sancionadores (DATER)*» Ref. PID2022-137826NB-I00, financiado por MCIN/AEI/10.13039/501100011033/FEDER, UE.

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.

Si quieres adquirir esta obra haz click aquí

# *Índice general*

*Página*

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

IGNACIO COLOMER HERNÁNDEZ . . . . . 25

PRIMERA PARTE

INFORMACIÓN Y DATOS PERSONALES EN LAS INVESTIGACIONES PENALES

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

RODRIGO MORENO FUENTES . . . . . 47

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

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

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

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

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



Si quieres adquirir esta obra haz click aquí

*Página*

**2. La regulación de los hallazgos casuales en las diligencias de intervención de las comunicaciones y tecnológicas** ..... 56

*2.1. Las diligencias de intervención de las comunicaciones y tecnológicas* ..... 57

*2.2. Los arts. 579 bis y 588 bis I de la LECRIM* ..... 59

**3. El supuesto de investigaciones sobre dispositivos electrónicos de almacenamiento masivo y los registros y rastreos remotos de equipos informáticos** ..... 65

*3.1. Hallazgo casual en el registro de dispositivos de almacenamiento masivo de información* ..... 66

3.1.1. El análisis de dispositivos electrónicos de almacenamiento masivo ..... 66

3.1.2. La autorización judicial de acceso al dispositivo ... 68

3.1.3. Los hallazgos casuales en esta diligencia de investigación ..... 72

3.1.3.1. Valor meramente investigador de lo encontrado y necesidad de cobertura de la autorización judicial original ..... 74

3.1.3.2. Eventual valor probatorio de lo hallado en casos de flagrancia ..... 77

3.1.3.3. El juego del principio de proporcionalidad . 83

*3.2. Hallazgo casual en el registro y rastreo remoto sobre equipos informáticos* ..... 85

3.2.1. El registro y rastreo remoto sobre equipos informáticos ..... 85

3.2.2. La autorización judicial de acceso al dispositivo ... 88

3.2.3. Los hallazgos casuales en esta diligencia de investigación ..... 89

3.2.3.1. Valor investigador o probatorio de lo encontrado y necesidad de cobertura de la autorización judicial original en función de si se interceptan las comunicaciones o no ... 89

3.2.3.2. El juego del principio de proporcionalidad . 92

**4. Conclusiones** ..... 97



Si quieres adquirir esta obra haz click aquí

*Página*

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

PABLO GRANDE SEARA . . . . . 101

**1. Introducción** . . . . . 101
**2. Afectación de derechos fundamentales** . . . . . 106
**3. La utilización de dispositivos técnicos de seguimiento y localización en la LECRIM** . . . . . 109

*3.1. Situación anterior a la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre* . . . . . 109
*3.2. Régimen jurídico actual de la utilización en la investigación penal de dispositivos técnicos de seguimiento y localización* . . . . . 112

3.2.1. Solicitud de autorización judicial. Los indicios de criminalidad . . . . . 113
3.2.2. Autorización judicial de la medida . . . . . 116

3.2.2.1. Juez competente . . . . . 116
3.2.2.2. Contenido del auto habilitante . . . . . 117

3.2.3. Adopción policial de la medida . . . . . 122
3.2.4. Duración de la medida . . . . . 125
3.2.5. Sujetos obligados a la asistencia y colaboración . . . . 127
3.2.6. Control judicial de la práctica de la medida . . . . . 128

**4. Bibliografía** . . . . . 129

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

JUAN ALEJANDRO MONTORO SÁNCHEZ . . . . . 131

**1. Introducción: el nuevo contexto digital y sus implicaciones para la justicia penal** . . . . . 132
**2. El análisis forense digital en la Unión Europea: desafíos actuales y estrategias para el fortalecimiento de las capacidades** . . . 137



Si quieres adquirir esta obra haz click aquí

*Página*

*2.1. Soluciones propuestas por el grupo de alto nivel para el análisis forense digital* . . . . . 140

**3. La retención de datos de comunicaciones electrónicas con fines penales: desafíos persistentes y propuestas del grupo de alto nivel para un marco renovado** . . . . . 142

*3.1. Propuestas y recomendaciones del grupo de alto nivel para la conservación de metadatos de tráfico* . . . . . 145

**4. La interceptación de comunicaciones en la Unión Europea: desafíos en la era digital y propuestas para mejorar su eficacia** . . 148

*4.1. Propuestas del grupo de alto nivel para la interceptación de las comunicaciones* . . . . . 155

**5. Conclusiones** . . . . . 157

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

JOSÉ LUIS RODRÍGUEZ LAINZ . . . . . 161

**1. Introducción** . . . . . 161

**2. De la negación absoluta de regímenes de conservación generalizada e indiscriminada de datos relativos a las comunicaciones a la búsqueda de líneas de apertura** . . . . . 165

**3. Hacia la convergencia del Tribunal Europeo de Derechos Humanos con la jurisprudencia del TJUE** . . . . . 178

**4. El difícil reto de la STJUE del caso La Quadrature du NET II** . 189

**5. La delicada situación de la legislación y jurisprudencia nacionales sobre conservación generalizada e indiscriminada de datos relativos a comunicaciones electrónicas** . . . . . 195

*5.1. Diagnosis crítica de la ley española de conservación de datos frente a la hostil jurisprudencia del TJUE* . . . . . 195

*5.2. La escasa permeabilidad de la jurisprudencia del TJUE sobre conservación preventiva de datos relativos a las comunicaciones en la jurisprudencia de Sala 2.ª del Tribunal Supremo* . . . . . 214

**6. Bibliografía** . . . . . 222



Si quieres adquirir esta obra haz click aquí

*Página*

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

PABLO AZAÚSTRE RUIZ . . . . . 227

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

SEGUNDA PARTE

INFORMACIÓN Y DATOS PERSONALES EN LOS PROCESOS PENALES

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

STEFANO RUGGERI . . . . . 241

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



Si quieres adquirir esta obra haz click aquí

*Página*

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

ANTONELLA FALCONE . . . . . 261

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

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

M.ª ÁNGELES CATALINA BENAVENTE . . . . . 295

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



Si quieres adquirir esta obra haz click aquí

*Página*

*2.3. Los derechos de información, acceso y supresión de las grabaciones de las cámaras* on board . . . . . 317

**3. Otros derechos fundamentales que pueden verse afectados por la utilización de las cámaras *on board*** . . . . . 321

**4. La utilización como prueba en un proceso penal de las imágenes grabadas por las cámaras *on board*** . . . . . 332

*4.1. La validez probatoria de las grabaciones videográficas legítimamente obtenidas* . . . . . 333

*4.2. La (también) validez probatoria de las grabaciones videográficas ilegítimamente obtenidas* . . . . . 337

4.2.1. La conexión de antijuricidad . . . . . 341

4.2.2. La violación de derechos fundamentales por particulares y la flexibilización de la regla de exclusión . 346

4.2.3. La prueba ilícita y las grabaciones de las cámaras *on board* . . . . . 357

4.2.4. La obligación de entregar a la policía las grabaciones efectuadas por las cámaras *on board* . . . . . 359

*4.3. El valor probatorio de las imágenes captadas por las cámaras* on board . . . . . 363

4.3.1. La inmediatez, autenticidad e integridad de las imágenes aportadas . . . . . 363

4.3.2. La reproducción de las imágenes en el juicio oral . . 369

**5. Bibliografía** . . . . . 370

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

ELOY VELASCO NÚÑEZ . . . . . 375

**1. Algunas consideraciones acerca del contenido conceptual de la inteligencia artificial y su enfoque regulatorio** . . . . . 375

**2. La IA asistencial como prueba pericial, como herramienta/aplicación práctica útil en la justicia, y especialmente en la jurisdicción penal** . . . . . 381

**3. La IA como objeto de prueba** . . . . . 386

**4. La IA como medio de prueba** . . . . . 389



Si quieres adquirir esta obra haz click aquí

*Página*

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

RAFAEL CASTILLO FELIPE . . . . . 395

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

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

ALBA LANCHARRO CASTELLANOS . . . . . 427

**1. Introducción** . . . . . 428



Si quieres adquirir esta obra haz click aquí

*Página*

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

TERCERA PARTE

DERECHO PENAL Y TRATAMIENTO DE LA INFORMACIÓN

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

NATALIA PÉREZ RIVAS . . . . . 471

**1. Introducción** . . . . . 472



Si quieres adquirir esta obra haz click aquí

*Página*

**2. La responsabilidad penal del alertador por comunicar o revelar públicamente información** . . . . . 475

*2.1. La comunicación o revelación pública de información: condiciones para la protección del alertador* . . . . . 475

2.1.1. Requisito objetivo . . . . . 476
2.1.2. Requisito intelectivo . . . . . 479
2.1.3. Requisito procedimental . . . . . 481

*2.2. La protección penal del alertador por comunicar o revelar información: el diferente tratamiento del legislador europeo y del legislador español* . . . . . 485

*2.3. Mapa de riesgos penales del informante: delimitación de los posibles supuestos de responsabilidad* . . . . . 489

2.3.1. La protección penal del secreto . . . . . 489

2.3.1.1. Los delitos de descubrimiento y revelación de secretos . . . . . 489
2.3.1.2. El delito de revelación de secretos de empresa . . . . . 491
2.3.1.3. El delito de revelación de secretos por autoridad o funcionario público . . . . . 493

2.3.2. La protección penal del honor . . . . . 496

2.3.2.1. El delito de calumnias . . . . . 496

**3. Causas de exclusión de responsabilidad penal del alertador en casos de comunicación o revelación pública de información** . . 497

*3.1. El efecto directo de las Directivas y el principio de primacía del Derecho de la Unión Europea* . . . . . 497

*3.2. El deber de denunciar como causa de justificación o atenuación de la responsabilidad penal* . . . . . 498

*3.3. Límites jurídico-penales a la protección del secreto: exclusión en casos de ilicitud* . . . . . 500

*3.4. La revelación pública de infracciones a los medios de comunicación como manifestación legítima de la libertad de información* . 503

3.4.1. La revelación pública y la libertad de información del trabajador según la doctrina del Tribunal Europeo de Derechos Humanos: el caso Halet v. Luxemburgo . . . . . 505



Si quieres adquirir esta obra haz click aquí

*Página*

3.4.1.1. La existencia de canales alternativos a la divulgación pública para comunicar los hechos . . . . . 506
3.4.1.2. El interés público de los hechos divulgados . 507
3.4.1.3. La autenticidad de la información divulgada . . . . . 507
3.4.1.4. La concurrencia de buena fe en el informante . . . . . 508
3.4.1.5. La ponderación entre el perjuicio causado y el interés público de la información divulgada . . . . . 509
3.4.1.6. La gravedad de la sanción impuesta al informante . . . . . 510
3.4.2. La prevalencia del derecho a la libertad de información del informante: doctrina constitucional . . . . . 511

**4. A modo de conclusión: propuestas de *lege lata* y de *lege ferenda*** . . 516
**5. Bibliografía** . . . . . 518

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

FRANCISCO SALVADOR GIL GARCÍA . . . . . 523

**1. La sociedad de control en la era digital** . . . . . 523
**2. De la era post-industrial a la modernidad** . . . . . 525
**3. Conservación de datos en la Unión Europea** . . . . . 549
**4. Transferencia y puesta a disposición de datos personales** . . . . . 553
**5. Conclusión** . . . . . 560

**INFORMACIÓN FINANCIERA, DATOS PERSONALES Y BLANQUEO DE CAPITALES**

CLARA COLOMER LÓPEZ . . . . . 563

**1. Planteamiento de la cuestión** . . . . . 563
**2. Delimitación del blanqueo** . . . . . 566
**3. Impacto social y económico del blanqueo** . . . . . 570



Si quieres adquirir esta obra haz click aquí

*Página*

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

CUARTA PARTE

INFORMACIÓN Y DATOS EN PROCESOS NO PENALES

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

IGNACIO COLOMER HERNÁNDEZ ..... 611

**1. Delimitación de la cuestión a analizar** ..... 611
**2. La pericial algorítmica** ..... 613
**3. Pericial algorítmica, transparencia y valoración de la prueba** ..... 617
**4. A modo de conclusión** ..... 633



Si quieres adquirir esta obra haz click aquí

*Página*

**LA NECESIDAD DE DISEÑAR UN PROCESO ORIENTADO AL DATO**

VICENTE PÉREZ DAUDÍ . . . . . 635

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

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

ALBERTO PALOMAR OLMEDA . . . . . 657

**1. Planteamiento inicial** . . . . . 657
**2. La regulación** . . . . . 659
*2.1. En el ámbito del derecho comunitario* . . . . . 659



Si quieres adquirir esta obra haz click aquí

*Página*

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

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

MARÍA JESÚS SANDE MAYO . . . . . 679

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



Si quieres adquirir esta obra haz click aquí

*Página*

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

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

ANTONIO VASCO GÓMEZ . . . . . 727

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

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

LUCÍA AGUADO PEÑAS . . . . . 759

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



Si quieres adquirir esta obra haz click aquí

*Página*

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



Si quieres adquirir esta obra haz click aquí

# Información, datos y pericial algorítmica en los procesos[1]

IGNACIO COLOMER HERNÁNDEZ
*Catedrático de Derecho Procesal*
*Universidad Pablo de Olavide de Sevilla*
*Investigador Principal Proyecto DATER*

SUMARIO: 1. DELIMITACIÓN DE LA CUESTIÓN A ANALIZAR. 2. LA PERICIAL ALGORÍTMICA. 3. PERICIAL ALGORÍTMICA, TRANSPARENCIA Y VALORACIÓN DE LA PRUEBA. 4. A MODO DE CONCLUSIÓN.

## 1. DELIMITACIÓN DE LA CUESTIÓN A ANALIZAR

El desarrollo exponencial de la IA, en especial desde la instauración de los modelos LLMM, ha acercado el uso de algoritmos para la realización de actividades por parte de los ciudadanos y por parte de los poderes públicos. Y son estos los dos campos de actividad en los que el uso de la IA ha determinado la necesidad de acudir a la prueba pericial en aquellos procesos en los que se ventilan materias relacionadas con el resultado obtenido a través del empleo de algoritmos.

En concreto, quiero referirme, de un lado, al uso de IA para la alteración y manipulación de la realidad, en particular la generación de *deepfakes* difícilmente identificables por las personas si no se cuenta con un análisis

1. Esta publicación es parte del proyecto «*Datos personales e información en la era digital: desafíos en su obtención y uso en los procesos judiciales y en los procedimientos sancionadores (DATER)*» Ref. PID2022-137826NB-I00, financiado por MCIN/AEI/10.13039/501100011033/FEDER, UE, y del Proyecto «*Justicia sostenible en estado de mudanza global*» (JUSOST) CIPROM 2023-64 GVA.



Si quieres adquirir esta obra haz click aquí

técnico o científico de un perito; y por otro lado, aquellos casos en los que se empleen en los procesos algoritmos predictivos, que dan lugar a lo que podemos denominar como «*pericial algorítmica*», esto es, los supuestos en los que el resultado de una actividad algorítmica que aporta una predicción sea objeto de prueba.

En este sentido, no pueden desconocerse las grandes posibilidades que la IA ha puesto a disposición de las personas y de las empresas para la alteración de la realidad, tanto de imágenes como de sonidos, generando verdaderas «realidades» o, más correctamente, «apariencias de realidad» que técnicamente se denominan *deepfakes*[2]. La dificultad evidente que existe para identificar estas apariencias de realidad tiene una directa consecuencia para el desarrollo de los procesos, muy en particular para el desenvolvimiento del juicio de hecho. Pues, es posible que entre el material fáctico que se aporte al proceso, en especial las imágenes y los sonidos, pueda existir algún elemento que haya sido creado, alterado o convenientemente maquillado a través del uso de IA, lo que dificulta considerablemente las posibilidades de percibir o detectar que se haya producido su alteración o modificación.

El uso de la IA por los particulares y por los profesionales en el ejercicio de su actividad pericial está, sin duda, modificando de manera esencial la propia naturaleza del juicio sobre la *quaestio facti* por cuanto está afectando al propio objeto de la prueba, esto es a los *facta probandum*, como a los propios medios de prueba que se articulan para acreditar la realidad de los hechos alegados. En este sentido, es preciso distinguir dos planos o elementos a la hora de analizar el papel de la IA, en especial la generativa, en el seno del juicio de hecho. De un lado, la IA como objeto de la prueba (pericia sobre un algoritmo), que son aquellos supuestos que en los que la propia actividad de la IA es el objeto de la prueba, entendida como prueba sobre prueba para acreditar la validez y autenticidad de la primera actividad desarrollada por la IA.

Y de otro lado, los casos en los que la IA actúa como medio de prueba para emitir una predicción o explicación científico-técnica sobre algún hecho o realidad (pericia mediante algoritmo). Son estos supuestos en

2. Sobre el impacto de los deepfakes en los derechos fundamentales ver JIMÉNEZ-CASTELLANOS BALLESTEROS, I. «La difícil convivencia entre la inteligencia artificial y los derechos fundamentales: la tecnología deepfake» en *Inteligencia artificial y protección de datos: desafíos en la era digital*, Febles Pozo y Nieto Rojas (dir.), Colex, A Coruña, 2025, págs. 151-178.



Si quieres adquirir esta obra haz click aquí

los que la intervención de la IA desempeña una estricta función pericial, aportando los conocimientos científicos, técnicos o artísticos necesarios para que el juez pueda decidir sobre algún aspecto del juicio de hecho. Es en este caso cuando se puede hablar stricto sensu de *prueba pericial algorítmica*[3].

## 2. LA PERICIAL ALGORÍTMICA

La primera de las dimensiones que es preciso analizar en relación con el uso de la IA en los procesos está vinculada con aquellos supuestos en los que la inteligencia artificial es usada para dar una predicción o una explicación sobre un hecho futuro o del pasado que forme parte del objeto fáctico del proceso. Es decir, es necesario analizar aquellos casos en los que la IA se utiliza para dar una opinión científica o técnica sobre un hecho pasado explicando o identificando su posible causa[4], o sobre un hecho futuro haciendo una predicción de su posible evolución[5].

En este caso el uso de la IA se concreta en la aportación de una predicción sobre las causas que han determinado una situación o un hecho, o en la aportación de una previsión sobre el desarrollo futuro de una situación

3. Nótese que, aunque en principio la distinción entre pericia sobre un algoritmo y pericia mediante un algoritmo parece clara, en la práctica se pueden difuminar los contornos en aquellos supuestos en los que la pericia sobre un algoritmo sea realizada por otro algoritmo. Es decir, en aquellos casos en los que los conocimientos científicos o técnicos aportados por la IA se dirijan a acreditar que el modelo de IA previamente usado se adecua a los estándares y exigencias del Reglamento (UE) sobre IA. Dicho, en otros términos, hay veces en los que la pericial algorítmica recae sobre el resultado previo del uso de una IA y en estos casos se difuminan las diferencias, pues en estos casos lo que se desarrolla es una pericial mediante un algoritmo que tiene por objeto hacer una pericial sobre un algoritmo, para analizar, auditar o validar los resultados que se hayan podido obtener a través de ese sistema de inteligencia artificial.
4. Por ejemplo, cuando a través de un análisis de una IA se dé una explicación sobre la causa del derrumbe de un edificio o cuando tras el examen de los resultados médicos de una persona, incluidos en su caso los datos obtenidos en una autopsia, se pueda identificar o explicar la causa de la muerte del sujeto. También cuando la IA se utilice para un análisis de posibles irregularidades o fraudes en la contabilidad de una empresa mediante «clustering» automático, esto es, mediante las exigencias de «cluster stability» y de validación de «clusters» sospechosos.
5. Cuando la IA a la vista de fotos de una grieta en los pilares de un puente pueda predecir de cara al futuro las posibilidades de colapso de la infraestructura o cuando en relación con los resultados de las pruebas médicas de un sujeto pueda predecir el porcentaje de prevalencia de unas determinadas enfermedades en ese individuo.



Si quieres adquirir esta obra haz click aquí

o de una cosa, por ello a la hora de calificar jurídicamente la naturaleza de esta actividad a través de algoritmos se puede hablar de pericial algorítmica. Pues no debe perderse de vista que en estos supuestos la IA actúa como si de un perito se tratase aportando los conocimientos científicos, técnicos o artísticos necesarios para una adecuada aprehensión y conocimiento de la concreta *quaestio facti* que se esté dilucidando en el proceso. En este sentido, la intervención de la IA ha de ser considerada una pericia de opinión científica de pasado o de futuro desde el punto de vista de su naturaleza jurídica.

El hecho de que la pericial algorítmica sea una pericial de opinión científica y no una pericial científicamente objetiva resulta trascendente en orden a la valoración de la prueba que haya de realizar el juzgador. Dicho, en otros términos, la circunstancia de que la pericial desarrollada a través de un algoritmo deba ser considerada una pericial de opinión científica permite que el juez al valorarla pueda separarse de la conclusión alcanzada por la IA, ya sea en la identificación de la causa de la situación o del estado de la cosa en el peritaje de pasado o de la consecuencia o predicción en el caso del peritaje de futuro o proyectivo.

La pericial algorítmica en cuanto es una simple opinión científica, esto es una mera pericial deducente, es apreciable y valorable por el juez aplicando las reglas de la sana crítica. De manera que el libre convencimiento del juez será el criterio determinante de la interpretación y posterior valoración de esta prueba pericial algorítmica.

Por otra parte, no debe tampoco perderse de vista que, dada su naturaleza de opinión científica, esta pericial que se desarrolla a través del empleo de la IA puede dar lugar a resultados, informes o dictámenes, que sean contradictorios con los que pueda producir otra IA. De forma que la valoración de la prueba pericial algorítmica aparece como un elemento esencial para que el juzgador pueda tomar su decisión sobre el juicio de hecho respecto de los *facta probandum* que hayan sido el objeto de la actividad algorítmica[6].

6. Por ejemplo, si un algoritmo establece que la causa de una situación, un derrumbe de un edificio, es consecuencia de un defecto de la estructura del inmueble a la vista de las circunstancias de hecho concurrentes, y, por el contrario, otra IA considera que la causa del colapso del inmueble se encuentra en un defecto de la planificación, resulta evidente que la función del juez debe ser establecer a través de la libre valoración de la prueba cuál de los dos conclusiones sobre la causa del derrumbe presenta un mayor grado de credibilidad o verosimilitud para tener por acreditada la causa del derrumbe del edificio.



Si quieres adquirir esta obra haz click aquí

El problema se encuentra sin duda en precisar cómo debe realizarse esa actividad jurisdiccional de valoración de la prueba pericial algorítmica o incluso si es posible llevarla a cabo dadas las limitaciones que existen en cuanto a la transparencia en el funcionamiento de los instrumentos de IA[7]. La respuesta ante este interrogante ha de ser claramente afirmativa. La actividad pericial llevada a cabo a través de IA o de algoritmos puede, y debe, ser valorada por los jueces para su uso como medio de prueba en los procesos, so pena en caso de no hacerlo de incurrir en una aporía como la siguiente: la IA es tan inteligente que sus predicciones no pueden ser controladas, ni verificadas, ni siquiera por otra IA.

En este sentido, resulta evidente que el resultado de la actividad desarrollada con un algoritmo tiene que ser sometida a la posibilidad de crítica y no es admisible su aceptación incondicionada por los jueces.

La razón que explica la necesidad de que los jueces realicen una adecuada valoración de la prueba pericial algorítmica se encuentra en su propia naturaleza de pericia de opinión científica y en el hecho de que no pueda ser considerada una pericia científicamente objetiva[8].

---

7. No solo la falta de transparencia dificulta la valoración, sino que tampoco lo facilita la complejidad y sofisticación de los sistemas de computación. Al respecto, la complejidad se constata simplemente con tener en cuenta los posibles niveles autónomos de razonamiento jurídico de la inteligencia artificial: «*Level 0: No Automation for AI Legal Reasoning. Level 1: Simple Assistance Automation for AI Legal Reasoning. Level 2: Advanced Assistance Automation for AI Legal Reasoning. Level 3: Semi-Autonomous Automation for AI Legal Reasoning. Level 4: Domain Autonomous for AI Legal Reasoning. Level 5: Fully Autonomous for AI Legal Reasoning. Level 6: Superhuman Autonomous for AI Legal Reasoning*» (*Cfr.* ELIOT, L, «Multidimensionality of Legal Singularity: Parametric Analysis and the Autonomous Levels of AI Legal Reasoning», 2020, pág. 9, https://www.researchgate.net/publication/343848479_Multidimensionality_of_Legal_Singularity_Parametric_Analysis_and_the_Autonomous_Levels_of_AI_Legal_Reasoning).
8. No se debe perder de vista que en el caso de la pericia científicamente objetiva el juez no puede apartarse del contenido del informe por ser el resultado de una actividad o método científico, si no es en los supuestos en los que se acredite la concurrencia de algún vicio en el desarrollo de ese procedimiento científico. Por el contrario, la pericia realizada por medio de algoritmos es una pericia de opinión científica en la que el juzgador puede apartarse del resultado y valorar el resultado, en particular cuando haya resultados contradictorios alcanzados por distintos algoritmos. Y es que no puede perderse de vista que lo transcendente, a los efectos de la valoración de la prueba pericial algorítmica, es la predicción o la explicación de la causa de una situación que realiza el algoritmo y esta actuación de la IA lleva un elemento nuclear de opinión y que no es simplemente una prueba científicamente objetiva.



Si quieres adquirir esta obra haz click aquí

El problema que se plantea en orden a una adecuada valoración de las pericias realizadas a través de IA se encuentra en la dificultad que van a encontrar las partes en el proceso y el juzgador para poder conocer los elementos que han de ser tenidos en cuenta para desarrollar esa valoración en relación con el ámbito de las premisas, con el ámbito del método y con el ámbito de las conclusiones[9]. Es decir, la principal dificultad que se plantea en relación con la valoración de la prueba pericial algorítmica se encuentra en la opacidad, o dicho en sentido negativo la falta de una adecuada transparencia en relación con el desarrollo de la actividad algorítmica[10]. De manera que sin la debida transparencia el juez no puede realizar una valoración racional del resultado de la prueba pericial debiendo de hacer un ejercicio de «credulidad cuasi mágica»[11] respecto del resultado que arroje el ejercicio de la actividad del algoritmo[12].

---

9. «*La valoración de la prueba pericial implica necesariamente dos cosas para el juez: que sea capaz de identificar las premisas empleadas por el perito para fundamentarla y de entender las inferencias realizadas a partir de dichas premisas. Si el juez del caso es incapaz de detectar tales premisas o inferencias, no podrá realizar una valoración racional de la pericia*» (*Cfr.* JL. RAMÍREZ ORTÍZ, «Un cambio de paradigma probatorio: prueba pericial y prueba científica en el Anteproyecto de Ley de Enjuiciamiento Criminal de 2020», en *Diario La Ley*, N.º 9901, Sección Tribuna, 28 de Julio de 2021).
10. En este sentido, es muy importante tener en cuenta que los técnicos y científicos cuando se acercan a los debates jurídicos en torno a las exigencias y posibles mecanismos para el control del uso de los algoritmos en las decisiones jurídicas en la mayoría de las ocasiones ponen de manifiesto la imposibilidad de conocer las reglas e inferencias internas que se producen en los sistemas profundos. Al respecto, se puede ver la opinión de J. J. MURILLO FUENTES en su ponencia «Deep learning, Algoritmos y Big Data en el Uso de la Información con Relevancia Penal» en *Congreso Internacional sobre Proceso Penal y límites en el uso de la información*, celebrado los días 26 y 27 de noviembre de 2019 en Sevilla (https://uses0-my.sharepoint.com/:b:/g/personal/murillo_us_es/EdQvBFGKg51PqsrLMA1e44kB4MiZrpvwKDCkRcHf2R55Aw?e=jTRJ5j). Sobre la problemática del control y conocimiento de las operaciones internas llevadas a cabo por los sistemas de *machine learning* desde un punto de vista científico-técnico también se puede consultar el trabajo de J. ZERILLI; A. KNOTT; J. MACLAURIN; y C. GAVAGHAN, «Algorithmic Decision-Making and the Control Problem» en *Minds and Machines* (2019) 29, pág: 555-578 (https://link.springer.com/article/10.1007/s11023-019-09513-7).
11. «*El error subjetivo del juzgador puede consistir en la sumisión acrítica al parecer del perito o, en sentido contrario, sustituir el criterio técnico del perito por el subjetivo del juzgador sin una motivación suficiente*» (*Cfr.* ABEL LLUCH, «Criterios orientadores de la valoración de la prueba pericial», en *Peritaje y Prueba Pericial*, Picó I Junoy [dir.], Bosch, Barcelona, pág. 211-248).
12. Como expresamente reconoce el magistrado RAMÍREZ ORTÍZ «*Si el juez del caso es incapaz de detectar tales premisas o inferencias, no podrá realizar una valoración racional de*



Si quieres adquirir esta obra haz click aquí

La cuestión por tanto se ha de concretar en exigir de la prueba pericial algorítmica que cumpla unos estándares de transparencia que permitan la valoración racional por parte del juez del resultado que arroje la opinión científica o técnica alcanzada por la IA en su labor de tratamiento y computación de los datos y circunstancias concurrentes en el objeto fáctico del procedimiento jurisdiccional.

## 3. PERICIAL ALGORÍTMICA, TRANSPARENCIA Y VALORACIÓN DE LA PRUEBA

Cómo se ha señalado en el apartado anterior la pericial algorítmica en cuanto es una pericia de opinión científica permite que el resultado al que se llegue en el desarrollo de su actividad, sea una predicción de futuro o sea una hipótesis sobre la causa de un hecho o de una situación del presente, pueda ser objeto de una apreciación conforme a las reglas de la sana crítica y desarrollar una racional valoración de la prueba.

Para desarrollar adecuadamente esa racional valoración y apreciación de la prueba el juzgador ha de tener acceso a unos mínimos elementos relativos a las premisas, la metodología y las conclusiones que existan en la actividad del algoritmo.

En concreto, del informe o dictamen elaborado por la IA, en particular cuando es realizado por una IA generativa, deberán poder desprenderse los siguientes contenidos:

(i) En relación con el ámbito de las premisas.

La predicción o explicación que haya realizado la IA deberá reflejar la situación fáctica que concurre en relación con los hechos para los que sea preciso aplicar los conocimientos científicos o técnicos para determinar su causa o predecir su evolución futura. Al respecto, en el informe realizado por el algoritmo deberá incluirse de forma expresa la descripción de los hechos y las circunstancias que son tenidas en cuenta por la IA para aplicar los conocimientos especializados, técnicos o científicos, para alcanzar una

---

*la pericia. A lo sumo, aceptará el resultado de la prueba o lo rechazará, enmascarando su incapacidad mediante el recurso a criterios estándar deductivos o subjetivos propios de la prueba testifical (v.gr. seguridad, claridad expositiva, perito oficial vs perito de parte), o a palabras rituales cuya mera enunciación parece bastar para satisfacer las exigencias de la lógica, la ciencia y la experiencia*» (*Cfr.* op.cit).



Si quieres adquirir esta obra haz click aquí

concreta conclusión sobre la causa o la posible evolución de una situación o hecho[13].

Para tener claro el alcance y contenido de todas las premisas que concurren en el ejercicio de la actividad pericial por parte de la IA es necesario que en el informe o dictamen en el que se contenga la predicción o explicación realizada con el algoritmo se incluyan de forma expresa los datos de entrada que se han introducido en el sistema de IA[14].

Al respecto, se pueden distinguir dos grandes elementos a través de los cuales se estructuran los datos de entrada suministrados al algoritmo: de una parte, los prompts u órdenes que se dan a la IA, en especial a las generativas, en las que se delimita y configura lo que se pretende de la actividad del sistema algorítmico[15]; y de otra parte, el propio contenido de entrada que se suministra al sistema de IA, que contiene todas las circunstancias concurrentes en las personas y las cosas de la situación respecto de la que se pretenda obtener una predicción de futuro o una explicación de pasado.

El conocimiento del juez acerca de los concretos prompts que se han suministrado a la IA resulta un elemento esencial para poder realizar una

13. En este sentido, puede concretarse aún más esta exigencia de incluir información detallada de las circunstancias concurrentes en relación con la situación, hecho o cosa que sea objeto de la pericia. Así, continuando con el ejemplo que estamos manejando a lo largo del trabajo, si la pericia versa sobre la determinación de la causa del derrumbe de un edificio será necesario que en el informe realizado por la IA se identifiquen de forma clara y minuciosa que, por ejemplo, en el inmueble existían unas determinadas grietas en las columnas de la estructura, señalando la longitud, la anchura, etc. Además, si se dispusiese de datos relativos a la composición del hormigón y cualquier otra circunstancia que resulte relevante para ser tenido en cuenta a la hora de establecer la posible causa del colapso del edificio también deberá aparecer el informe de la IA para que el juzgador pueda racionalmente apreciarlo y valorarlo, en particular en aquellos casos en los que puedan existir dos pericias algorítmicas con resultados incompatibles o diversos en la determinación de la causa de la situación provocada.
14. Respecto al papel de los datos de entrada en los sistemas algorítmicos usados en la justicia ver, entre otros, MJ. ARIZA COLMENAREJO «Fuentes de datos al servicio de sistemas de inteligencia artificial dirigidos a la toma de decisiones judiciales» en *Inteligencia artificial y proceso penal: un reto para la Justicia*, Castillejo Manzanares y Noya Ferreiro (dir.), Aranzadi, Cizur Menor, 2023, pág. 15-42.
15. Un prompt es una instrucción, pregunta o texto que se utiliza para interactuar con sistemas de inteligencia artificial. En este sentido, podría decirse que es similar a un comando u orden con la que se pide al sistema que realice una concreta tarea o actividad.



Si quieres adquirir esta obra haz click aquí

adecuada valoración de la prueba, ya que le permitirá delimitar adecuadamente el ámbito de las premisas en la prueba pericial algorítmica. Y es que los prompts u órdenes que se le hayan dado a la IA para encauzar o dirigir su actividad pueden poner de manifiesto eventuales sesgos[16], condicionamientos o limitaciones en cuanto a la información que maneje la IA en su actuación que afecten directamente a las conclusiones que pueda haber alcanzado el sistema algorítmico y que en consecuencia determinen una reducción de valor probatorio o incluso una pérdida total del mismo.

En particular a la hora de reflejar en el informe de la pericial algorítmica los prompts utilizados resulta muy importante indicar el rol que se le asigna a la IA para el ejercicio de la actividad pericial[17].

La importancia de indicar exhaustivamente los prompts utilizados para la valoración de esta clase de pruebas se encuentra en que un prompt bien formulado determina directamente la generación de una respuesta adecuada por parte de la IA, dejando a salvo claro está los supuestos de

16. LLANO ALONSO afirma que «*la premisa de la que debemos partir al referirnos a las posibles consecuencias discriminatorias derivadas de la presencia de sesgos en los algoritmos es que ni éstos son causados ex nihilo por las máquinas, ni tienen voluntad propia, sino que en realidad son el producto del diseño humano y que, por tanto, también tienen origen humano. En otras palabras: somos las personas quienes, de manera consciente o inconsciente, poseemos prejuicios y tenemos una visión sesgada de la realidad que al final termina proyectándose en el diseño y despliegue de los algoritmos*» (*Cfr.* F. LLANO ALONSO, *Homo ex machina: ética de la inteligencia artificial y Derecho Digital ante el horizonte de la singularidad tecnológica*, Tirant lo Blanch, Valencia, 2024, pág. 207). De ahí que resulte tan útil el conocimiento de los prompts que se hayan usado al solicitar la actividad pericial por parte del sistema algorítmico, para identificar y apreciar la existencia de eventuales sesgos o datos sesgados que se suministren a la IA, que puedan determinar unas predicciones, explicaciones o conclusiones igualmente sesgadas como resultados de la actividad del algoritmo en el caso concreto.

17. De manera que si lo que se está intentando es que la IA determine la causa de un derrumbe de un edificio será muy relevante para la valoración de la prueba que el juez pueda saber si el rol que se le ha asignado a la IA ha sido el de un ingeniero o el de un arquitecto atendiendo a la concreta formulación del prompt en el que se haya definido el papel de la IA en relación con lo que se le pida. Pues, no hay duda de que el rol que se haya asignado a la actuación de la IA puede ser un elemento para valorar el resultado de la prueba desde el punto de vista de la cualificación del perito, elemento de valoración que como es sabido constituye uno de los criterios esenciales para graduar el valor probatorio de la prueba pericial, en especial en los casos en los que haya varias pericias con resultados contradictorios o diferentes en relación a unos mismos hechos (por ejemplo, en un caso de una agresión sexual resulta evidente que el examen de la mujer que haya sido víctima de la agresión no tendrá el mismo valor si es realizado por un ginecólogo o si es realizado por un médico de familia).



Si quieres adquirir esta obra haz click aquí

alucinaciones cada vez más infrecuentes. Por el contrario, un prompt mal o inadecuadamente planteado puede producir resultados no deseados, erróneos, sesgados o no completos. De ahí que se haya creado una rama del conocimiento el *prompt engineering*[18] que se dedica a estudiar y analizar el proceso de diseño y elaboración de prompts para la consecución y la realización de tareas específicas y concretas a través de IA. En este sentido, resulta esencial conocer y aplicar el *prompt engineering* para poder entender y valorar adecuadamente la precisión y la fiabilidad de los resultados de la IA atendiendo a los prompts que haya determinado el marco dentro del cual el algoritmo ha desarrollado su actividad[19].

En segundo lugar, junto a los prompts, es necesario que en el informe pericial realizado por la IA se incluya todo el contenido de entrada que se le haya suministrado al algoritmo para fijar las circunstancias concurrentes en la situación de hecho, cosa o persona que va a ser objeto de la aplicación de los conocimientos científicos o técnicos por parte de la IA en el desarrollo de su actividad pericial de predicción de futuro o de explicación de las causas de una situación pasada.

Esta necesidad de incluir los datos de entrada que sirvan para encuadrar adecuada y particularmente el objeto de la actividad pericial desarrollada por un algoritmo resulta crucial para poder contar con un detallado conocimiento de las premisas que condicionan el desarrollo de la actuación pericial.

No se debe perder de vista que los tribunales sintetizan los factores de ponderación y valoración de la prueba pericial señalando que son: «*A) La cualificación del perito, y, por lo tanto, su especialización sobre el tema a informar. B) El método aplicado en la elaboración del dictamen. C) Las condiciones*

18. https://es.wikipedia.org/wiki/Ingenier%C3%ADa_de_instrucciones
19. Al respecto, hay que tener en cuenta que existen los conocidos como *prompts AI generators* (entre otros, *PromptStorm* y *PromptBase),* que de manera automatizada facilitan la generación de prompts efectivos y adecuados para estructurar y optimizar la interacción con los sistemas algorítmicos. De ahí que, también a la hora de que el juzgador proceda a valorar la prueba pericial algorítmica, será determinante no solo conocer los prompts que se hayan utilizado en el caso concreto para dar las órdenes y fijar el marco de la actuación de la IA, sino también saber si, en su caso, esas órdenes han sido creadas por una persona o de forma automatizada a través del uso de un algoritmo. Y es que, en este segundo caso, sería necesario que el juez pudiera conocer, a su vez, cuáles han sido los prompts que se han suministrado al algoritmo que haya elaborado los prompts que sean usados por el sistema algorítmico que realice la actividad pericial.



Si quieres adquirir esta obra haz click aquí

*de observación o reconocimiento. D) La vinculación del perito con las partes. E) La proximidad en el tiempo y el carácter detallado del dictamen con respecto al hecho objeto de pericia. F) El criterio de la mayoría coincidente. G) El examen del propio informe técnico, teniendo en cuenta su coherencia interna, si incurre en contradicciones, si justifica sus conclusiones, si cuenta con omisiones manifiestas, si es congruente con las peticiones que le fueron formuladas, si es inteligible. H) Existen supuestos en los que el hecho u objeto del proceso es tan evidente, que hiere los sentidos ("res ipsa loquitur", los hechos hablan por sí mismos)*»[20]. De manera que dentro de las «*condiciones de observación o reconocimiento*» se pueden incluir todas las circunstancias concurrentes en la situación, cosa o persona que vaya a ser objeto de la actividad pericial de la IA.

En conclusión, hay que considerar que la explicitación de las premisas concurrentes en la actividad pericial desarrollada por la IA resulta una exigencia ineludible del informe, dictamen u opinión científica emitida por el sistema algorítmico, por constituir uno de los elementos esenciales sobre los que el juzgador puede articular su criterio de valoración del resultado de la prueba pericial algorítmica.

(ii) En relación con el ámbito del método.

En cuanto al método que usa el algoritmo para llegar a las conclusiones o predicciones que alcance se han planteado en los primeros estudios sobre el funcionamiento de la IA en el ámbito del Derecho innumerables digresiones sobre el alcance de la oscuridad o falta de transparencia de los algoritmos, en particular en los casos de *machine learning* o *deep learning*[21]. En este sentido ha sido argumento recurrente el empleo de la idea

20. *Cfr.* Sentencia de la Audiencia Provincial de A Coruña de 9 de marzo de 2016.

21. Como ponen de manifiesto los técnicos en los sistemas de aprendizaje profundo («*deep learning*») es probable que el sistema aprenda por sí mismo y que a partir de datos aparentemente neutros pueda llegar a inducir un determinado sesgo. El ejemplo paradigmático que se suele utilizar para ilustrar esta capacidad es el siguiente: la realización de una predicción sobre la probabilidad de impagos futuros a la hora de conceder o no un préstamo hipotecario en la que no se introduce la raza del solicitante de la hipoteca, pero el algoritmo induce o deduce a partir de otros datos como pueden ser el lugar dónde vive el solicitante, sus ingresos económicos y su concreta distribución, etc. Ello, no obstante, hay que seguir defendiendo que, a pesar de que los algoritmos de *machine learning* puedan producir sesgos no buscados de propósito a la hora de introducir la información con la que se ha entrenado su aprendizaje, en todo caso habrá que establecer mecanismos de control y supervisión para verificar que los datos que se suministren no sean ya desde su propia naturaleza sesgados.



Si quieres adquirir esta obra haz click aquí

de las «*black boxes*» de los algoritmos como argumento para descalificar, o al menos intentar limitar, su uso en los procedimientos jurisdiccionales[22]. En innumerables trabajos, sobre todo en los momentos iniciales de hace unos años, se exigía la necesidad de conocer cómo funcionaba internamente la IA, para lo cual se requería el acceso al código fuente del algoritmo[23] con toda la problemática que ello suponía, no solo desde el punto de vista técnico, sino también desde el punto de vista jurídico por la necesidad de proteger el secreto, la propiedad intelectual[24], la confi-

22. «*The fact that machine-learning AI learns on its own, translating inputs to outputs in ways that are unintuitive to humans, highlights an essential tension: AI may gain its accuracy through some lack of transparency. Deployed carelessly in contexts where transparency matters, such tools may challenge our fundamental need to know, explain, and ensure fairness. Without knowing how an AI tool creates its information outputs, we might not be able to provide the explanations that those affected by these outputs need or deserve. Furthermore, it may be impossible to ensure that the AI tool has not perpetuated unwanted or unlawful biases from its input data*» (*Cfr.* J. WARD, «From judicature: 10 things Judges should know about AI» en *Bolch Judicial Institute. Duke Law*, https://judicialstudies.duke.edu/2019/04/10-things-judges-should-know-about-ai/).

23. Hay que tener en cuenta en relación con el código del algoritmo que el Reglamento (UE) 2024/1689 sobre IA en su artículo 2.12 prevé expresamente que «*El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50*».

24. En España la Sentencia del Juzgado Central de lo Contencioso-Administrativo número 8, de 30 de diciembre de 2021 (procedimiento ordinario 18/2019) y la de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional (Sección 7.ª) de 30 de abril de 2024 (recurso de apelación 118/2022) en el asunto del sistema informático BOSCO (para la determinación de las personas solicitantes del bono social eléctrico que tienen derecho a su percepción) han denegado de forma reiterada el acceso al código fuente de la aplicación informática por razones de protección del derecho a la propiedad intelectual. Sin embargo, esta posición se ha matizado por la Sala Tercera del Tribunal Supremo cuando ha señalado «*Surge así, con motivo de la actividad administrativa automatizada, el llamado principio de "transparencia algorítmica", que impone a las Administraciones públicas obligaciones de información pública para facilitar el acceso de los ciudadanos, en mayor o menor medida, a las características fundamentales de los algoritmos empleados en la toma de decisiones o su código fuente, como una manifestación del principio de transparencia, consagrado constitucionalmente (artículo 105.b) de la CE*)» (Sentencia del Tribunal Supremo de 11 de septiembre de 2025 (Sala de lo Contencioso-Administrativo, sección tercera, núm. 1119/2025) Ver sobre este caso Bosco el análisis de A. HUERGO LORA, «Por qué aciertan las sentencias sobre el "algoritmo" del bono social eléctrico» en *Almacén de Derecho*, 10 mayo 2024 (https://almacendederecho.org/por-que-aciertan-las-sentencias-sobre-el-algoritmo-del-bono-social-electrico).



Si quieres adquirir esta obra haz click aquí

dencialidad y el know how empresarial[25] en el diseño e implementación de los sistemas de IA[26].

Sin embargo, en la actualidad el enfoque debe cambiar y debe centrar el foco, no en el funcionamiento interno del algoritmo[27], sino en el conocimiento de los datos de entrada y de los datos de salida. Lo que supone, de una parte, conocer los datos de entrenamiento del algoritmo, así como las circunstancias fácticas del caso concreto respecto de las que se quiera obtener la pericial algorítmica, y, de otra parte, conocer las conclusiones o predicciones que haga la IA en el desarrollo de su actividad.

Al respecto, hay que tener presente que el nuevo Reglamento (UE) 2024/1689 sobre IA[28] reconoce en el Considerando 133 la necesidad de transparencia en el uso de la IA[29].

---

25. Ver sobre esta cuestión la STJUE 7 diciembre 2023, SCHUFA Holding AG (C-634/21).
26. Respecto al levantamiento del secreto sobre el funcionamiento interno del sistema algorítmico VARELA GÓMEZ señala que «*no se nos oculta sin embargo la dificultad de esta exigencia, primero porque es sabido que en sus formas más avanzadas o futuras ni siquiera los programadores podrán explicarnos cuál ha sido el camino mediante el cual se ha llegado a la conclusión, y por otro lado, porque se trata de cuestiones amparadas por el secreto o la propiedad intelectual e industrial, que además tienen un altísimo valor económico. De esta manera la exigencia de transparencia puede devenir en casi imposible*» (*Cfr.* «Inteligencia artificial y decisión del conflicto judicial: una primera aproximación» en *Inteligencia artificial y proceso penal: un reto para la Justicia*, Castillejo Manzanares y Noya Ferreiro [dir.], Aranzadi, Cizur Menor, 2023, pág. 308).
27. En este sentido, como señala JULIÁ-PIJOAN «*muchas veces los propios expertos en el diseño del sistema o en la materia correspondiente son incapaces de explicar cómo el sistema funciona o qué partes son esenciales. Ello es así, porque el algoritmo no es un objeto, sino que está configurado por un conjunto de relaciones, que son difícilmente convertibles en algo transparente y entendible. No se requiere únicamente ver qué hay en esa caja negra, sino cómo funciona (las relaciones que opera). Debemos entender el instrumento como un sistema. Se puede mirar dentro de ellos, pero ello no agotará el conocimiento sobre lo que son. Por consiguiente, no deberíamos desatender que lo que interesa en la función jurisdiccional no es una respuesta genérica sobre el funcionamiento del sistema, sino cómo ha funcionado en un determinado caso*» (*Cfr.* M. JULIÁ-PIJOAN, *La computarización del Derecho, a partir del proceso y de los procedimientos judiciales*, Dykinson, Madrid, 2024, pág. 89).
28. Para una aproximación al contenido y alcance del Reglamento (UE) sobre la IA ver BARRIO ANDRÉS, M. «El Reglamento de la IA de la Unión Europea: el gobierno democrático de la inteligencia artificial» en *Inteligencia artificial y protección de datos: desafíos en la era digital*, Febles Pozo y Nieto Rojas (dir.), Colex, A Coruña, 2025, págs. 19-40.
29. «*Las obligaciones impuestas a los proveedores y a los responsables del despliegue de determinados sistemas de IA en el presente Reglamento destinadas a permitir que se detecte y divulgue que los resultados de dichos sistemas han sido generados o manipulados de manera artificial resultan especialmente pertinentes…*».



Si quieres adquirir esta obra haz click aquí

Esta necesidad de transparencia se refuerza en los casos de sistemas de alto riesgo del artículo 6 del Reglamento (UE) sobre IA[30]. Y en este sentido no debe perderse de vista que el apartado 2 Anexo III 8 *a)* recoge dentro de los sistemas de alto riesgo aquellos «*Sistemas de IA destinados a ser utilizados por una autoridad judicial, o en su nombre, para ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos, o a ser utilizados de forma similar en una resolución alternativa de litigios*».

De manera que, por tanto, un sistema algorítmico que sea usado para el desarrollo de una pericial algorítmica será considerado un sistema de alto riesgo a los efectos de la previsión del artículo 6 del Reglamento (UE) 2024/1689 sobre IA. Pues no hay duda, de que en estos casos el uso de la IA servirá para ayudar al juez a interpretar los hechos, aportándole una opinión científica sobre la causa de un hecho o una predicción sobre la evolución y desarrollo de una situación.

En este sentido, dentro de este ámbito de la metodología con la que actúa la IA para el desarrollo de una función pericial es preciso que se pueda constatar y comprobar el cumplimiento de las exigencias en cuanto a datos y gobernanza de datos que se contienen en el artículo 10 del Reglamento (UE) sobre IA. Puesto que es imprescindible para una adecuada valoración judicial del resultado de la pericial algorítmica que se pueda verificar que los datos de entrada y de entrenamiento del algoritmo reúnen las exigencias previstas en dicho precepto.

En particular, el conjunto de datos de entrenamiento, validación y prueba habrán de estar sometidos a prácticas de gobernanza y gestión de datos adecuados para la finalidad previstas del sistema de IA de alto riesgo, que en el caso que nos interesa será «*ayudar a una autoridad judicial en la investigación e interpretación de hechos y de la ley, así como en la garantía del cumplimiento del Derecho a un conjunto concreto de hechos*». Lo que implica que, en concreto, en el informe pericial que realice la IA deberá indicarse, al menos, las siguientes exigencias de las contenidas en el artículo 10.2 del Reglamento (UE) sobre IA: a) los procesos de recogida de datos y el origen

30. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). «DOUE» núm. 1689, de 12 de julio de 2024.



Si quieres adquirir esta obra haz click aquí

de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos; b) la formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos; c) una evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios; d) un examen de los posibles sesgos; e) la detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del presente Reglamento, y la forma de subsanarlas.

Sin lugar a duda, desde el punto de vista de la valoración probatoria de las pericias realizadas a través de IA el examen de los posibles sesgos en los datos de entrenamiento es uno de los elementos esenciales para que se pueda realizar una racional valoración de la prueba algorítmica[31]. Y es que la eventual existencia de sesgos en los datos de entrada o de entrenamiento del algoritmo va a determinar que las conclusiones a las que se lleguen en el funcionamiento de la IA estén lastradas por esos mismos sesgos[32] y, en consecuencia, su valor probatorio será claramente reducido o incluso podría llegar a desaparecer totalmente, atendiendo a la gravedad de los sesgos en los que pueda haber incurrido.

Al respecto, el Reglamento (UE) sobre IA prevé expresamente que el examen de los posibles sesgos de los datos de entrada, entrenamiento, validación y prueba debe buscar en particular aquellos sesgos «*que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho*

31. Buena prueba de la importancia que tiene la evitación de sesgos en los datos de entrenamiento o de entrada de las periciales desarrolladas a través de IA es que el artículo 10.5 del Reglamento (UE) sobre IA prevé expresamente que «*En la medida en que sea estrictamente necesario para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, de conformidad con lo dispuesto en el apartado 2, letras f) y g) del presente artículo, los proveedores de dichos sistemas podrán tratar excepcionalmente las categorías especiales de datos personales, siempre que ofrezcan las garantías adecuadas en relación con los derechos y las libertades fundamentales de las personas físicas*». Es decir, para la detección y corrección de posibles sesgos se habilita de forma excepcional a los proveedores de sistemas de IA de alto riesgo al tratamiento de categorías especiales de datos personales, siempre de acuerdo con las exigencias y requisitos previstos en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680, ofreciendo garantías adecuadas y suficientes para la protección de los derechos y libertades fundamentales de las personas físicas.

32. Sobre la relevancia de los sesgos se puede ver, entre otros, N. BELLOSO MARTÍN, «La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿hacia un derecho a la protección contra los sesgos?» en *Inteligencia Artificial y Filosofía del Derecho*, F. Llano Alonso (dir.), Laborum, 2022, pág. 45-78.



Si quieres adquirir esta obra haz click aquí

*de la Unión*» (artículo 10.2 f). Por ello, en el caso de que pueda existir algún sesgo en relación con los datos de entrada y de entrenamiento de una pericial algorítmica, esto es, dentro de un sistema de IA de alto riesgo, parece evidente que se podrán afectar negativamente derechos fundamentales de las personas, y en concreto el derecho a la tutela judicial efectiva, toda vez que el juez estará recibiendo una prueba pericial elaborada por un IA que contenga una predicción o una explicación de una situación pasada que pueda estar sesgada. De ahí que el propio Reglamento europeo prevea que también se indiquen las «*medidas adecuadas para detectar, prevenir y mitigar posibles sesgos detectados*». Lo que implica que para permitir una adecuada valoración de la prueba pericial realizada por IA será preciso no solo que se identifiquen los posibles sesgos de los datos de entrada y de los datos de entrenamiento, sino también que el propio algoritmo en su diseño tenga medidas adecuadas para detectar, prevenir y mitigar esos posibles sesgos que se detecten «*especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones*»[33].

Otro de los elementos que deben constar en la pericia algorítmica para poder permitir una adecuada y racional valoración de la prueba por el juez se encuentra en las exigencias que expresamente recoge el Reglamento (UE) 2024/1689 sobre IA en relación con los conjuntos de datos de entrenamiento, validación y prueba.

---

33. No se debe perder de vista que el resultado de la pericial algorítmica es probable, por no decir que es seguro, que condicione ulteriores pericias que puedan desarrollarse sobre unos hechos o materia similar. Es decir, los datos de salida de la actividad de la IA, esto es las conclusiones de la pericia algorítmica, podrán ser usados, o mejor dicho, con casi toda seguridad, serán empleados para el futuro entrenamiento del algoritmo, y por eso es imprescindible que en el desarrollo de la actividad algorítmica existan controles para detectar, prevenir o mitigar los posibles sesgos de los datos de entrada, así como los posibles sesgos que existan en los datos de salida. La existencia de estos controles o medidas de detección será un elemento importante que habrá de tener en cuenta el juzgador a la hora de valorar el resultado de la prueba pericial algorítmica que se presente en un proceso. Por ejemplo, en una autopsia realizada por IA a la que se le suministran todos los datos del examen y análisis del cuerpo para que una vez tratados identifique la posible causa de la muerte, es decir, exprese una opinión científica sobre la causa que determinó la muerte de esa persona, resulta evidente que si el algoritmo no tiene medidas para la detección de los datos sesgados con los que se entrena (datos de otras autopsias que incluyan las conclusiones que se hubiesen alcanzado sobre la causa de la muerte) o para los datos sesgados de entrada (datos y circunstancias del caso concreto en que va a actuar la IA), es probable que las conclusiones sobre la causa o causas de la muerte estén condicionadas y sesgadas por lo que su valoración como prueba deberá decaer o cuando menos minusvalorarse.



Si quieres adquirir esta obra haz click aquí

En concreto se exige en los números 3 y 4 del artículo 10 que esos conjuntos de datos: a) sean pertinentes, suficientemente representativos y, en la mayor medida posible, que carezcan de errores y sean completos en vista de la finalidad prevista para el modelo de IA; b) tengan en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice ese concreto sistema de IA de alto riesgo.

Ambas exigencias son claves en orden a la valoración de la pericial realizada por una IA. Pues hay que tener en cuenta que si el conjunto de datos de entrada en el algoritmo no reúne las características exigidas por el Reglamento (UE) sobre IA el juez podrá apreciar en relación con el ámbito del método la existencia de elementos que priven o minusvaloren el resultado probatorio alcanzado por la IA.

Así que, si el conjunto de datos de entrada y entrenamiento no es pertinente[34], no es suficientemente representativo[35], tiene errores[36] o no resulta completo para la finalidad perseguida[37], la consecuencia será que la predic-

34. La pertinencia debe interpretarse como la relación del conjunto de datos con lo que constituya el objeto de la actividad pericial que se desarrolle a través de la IA. A modo de ejemplo, si la pericia tiene por objeto determinar la causa del derrumbe de un edificio, no serán pertinentes los datos de entrenamiento o de entrada que se refieran a los contratos de arrendamiento de inmuebles de un determinado país. Sin embargo, este mismo ejemplo demuestra que en relación con la actividad de la IA no siempre resulta fácil determinar si los datos de entrenamiento son o no pertinentes en relación con la actividad de algoritmo. Pues, en el ejemplo podría considerarse que los datos sobre arrendamientos podrían de alguna manera tener una conexión, siquiera indirecta, con el análisis de la posible causa del derrumbe que se esté analizando por la IA (por ejemplo, si se considerase que la actuación de los arrendatarios de un inmueble puede, de alguna manera, condicionar o contribuir al colapso de un edificio).

35. Si el conjunto de datos de entrenamiento o de entrada no es lo suficientemente representativo las conclusiones que se extraigan por el algoritmo verán reducida su valoración en la apreciación del juzgador. El problema se encuentra sin duda en cómo determinar y dar contenido a ese concepto jurídico indeterminado de la «*suficiencia representativa*» de los datos de entrada en el modelo algorítmico.

36. Los errores en los datos de entrenamiento o de entrada condicionan directamente las conclusiones a las que pueda llegar la IA, no solo en cuanto que pueda verse reducido notablemente su valor probatorio, sino que incluso puede llegar a excluir cualquier valor como prueba en los casos en los que los errores sean especialmente graves y relevantes.

37. Esta exigencia de completitud del conjunto de datos de entrenamiento y de entrada en relación con la finalidad perseguida con el modelo de IA de alto riesgo, si bien es un elemento que el juez puede utilizar para la fundamentación de su apreciación sobre el



Si quieres adquirir esta obra haz click aquí

ción o la explicación dada por el algoritmo tendrá un menor valor probatorio que aquellos resultados de un modelo de IA cuyo conjunto de datos de entrada y entrenamiento no tenga alguna de esas carencias.

Por otra parte, en el artículo 10.4 del Reglamento (UE) 2024/1689 sobre IA se encuentra un criterio específico para la valoración de esta clase de prueba por parte del juzgador[38]: la necesidad de especificidad de los datos de entrenamiento y de entrada en relación con las características o elementos particulares del objeto de la pericial que se desarrolle a través de la IA.

Esta especificidad impone que el conjunto de datos de entrenamiento y de entrada que se suministren al algoritmo recojan específicamente las particularidades del entorno geográfico, del contexto, de la conducta o de la función en la que se va a utilizar el sistema de IA de alto riesgo. Esto supone, desde el punto de vista del examen del método de la pericial algorítmica, que el juez, en la valoración de la prueba, deberá verificar la mayor o menor especificidad de los datos manejados para otorgar un determinado valor a esa concreta pericial algorítmica, en particular cuando el juzgador pueda encontrarse con dos pericias de opinión científica contradictorias o simplemente diversas realizadas a través de IA[39].

---

valor de la prueba pericial algorítmica, en la práctica va a ser difícil aquilatar cuándo se ha cumplido o no en relación con una concreta finalidad de la pericia a través de IA. Puesto que, en definitiva, esta idea del carácter completo de los datos en relación con la finalidad perseguida con el modelo de IA de alto riesgo aparece directamente condicionada por el criterio de la suficiencia representativa de los datos. De manera que cuando los datos de entrenamiento y de entrada sean suficientemente representativos para que las conclusiones alcanzadas por la IA en esa actividad de opinión científica o técnica que es la esencia de la pericia, en principio, habrá de considerarse que el conjunto de datos será completo para la finalidad perseguida con la pericia algorítmica, por cuanto el algoritmo habrá tenido datos de entrenamiento y de entrada suficientes para alcanzar la finalidad que se le ha asignado.

38. «*Los conjuntos de datos tendrán en cuenta, en la medida necesaria para la finalidad prevista, las características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo*».

39. En estos casos, en los que dos IA hayan llegado a conclusiones diversas o incluso contrarias, el juzgador, para apreciar de forma racional el valor de la prueba pericial algorítmica, deberá atender, entre otros argumentos, al grado de especificidad de los datos de entrenamiento y de entrada. De manera que, cuando el juez constate que una de las periciales realizadas presenta mayor especificidad, atendido el objeto de la pericia, en los datos manejados para su entrenamiento y, sobre todo, en los datos de entrada del caso en concreto, esto es, en las circunstancias concurrentes en la situación que se intenta explicar o en la predicción de futuro que se solicita, es evidente que le otorgará mayor eficacia probatoria.



Si quieres adquirir esta obra haz click aquí

Por otro lado, para una adecuada valoración de la prueba pericial por parte del juez es preciso que en relación con el método científico o técnico empleado por el algoritmo se expresen en el informe u opinión que realice la IA las concretas características de la metodología usada[40].

La exigencia de este requisito de explicitación del concreto método, técnica o procedimiento que resulta aplicado por la IA es una cuestión que se vincula con la necesaria transparencia del algoritmo[41], o mejor dicho con la ineludible transparencia que debe presidir la explicación del resultado o conclusiones alcanzadas por el sistema de IA[42].

En este sentido, hay que tener presente que la necesaria transparencia del algoritmo y de su funcionamiento se encarga en el Reglamento (UE) sobre IA a las instrucciones de uso del sistema de IA de alto riesgo[43]. A efectos de lograr una adecuada transparencia sobre el funcionamiento del algoritmo, que permita la valoración de la prueba pericial algorítmica cuando el juez se encuentre con dos o más actuaciones periciales desarro-

---

40. A modo de ejemplo si se utilizase un sistema de IA de alto riesgo para determinar si una determinada persona tiene alguna enfermedad mental a través del análisis de los síntomas concurrentes será preciso que en el informe que se realice por la IA se indique qué versión de la DSM (*Diagnostic and Statistical Manual of Mental Disorders*) se ha aplicado. Pues, es claro que no tendrá el mismo valor probatorio una pericia realizada conforme a la DSM 4, que una que se haya realizado según lo previsto en la DSM 5-TR que es la última publicada. En el sentido, de que el empleo por parte de la IA de una metodología de análisis que no sea la última existente puede determinar en la convicción del juez en el momento de la apreciación de la prueba un menor valor probatorio.
41. Como establece el artículo 31.1 del Reglamento (UE) 2024/1689 sobre IA «*Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que se garantice que funcionan con un nivel de transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida*».
42. Según la norma ISO/IEC 22989: 2022 «*La explicabilidad es la propiedad de un sistema de IA que significa que los factores importantes que influyen en una decisión pueden expresarse de forma comprensible para los humanos*». La propia norma ISO/IEC 22989: 2022 destaca la trascendencia de la explicabilidad cuando señala que «*puede ser especialmente importante cuando las decisiones tomadas por un sistema de IA afectan a uno o varios humanos. Los humanos tienden a desconfiar de una decisión a menos que comprendan cómo se tomó, especialmente si la decisión les resulta adversa a nivel personal (…) La explicabilidad también puede ser un medio útil para validar el sistema de IA, incluso cuando las decisiones no afectan directamente a los humanos*».
43. «*Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue*» (artículo 13.2).



Si quieres adquirir esta obra haz click aquí

lladas con IA, resultan especialmente trascendentes dos de los contenidos que tienen que recogerse de forma necesaria en las instrucciones de uso de la IA. De un lado, como prevé el número VI del artículo 10.3 las «*especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA de alto riesgo*», y de otro lado, conforme a lo establecido en el número VII de ese mismo apartado, la «*información que permita a los responsables del despliegue interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente*».

De manera que a la hora de valorar pruebas periciales llevadas a cabo con IA el juez deberá tener en cuenta como instrumento de suma utilidad en relación con los datos de entrada todas las especificaciones e indicaciones que se contengan en las instrucciones de uso de la IA sobre el conjunto de datos de entrenamiento, validación y prueba que se hayan usado en esa IA en atención a la finalidad de ese sistema de IA de alto riesgo.

En este sentido, la exigencia de transparencia del algoritmo se extiende a los datos de entrada, esencialmente a los de entrenamiento, lo que constituye un elemento capital para que el juez pueda decidir ante dos predicciones de futuro o ante dos explicaciones de una situación pasada que resulten diferentes, o incluso contradictorias, cuál de ellas tiene mayor valor probatorio y resulta más verosímil en su predicción o explicación.

Por otro lado, desde el punto de vista de los datos de salida la exigencia de transparencia obliga a que en las instrucciones de uso se contenga información que permita interpretar los resultados de salida del sistema de IA de alto riesgo y utilizarla adecuadamente. Esta exigencia de información para la interpretación de los resultados de salida del uso de la IA se va a convertir en una pieza imprescindible para una adecuada valoración de la pericial algorítmica. Toda vez que esa información puede ser empleada para la interpretación de las conclusiones (resultados de salida) de la pericia desarrollada con IA y el juez podrá tenerla en cuenta de cara a la apreciación del valor probatorio que conceder a las distintas pericias algorítmicas que se hayan aportado al proceso.

(iii) En relación con el ámbito de las conclusiones.

La valoración de las periciales que se llevan a cabo a través de sistemas de IA requiere desde el ámbito de las conclusiones que el juez proceda a examinar si atendidas las premisas, en particular los prompts, los datos de



Si quieres adquirir esta obra haz click aquí

ESTUDIOS

En esta obra colectiva se ofrece un análisis transversal, multidisciplinar y actualizado sobre los desafíos que plantea el tratamiento de la información y los datos personales en los procesos judiciales y en los procedimientos sancionadores. A través de una estructura organizada en cuatro grandes bloques temáticos, se abordan los principales problemas que suscita el uso de la información y los datos en contextos jurídicos complejos, marcados por la transformación digital y la evolución de los instrumentos tecnológicos.

La obra presta especial atención a los límites jurídicos en el uso de la información en el proceso penal, incluyendo el respeto al derecho de defensa, la protección de la privacidad y el secreto profesional. Asimismo, se analizan los retos que plantea el uso de la información y los datos en otros ámbitos procesales, vinculados con la contratación administrativa, la responsabilidad civil o la protección de datos en el entorno empresarial y financiero.

Este volumen constituye una herramienta esencial para juristas, investigadores y operadores jurídicos interesados en comprender las implicaciones jurídicas del uso de la información y los datos en el contexto procesal contemporáneo.

**Si quieres adquirir esta obra haz click aquí**

ISBN: 978-84-1085-636-3

AENOR GESTIÓN DE LA CALIDAD ISO 9001 ER-0280/2005
IQNET RECOGNIZED CERTIFICATION
AENOR GESTIÓN AMBIENTAL ISO 14001 GA-2005/0100

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Cofinanciado por la Unión Europea
AGENCIA ESTATAL DE INVESTIGACIÓN
DATER
ARANZADI