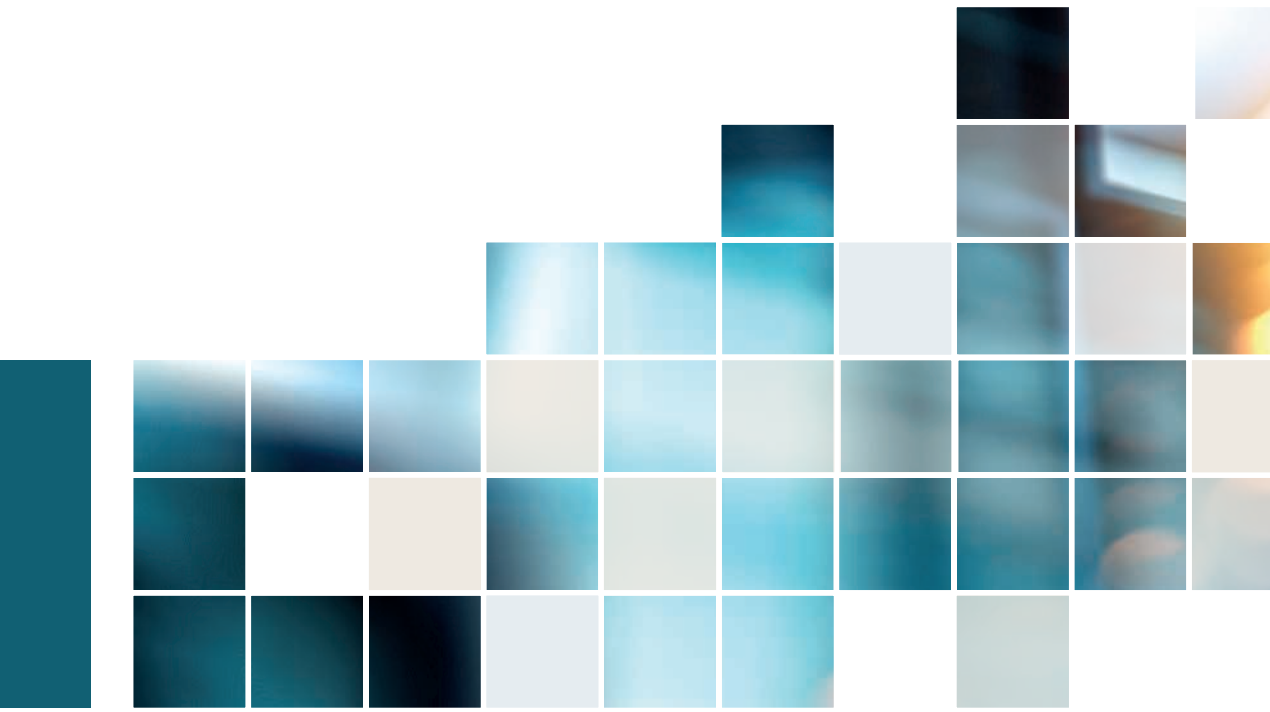
TEMAS

Derecho procesal digital

Problemas derivados de la aplicación de las tecnologías al proceso judicial

Joaquín Delgado Martín



LA LEY

© **Joaquín Delgado Martín**, 2024
© **LA LEY Soluciones Legales, S.A.U.**

LA LEY Soluciones Legales, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@aranzadilaley.es
https://www.aranzadilaley.es

Primera edición: Octubre 2024

Depósito Legal: M-20585-2024
ISBN versión impresa: 978-84-19905-98-7
ISBN versión electrónica: 978-84-19905-99-4

Diseño, Preimpresión e Impresión: LA LEY Soluciones Legales, S.A.U.
Printed in Spain

© LA LEY Soluciones Legales, 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, LA LEY Soluciones Legales, 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.

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

LA LEY SOLUCIONES LEGALES 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.

LA LEY SOLUCIONES LEGALES 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 **LA LEY Soluciones Legales, 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 SISTEMÁTICO

PARTE I
EL PROCESO DIGITAL Y EL DERECHO PROCESAL DIGITAL

PARTE VI

PRESENCIA TELEMÁTICA EN ACTOS PROCESALES

PARTE X

RETIRADA DE CONTENIDOS ILÍCITOS Y COLABORACIÓN DE LOS PRESTADORES DE SERVICIOS. EL REGLAMENTO DE SERVICIOS DIGITALES

CAPÍTULO 2

ACCESO DIGITAL A LA ADMINISTRACIÓN DE JUSTICIA

1. INTRODUCCIÓN CONCEPTUAL
2. SEDES JUDICIALES ELECTRÓNICAS
3. CARPETA JUSTICIA: ACCESO A LA INFORMACIÓN DE LA ADMINISTRACIÓN DE JUSTICIA

1. INTRODUCCIÓN CONCEPTUAL

En un sentido amplio, es la relación de las personas físicas y jurídicas con el sistema de justicia por medios electrónicos, lo que engloba **todas las posibilidades de acceso online a la información y servicios de la Administración de Justicia**: la participación por medios electrónicos en actos procesales orales (videoconferencia); las notificaciones electrónicas; la presentación de escritos por profesionales mediante el sistema Lexnet o similar, el acceso al expediente digital por los profesionales, la realización de trámites por ciudadanos/as y empresas…..En este Capítulo del libro vamos a analizar varios elementos regulados Título II del Libro Primero del DL 6/23, bajo la rúbrica «Acceso digital a la Administración de Justicia»:

a) Las sedes judiciales electrónicas y el Punto de Acceso General a la Administración de Justicia (Capítulo I);

b) La Carpeta Justicia (Capítulo II); y

c) Los sistemas de identificación y firma electrónicas para la relación online con la Administración de Justicia (Capítulo III).

2. SEDES JUDICIALES ELECTRÓNICAS

2.1. ¿Qué es y para qué sirve la sede judicial electrónica?

Según el Preámbulo del RDL 6/23, «*se mejora el concepto de sede judicial electrónica que existe en la Ley 18/2011, de 5 de julio, regulándose las características de las sedes judiciales electrónicas y sus clases, así como su contenido, servicios que han de prestar y reglas especiales de responsabilidad*».

La sede electrónica de una Administración es un entorno seguro de comunicaciones con el administrado para la realización de trámites administrativos utilizando los medios electrónicos; aunque ofrece los servicios de acceso al estado del expediente, la publicación electrónica de resoluciones y comunicaciones, así como un enlace para formular quejas y sugerencias.

El artículo 8.1 RDL 6/23 define la sede judicial electrónica (SJE) de igual manera que lo hacía el artículo 9.1 de la Ley 18/2011: «*aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a cada una de las Administraciones competentes en materia de justicia*». La finalidad principal de la sede judicial electrónica es la materialización del derecho del ciudadano a relacionarse con la Administración de justicia por medios electrónicos, pudiendo realizar en la misma diferentes actuaciones, procedimientos y servicios.

2.2. ¿Cuál es su régimen jurídico?

La regulación de la sede judicial electrónica se encuentra, en un **primer nivel**, en los artículos 8 y ss. RDL 6/23. Y un **segundo nivel** normativo se encuentra en las disposiciones del Ministerio de Justicia y de las CCAA con competencias que regulan la creación y régimen de funcionamiento de las respectivas sedes judiciales electrónicas, al amparo de lo establecido por el artículo 8.4 RDL 6/23.

El instrumento de creación de la sede judicial electrónica será accesible directamente o mediante enlace a su publicación en el BOE o en el de la Comunidad Autónoma correspondiente (art. 8.9 RDL 6/23). Y, en todo caso, con sometimiento a lo dispuesto por el artículo 38 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, que regula la sede electrónica de las Administraciones Públicas. Como ejemplo cabe señalar la Orden JUS/1126/2015, de 10 de junio, por la que se crea la sede judicial electrónica correspondiente al ámbito territorial del Ministerio de Justicia.

2.3. ¿Cuáles son las principales novedades de 2023?

- Lo más relevante es que el RDL 6/23 contempla la **conexión con las leyes procesales**, de tal manera que se adapta la normativa procesal a la existencia y funciones de la SJE.
- Se contiene una especie de **habilitación** para el establecimiento de servicios o aplicaciones que permitan realizar el trámite, presentación o actuación telemáticamente (párrafo 2.º de la Disposición adicional novena de la LEC introducida por el Decreto-Ley).
- **Acceso a la información del proceso**. Ha de incluir el «Acceso al expediente judicial electrónico, a la presentación de escritos, a la práctica de notificaciones y a la agenda de señalamientos e información, de los sistemas habilitados de videoconferencia» (letra e del artículo 8.1 y letra

d del artículo 10.1). Anteriormente solamente se hacía referencia a al acceso al estado de tramitación del expediente en los términos legalmente establecidos.

• **Conexión con el sistema de asistencia jurídica gratuita**. Ha de incluir enlace al apartado de instrucciones o gestión de cita para la solicitud de asistencia jurídica gratuita (artículo 10.2-l).

2.4. ¿Qué es el Punto de Acceso General de la Administración de Justicia?

El RDL 6/23 contempla en su artículo 12 el **Punto de Acceso General de la Administración de Justicia**, que ya se regulaba en el artículo 13 de la Ley 18/2011 y al que puede acceder a través del enlace que figura en esta nota[(1)], cuya gestión se encomienda al Ministerio de la Presidencia, Justicia y Relaciones con las Cortes conforme a los acuerdos que se adopten en el Comité técnico estatal de la Administración judicial electrónica (CTAJE). El propio artículo 12 lo define como un portal orientado a los ciudadanos y ciudadanas que dispondrá de su sede electrónica que, como mínimo, contendrá la Carpeta Justicia y el directorio de las sedes judiciales electrónicas que, en este ámbito, faciliten el acceso a los servicios, procedimientos e informaciones accesibles correspondientes a la Administración de Justicia, al Consejo General del Poder Judicial, a la Fiscalía General del Estado y a los organismos públicos vinculados o dependientes de la misma, así como a las administraciones con competencias en materia de Justicia. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras administraciones públicas o corporaciones que representen los intereses de los y las profesionales que se relacionan con la Administración de Justicia, mediante la celebración de los correspondientes convenios.

En la nueva normativa se introducen las siguientes **novedades** relevantes:

• Debe garantizarse la interoperabilidad con los posibles puntos ubicados en los portales habilitados por cada administración competente.

• Responderá a los principios de accesibilidad universal y claridad de la información.

• Incluirá contenidos dirigidos a colectivos vulnerables, especialmente a niños, niñas y adolescentes, que pudieran ser de su interés.

• Ofrecerá al ciudadano o ciudadana, al menos, un servicio de consulta de expedientes en los que figure como parte en procedimientos

(1) Véase https://www.administraciondejusticia.gob.es

judiciales, y en todo caso la posibilidad de conocer y acceder a recibir las notificaciones de todos los órganos judiciales.

• Se ofrecerá a las personas jurídicas, cuyo volumen de causas pudiera dificultar una gestión a través del punto de acceso general, sistemas específicos en función de niveles de volumen de expedientes o de áreas de gestión en atención a los referidos acuerdos que se adopten conforme al apartado 2 de este artículo[2].

Se trata de un elemento de especial importancia para garantizar que todos los ciudadanos del Estado pueden **acceder online a la información** sobre la Administración de Justicia, así como sobre los procesos judiciales en los que figuren como parte (consulta de procedimientos y notificaciones) y, por tanto, desde cualquier lugar y en cualquier tiempo. **Su eficacia real dependerá del establecimiento de una interoperabilidad efectiva** entre el Punto de Acceso General y las Administraciones prestacionales, el Consejo General del Poder Judicial, la Fiscalía General del Estado y colegios profesionales; con fundamento en convenios que garanticen las dimensiones de la interoperabilidad: técnica y semántico-jurídica. En este sentido, cabe recordar que el Anexo RDL 6/23 define interoperabilidad como «*capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos*».

2.5. ¿Qué actos de trámite puede realizar una persona en la sede judicial electrónica?

El RDL 6/23 contiene un principio general relevante (párrafo 2.º de la Disposición adicional novena de la LEC): «*Las referencias que la presente ley u otras hagan a la sede de la oficina judicial, o del Juzgado o Tribunal, se entenderán efectuadas también a la sede judicial electrónica y a la Carpeta Justicia, cuando ésta o aquélla dispongan de los servicios o aplicaciones que permitan realizar el trámite, presentación o actuación telemáticamente*». En definitiva, **cualquier acto procesal podría ser realizado en la SJE siempre que la Administración establezca los medios para su realización online**; y añado que **siempre que se respeten los requisitos establecidos por las leyes procesales**.

(2) Estimamos que se refiere al apartado 1 del artículo 12.

CAPÍTULO 2

FASES DE LA PRUEBA DIGITAL

1. FASE DE OBTENCIÓN DE LA PRUEBA
2. FASE DE APORTACIÓN AL PROCESO
3. FASE DE VALORACIÓN JUDICIAL

1. FASE DE OBTENCIÓN DE LA PRUEBA

Esta primera fase consiste en la obtención de los datos o información producidos, almacenados o transmitidos, mediante el acceso a las fuentes de la prueba electrónica o digital antes de su incorporación al proceso; recordemos la gran heterogeneidad de estas fuentes. En esta fase, las partes (o la autoridad pública en el ámbito penal y de forma excepcional en otras jurisdicciones) han de acceder a la información o datos de forma lícita, es decir, sin violación de derechos fundamentales.

La concreta modalidad de obtención (acceso a los datos) dependerá a la específica fuente probatoria: acceso a dispositivos electrónicos; acceso a datos de Redes Sociales o de sitios web; aportación de datos propios (mails, conversaciones de mensajería instantánea como whatsapp y similares…).

En el proceso civil, el **principio de aportación de parte** determina que cada una elegirá cómo obtener las fuentes de prueba y qué medios probatorios propone. Pero las partes se encuentran con graves problema de obtención de determinadas pruebas digitales. Cabe recordar que la naturaleza primordialmente dispositiva del proceso civil determina que la investigación previa de las pruebas[(1)] corresponda exclusivamente a las partes, salvo las limitadas facultades de las diligencias finales[(2)]. Son las partes quienes deben realizar las actividades de obtención de la información fuera del proceso y generalmente antes de éste, quienes únicamente pueden acceder a aquellas informaciones que resulten legalmente accesibles[(3)]; sin perjuicio de determinadas actuaciones preparatorias de la prueba que pueden solicitarse al juez, especialmente a través de las diligencias preliminares.

---

(1) Esta investigación previa se concreta en la actividad de la parte destinada a descubrir las fuentes de la prueba digital y preparar su posterior proposición como prueba.

(2) Hernando DEVIS ECHANDÍA, *Teoría General de la Prueba judicial*, Tomo I, Víctor P. De Zabalía Editor, Buenos Aires, página 278.

(3) Manuel RICHARD GONZÁLEZ recuerda que *«en el proceso civil el problema consiste en la ausencia de normas legales que permitan realizar una adecuada investigación de los*

1.1. Dificultades de acceso a la prueba digital en el proceso civil

El principal problema radica en las dificultades para acceder a determinadas fuentes de prueba, dado que las partes carecen del carácter de autoridad o funcionario público (a diferencia de lo que ocurre con las investigaciones en el proceso penal).

En la práctica, cada una de las partes realiza fuera del proceso la investigación de los hechos que han de ser objeto de prueba en el proceso civil, de forma que puede requerir el acceso a datos (fuentes de prueba) contenidos en soportes electrónicos o transmitidos por redes de comunicación; y la parte interesada propondrá posteriormente como prueba la incorporación de dichos datos al proceso (a través del medio probatorio que considere procedente). De esta manera, y con carácter general, la parte del proceso civil aportará como prueba los datos que se contienen en fuentes abiertas al público (por ejemplo, determinadas páginas web) o que se encuentren en sus propios dispositivos electrónicos, sin perjuicio del registro de dispositivos en el ámbito laboral. En otros casos será más difícil su obtención para su ulterior incorporación al proceso.

La Ley de Enjuiciamiento Civil no contempla con carácter general el procedimiento para que una parte pueda acceder a los datos (en formato electrónico) que se encuentren en poder de otra parte o de un tercero, ya sea para su aportación como prueba al proceso, ya sea para la práctica de una pericial de parte, de tal forma que se posibilite el examen de dichos datos por el perito para la elaboración del dictamen. Dicha Ley solamente recoge algunos supuestos puntuales y diversos de tutela anticipatoria que tienen por objeto una finalidad preparatoria, asegurativa o probatoria[4]: diligencias preliminares cuya normativa reguladora (arts. 256 a 263 LEC), aunque contiene un *numerus clausus*, permite una interpretación de cada uno de los supuestos del art. 256 LEC adaptada a la realidad social (art. 3.1 del Código Civil), de tal forma que puedan referirse a la obtención de este tipo de datos si se entiende que, dentro de la categoría de «documentos» prevista por algunas de dichas medidas, se incluyen también aquéllos que se encuentren en

hechos electrónicos ante el límite que supone por una parte la plena vigencia de los derechos fundamentales que impiden que un Juez civil pueda acordar ninguna clase de intervención o mandato para interferir o intervenir de ningún modo las comunicaciones de una persona en un proceso civil»; en «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal* 43 (2017).

(4) Así lo recuerda Sonia PUIG FAURA, quien también expone los diferentes supuestos, en «El acceso del perito informático-forense a fuentes de prueba en poder de terceros. Análisis del apartado 5.º del art. 336 LEC tras la reforma de la LEC por la Ley 42/2015 de 5 de octubre», *Diario La Ley*, n.º 8808, Sección Práctica Forense, 21 de julio de 2016.

soporte digital (documentos electrónicos)[5]; y diligencias preliminares relativas a la obtención de datos que pueden solicitarse en materia de propiedad intelectual o de propiedad industrial que se contienen en los apartados 7, 8, 10 y 11 del art. 256.1 LEC; todo ello sin perjuicio de los supuestos de deber de exhibición documental, o incluso de determinadas medidas de aseguramiento de prueba o de medidas cautelares.

1.2. Licitud en la obtención

El segundo gran problema se localiza en la llamada prueba digital ilícita. El acceso a las fuentes de la prueba electrónica (obtención de la información o datos por las partes), antes de su aportación al proceso, ha de realizarse con pleno respeto de los derechos fundamentales (licitud), especialmente el derecho a la intimidad y el derecho al secreto de comunicaciones; así como sobre el derecho a la autodeterminación informativa en el ámbito de la protección de datos personales (art. 18.4 CE) y el derecho a la propia imagen en determinados supuestos de captación y grabación de imágenes.

Téngase en cuenta que los derechos fundamentales también tienen vigencia en las relaciones entre ciudadanos o entre éstos y entidades no investidas de poder público (eficacia horizontal de los derechos fundamentales o *Drittwirkung*).

En principio, la prueba digital ilícita es nula, extendiéndose esa nulidad a aquellas pruebas con las que exista una conexión de antijuridicidad. Esta nulidad puede ser apreciada de oficio por el Juez (art. 240.2 LOPJ y art. 287.1, 2.º LEC), o puede ser solicitada por una parte procesal legitimada. Aunque es necesario tener en cuenta que el Tribunal Constituciones ha desarrollado la llamada «doctrina Falciani», que introduce matices relevantes en dicho principio general; pero su examen excede el objeto de este trabajo.

1.3. Fiabilidad

Cuando el Juez procede a la valoración de la prueba electrónica conforme a las reglas de la sana crítica, habrá de atender especialmente a dos carac-

(5) A esta idea se refiere Manuel DÍAZ MARTÍNEZ cuando, al comentar la exhibición de documentos del supuesto del art. 256.1, 4.º LEC, afirma que aparece «*el objeto de exhibición designado genéricamente bajo la fórmula de "documentos y cuentas", si bien, entendemos que puede ampliarse a toda clase de antecedentes, tales como contratos, correspondencia, libros, etc., e incluso de soportes materiales no documentales donde se recojan las cuentas de la sociedad (disquetes informáticos, hojas de cálculo, etc.)*», en «Las diligencias preliminares: supuestos y requisitos de la solicitud», *Práctica de Tribunales*, n.º 40, Sección Estudios, julio-agosto 2007.

terísticas: la autenticidad del origen y la integridad del contenido. Si concurren dudas sobre la autenticidad y/o integridad de los datos, resultará muy probable que el Juez deniegue fuerza o eficacia probatoria a la prueba[6].

A estos conceptos se refiere el art. 382.2 LEC cuando se refiere a *«la autenticidad y exactitud de lo reproducido»* (aplicable por expresa remisión del art. 384.2 LEC); el art. 588 sexies c.1 LECRIM cuando dispone que la autorización judicial *«fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial»;* así como la propia Ley Orgánica del Poder Judicial, cuyo art. 230.2 establece que *«los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales»*.

1.3.1. Autenticidad

Tradicionalmente llamamos autenticidad del documento a la coincidencia de su autor aparente con su autor real[7]. En el ámbito de la prueba electrónica, cabe definirse como la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos[8].

Si de la valoración conjunta de los elementos probatorios se deducen circunstancias que llevan al Juez a dudar de la autenticidad de la prueba electrónica practicada, la aplicación de la sana crítica (reglas de la razón) le conducirá a negar fuerza probatoria.

1.3.2. Integridad

Por integridad de la prueba electrónica cabe entender la propiedad o característica consistente en que los datos (activo de información) no han sido alterados de manera no autorizada[9]. En definitiva, se trata de aplicar la

(6) Josefina QUEVEDO GONZÁLEZ se refiere al «*juicio de fiabilidad*», que «*pretende analizar la fiabilidad de todo el material probatorio, en el sentido de que la información, el dato, el archivo sobre el que ha de recaer la convicción judicial, no venga viciado de inveracidad*»; en «Investigación y prueba del ciberdelito», Sepin, 2017, página 232.

(7) Emilio GÓMEZ ORBANEJA, *Derecho Procesal. Volumen I Derecho Procesal Civil*, 4.ª edición, Madrid, página 323.

(8) Definición del Anexo del RDL 6/23.

(9) Véase la definición contenida en el Anexo del RDL 6/23.

construcción de la cadena de custodia a este ámbito: la preservación de los datos.

En caso de que, tras la práctica de los medios probatorios, surgieran elementos que determinaran que ha existido una manipulación de la prueba electrónica, la sana crítica (reglas de la razón) también determinará probablemente que el Juez niegue eficacia probatoria.

1.3.3. Garantías de autenticidad e integridad

Para cualquier análisis de los datos contenidos en un dispositivo electrónico, es necesario realizar un proceso de «copia forense»: captura de todos los datos de la fuente de la evidencia electrónica, de manera que ésta permanezca inalterada; tras lo cual se puede practicar el informe pericial correspondiente, por unidades policiales especializadas o por peritos informáticos no públicos. Existen determinadas normas internacionales para ello: RFC 3227 (2002) Directrices para la recopilación de evidencias y su almacenamiento; ISO/IEC 27037 (2012) Guía para la Identificación, recolección, adquisición y preservación de evidencia digital.

El principal instrumento técnico al efecto es el **código hash**, que se calcula a partir de un algoritmo de cifrado estándar (MD5, SHA-1, SHA-256, SHA-512,...) que posibilita concluir que los datos hallados en el dispositivo en el momento de su aprehensión no han sido objeto de ulterior manipulación. Se trata de un algoritmo matemático que se realiza sobre el conjunto de los datos contenidos en un concreto dispositivo o soporte digital: el resultado genera un valor de 32 o más dígitos de tal forma que, si se modifica un solo bit del conjunto de datos sobre el que se ha realizado, el valor del hash es diferente.

2. FASE DE APORTACIÓN AL PROCESO

La segunda fase radica en la incorporación al proceso de la información o datos obtenidos que sean relevantes para la acreditación de hechos. De esta manera, cabe hablar de tres tipos de requisitos en esta fase:

- Por un lado, la pertinencia y la necesidad, que resulta de aplicación en cualquier jurisdicción y con independencia de la normativa procesal aplicable;
- Por otra parte, licitud, entendida como el respeto a los derechos fundamentales durante la práctica del concreto medio probatorio;

CAPÍTULO 4

PRESENCIA TELEMÁTICA EN LA COOPERACIÓN JUDICIAL INTERNACIONAL

1. ÁMBITO CIVIL
2. ÁMBITO PENAL

1. ÁMBITO CIVIL

1.1. Unión Europea

Resultan de aplicación los artículos 10.4 y 17.4 del Reglamento 1206/2001, de 28 de mayo de 2001, relativo a cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la **obtención de pruebas en materia civil o mercantil**, que permiten de forma explícita la práctica de pruebas mediante videoconferencia[1]. Cabe recordar que es aplicable a todos los Estados miembros de la UE, a excepción de Dinamarca.

A.– En primer lugar, se contempla su uso en la **ejecución de la solicitud de obtención de prueba por parte del órgano judicial del Estado requerido**. En este supuesto, el artículo 10.4 dispone lo siguiente:

> *El órgano jurisdiccional requerido cumplirá dicha petición, a no ser que ésta sea incompatible con el Derecho del Estado miembro del órgano jurisdiccional requerido o que existan grandes dificultades de hecho.*
>
> *En caso de que el órgano jurisdiccional requerido no acceda a la petición por alguno de los motivos arriba citados, informará al órgano jurisdiccional requirente mediante el formulario E que figura en el anexo.*
>
> *Si en el órgano jurisdiccional requirente o requerido no se dispone de acceso a los medios técnicos mencionados anteriormente, los órganos jurisdiccionales podrán facilitarlos de mutuo acuerdo.*

B.– En segundo lugar, es posible en los casos de **obtención directa de pruebas por el órgano jurisdiccional requirente.** En estos supuestos, el artículo 17.4,3.º dispone que «*el órgano central o la autoridad competente fomentará la utilización de los medios tecnológicos de comunicación como videoconferencias y teleconferencias*». Es decir, en estos casos, es posible

(1) Javier GARCÍA SANZ y Javier GONZÁLEZ GUIMARAES-DA SILVA, «Las "vistas telemáticas" en el proceso civil español: visión comparada, regulación y cuestiones prácticas que suscita su celebración», *Diario La Ley*, N.º 9659, Sección Plan de Choque de la Justicia / Tribuna, 23 de Junio de 2020, Wolters Kluwer.

que el órgano judicial requirente realice por sí mismo la prueba por videoconferencia con persona que se encuentre en el Estado requerido; aunque con pleno sometimiento el régimen jurídico contemplado en el artículo 17.

1.2. Conferencia de la Haya de Derecho Internacional Privado (HCCH)

Hay que acudir al Convenio relativo a la obtención de pruebas en el extranjero en materia civil o mercantil, hecho en La Haya el 18 de marzo de 1970. ¿Cuál el estado actual de los Estados que lo han ratificado? véase el sitio web de la HCCH[(2)].

Aunque la Convención sobre la Prueba no contiene ninguna referencia específica al uso de la videoconferencia, lo cierto es que su utilización está permitida para las Comisiones Rogatorias[(3)]. Pese a ello, la Conferencia de la Haya de Derecho Internacional Privado (HCCH) publicó la Guía de Buenas Prácticas sobre el uso de las videoconferencias bajo la Convención de 1970 (2020)[(4)].

1.3. Iberoamérica

Cuando la autoridad judicial estime necesario examinar a una persona en el marco de un proceso judicial, en calidad de parte, testigo o perito, y ésta se encontrare en otro Estado de Iberoamérica, podrá solicitar su declaración por videoconferencia con fundamento en el Convenio Iberoamericano sobre el uso de la videoconferencia en la Cooperación Internacional entre Sistemas de Justicia, hecho en Mar del Plata el 3 de diciembre de 2010 (BOE de 13 de agosto de 2014). Y también es aplicable el Tratado de Medellín de 25 de julio de 2019 relativo a la transmisión electrónica de solicitudes de cooperación jurídica internacional entre Autoridades Centrales.

Véanse el resto de informaciones que se contienen en el apartado de Iberoamérica de la cooperación penal.

1.4. Otros ámbitos territoriales

En caso de inexistencia de convenio internacional aplicable, cabe acudir a las disposiciones previstas en la Ley 29/2015, de 30 de julio, de cooperación jurídica internacional en materia civil. Su artículo 30, al regular el con-

(2) https://www.hcch.net/es/instruments/conventions/status-table/?cid=82
(3) Guía de Buenas Prácticas sobre el uso de las videoconferencias bajo la Convención de 1970 (2020), página 37 https://www.hcch.net/en/news-archive/details/?varevent=728
(4) https://www.hcch.net/en/news-archive/details/?varevent=728

tenido de la solicitud para la práctica y obtención de pruebas, se refiere a «c) *La indicación de si se solicita el uso de medios tecnológicos de comunicación*».

2. ÁMBITO PENAL

El uso de la videoconferencia está muy extendido en la cooperación judicial internacional para testigos, peritos, víctimas e inculpados que se encuentran en el extranjero. La Comisión Rogatoria Internacional o solicitud de asistencia judicial mutua deberá fundamentarse en un instrumento internacional aplicable. En este sentido, el apartado 44 de la «Guía para la celebración de actuaciones judiciales telemáticas» recuerda que «para la intervención telemática de personas que se encuentren fuera de España, es aconsejable recabar el auxilio judicial internacional».

2.1. Unión Europea

En relación con **testigos, peritos o investigados/encausados que se encuentran en otro Estado miembro de la UE**, la Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, contempla la posibilidad de práctica mediante videoconferencia (artículo 24) o incluso por conferencia telefónica (artículo 25). Esta Directiva fue transpuesta en el ordenamiento interno español por la Ley 3/2018, de 11 de junio, que añadió un Título X a la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.

En este sentido, el artículo 197 de la Ley 23/14 se refiere a emisión de la orden para que la declaración del investigado o encausado o de un testigo o perito se realice «por videoconferencia u otros medios de transmisión audiovisual»; y el artículo 216 de dicha Ley regula la ejecución en España de una orden europea de investigación para una comparecencia por videoconferencia u otros medios de transmisión audiovisual.

2.1.1. OEI: España como Estado de emisión

La emisión de una orden europea de investigación para una comparecencia por videoconferencia u otros medios de transmisión audiovisual está regulada en el artículo 197 de la Ley 23/14, para los supuestos en los que la autoridad competente española que esté conociendo de un proceso penal en España considere necesario oír al investigado o encausado o a un testigo o

perito que se encuentre en el territorio de otro Estado miembro; conteniendo las siguientes reglas:

• Colaboración: las disposiciones prácticas con arreglo a las cuales se llevará a cabo la comparecencia se determinarán de acuerdo con la autoridad de ejecución competente.

• Medios técnicos: si en un caso concreto la autoridad de ejecución no dispusiera de los medios técnicos necesarios para celebrar la comparecencia por videoconferencia u otros medios de transmisión audiovisual, la autoridad competente española que la hubiera solicitado podrá ponerlos a su disposición previo acuerdo.

2.1.2. OEI: España como Estado de ejecución

La ejecución de una orden europea de investigación para una comparecencia por videoconferencia u otros medios de transmisión audiovisual está regulada en el artículo 216 de la Ley 23/14.

Causas de denegación. La autoridad española competente denegará el reconocimiento y ejecución de la orden europea de investigación para una comparecencia por videoconferencia u otros medios de transmisión audiovisual:

• Supuestos previstos en el apartado 1 del artículo 32 (motivos generales para la denegación del reconocimiento o la ejecución de las medidas solicitadas) y en el artículo 207 (causas de denegación del reconocimiento y ejecución de la orden europea de investigación);

• En caso de que la **ejecución de dicha medida de investigación en un caso concreto sea contraria a los principios jurídicos fundamentales del Derecho español**; y

• Si el investigado o el acusado **no da su consentimiento** para la práctica de la medida.

Forma de realización:

• Cuando la autoridad competente española reciba una orden europea de investigación en la que se solicite una comparecencia por videoconferencia u otros medios de transmisión audiovisual, la llevará a cabo en la forma que hubiera acordado con la autoridad de emisión. En todo caso, la autoridad competente española se encargará de:

– Notificar la medida al testigo o perito correspondiente, indicando el momento y el lugar de la comparecencia.

– Citar a las personas investigadas o encausadas para que asistan a la comparecencia conforme a las normas específicas que establezca el Derecho español, e informarles de sus derechos con arreglo al Derecho del Estado de emisión, con tiempo suficiente para que puedan acogerse efectivamente a las garantías procesales.

– Asegurarse de la identidad de la persona que deba prestar declaración.

• La autoridad española competente se pondrá de acuerdo con la autoridad de emisión sobre la práctica de la ejecución de la medida que, en todo caso, se regirá por las siguientes normas:

– Durante la declaración estará presente la autoridad española competente, asistida por un intérprete cuando sea necesario, para identificar a la persona que deba prestar declaración y velar por el respeto del ordenamiento jurídico español.

– La autoridad española competente acordará, en su caso, con la autoridad de emisión, la adopción de medidas de protección de la persona que deba declarar.

– La declaración tendrá lugar ante la autoridad competente del Estado de emisión o bajo su dirección.

– Si así lo solicita la autoridad de emisión o la persona compareciente, la autoridad española facilitará un intérprete para que le asista.

– Con carácter previo a la declaración, se informará a los testigos o peritos de los derechos procesales que les asisten al amparo tanto del Derecho del Estado de emisión como del español, incluido el derecho a no declarar cuando así se disponga.

• Finalizada la declaración, la autoridad española en cuyo territorio se haya ejecutado la medida levantará acta de la misma, en la que constarán la fecha y el lugar, la identidad de la persona oída, la identidad del resto de personas que hayan participado, el juramento formulado y las condiciones técnicas en las que se haya llevado a cabo la declaración. El acta se transmitirá a la autoridad competente del Estado de emisión.

• En el caso de que la persona que deba ser oída en España en ejecución de una orden europea de investigación no preste testimonio estando sometida a la obligación de testificar o no preste testimonio veraz, se le aplicará el ordenamiento jurídico español del mismo modo

que si la comparecencia se hubiera celebrado dentro de un proceso nacional.

2.2. Iberoamérica

Cuando la autoridad judicial estime necesario examinar a una persona en el marco de un proceso judicial, en calidad de parte, testigo o perito, o en diligencias preliminares de investigación, y ésta se encontrare en otro Estado de Iberoamérica, podrá solicitar su declaración por videoconferencia con fundamento en el Convenio Iberoamericano sobre el uso de la videoconferencia en la Cooperación Internacional entre Sistemas de Justicia, hecho en Mar del Plata el 3 de diciembre de 2010 (BOE de 13 de agosto de 2014).

Los Estados que lo han ratificado son los siguientes[5]: Panamá (16 mayo 2011); México (7 julio 2011); España (27 octubre 2011); República Dominicana (7 septiembre 2012); Ecuador (5 marzo 2014); Costa Rica (26 abril 2016); Paraguay (14 septiembre 2018). Argentina lo aprueba por Ley 27162 del 15 de julio de 2015. Pendiente el depósito del instrumento de ratificación. El Salvador lo aprueba por ley de 26 enero de 2011, pero no se ha hecho el depósito del instrumento de ratificación. Nicaragua depositó el instrumento de adhesión el 7 de noviembre de 2022.

La remisión de la solicitud puede hacerse por medios electrónicos a través de la plataforma contemplada en el Tratado de Medellín de 25 de julio de 2019 relativo a la transmisión electrónica de solicitudes de cooperación jurídica internacional entre Autoridades Centrales. Como se examina en otro lugar (apartado 4.1 del Capítulo 1 de la Parte IX de esta obra), este tratado regula el uso de la plataforma electrónica Iber@ como medio formal y preferente de transmisión de solicitudes de cooperación jurídica internacional entre Autoridades Centrales, en el marco de los tratados vigentes entre las partes y que contemplen la comunicación directa entre dichas instituciones (artículo 1).

2.3. Otros ámbitos territoriales

También existen disposiciones que contemplan la videoconferencia en diferentes convenios internacionales ratificados por España. A título de ejemplo, cabe destacar la Convención de las Naciones Unidas contra la Delin-

(5) file:///C:/Users/joaqu/Downloads/Estado%20de%20tratados%20COMJIB%20(1).pdf

cuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000, cuyo artículo 18.18 establece lo siguiente: «*Siempre que sea posible y compatible con los principios fundamentales del derecho interno, cuando una persona se encuentre en el territorio de un Estado Parte y tenga que prestar declaración como testigo o perito ante autoridades judiciales de otro Estado Parte, el primer Estado Parte, a solicitud del otro, podrá permitir que la audiencia se celebre por videoconferencia si no es posible o conveniente que la persona en cuestión comparezca personalmente en el territorio del Estado Parte requirente. Los Estados Parte podrán convenir en que la audiencia esté a cargo de una autoridad judicial del Estado Parte requirente y en que asista a ella una autoridad judicial del Estado Parte requerido*».

2.4. Futuro próximo de la videoconferencia en la cooperación penal

2.4.1. Unión Europea: nueva normativa sobre digitalización de la cooperación judicial

Cabe destacar la aprobación del Reglamento (UE) 2023/2844, de 13 de diciembre de 2023, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial (publicado en el DOUE de 27-12-23); que será **aplicable a partir del 1 de mayo de 2025**. Este Reglamento se complementa con la Directiva (UE) 2023/2843 de 13 de diciembre de 2023, dado que el nuevo sistema diseñado en el Reglamento afecta a normas ya incorporadas al ordenamiento jurídico interno de los Estados miembros siguiendo la obligación de transposición de determinadas Decisiones Marco y Directivas. Esta normativa se examina en la Parte IX de esta monografía.

2.4.2. Segundo Protocolo Adicional a la Convención sobre la Cibercriminalidad

Fue firmado por 22 Estados (entre ellos España) el 12 de mayo de 2022, y se encuentra abierto el proceso de ratificación por parte de los países, de tal manera que el convenio entrará en vigor cuando se ratifique por cinco Estados[(6)]. Actualmente solo ha sido ratificado por Serbia y Japón[(7)].

(6) Véase mi trabajo sobre «Presente y futuro de la prueba digital internacional. El Segundo Protocolo Adicional del Convenio de Budapest contra la cibercriminalidad», *Diario La Ley*, N.º 62, Sección Ciberderecho, 24 de mayo de 2022.

(7) https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

Este Segundo Protocolo contiene una regulación de la videoconferencia en su artículo 11. Se puede utilizar para la declaración de un testigo o un perito; aunque puede ser utilizada para fines distintos, incluso para identificar personas u objeto; o para la audiencia de un sospechoso o acusado, si lo admite la Parte requerida. Admite la remisión electrónica de la solicitud entre las autoridades centrales. Los procedimientos para la realización de la videoconferencia especificados por la Parte Requirente serán de aplicación a menos que sean incompatibles con la legislación interna de la Parte requerida. Cuando una Parte requerida opte por permitir la audiencia de un sospechoso o acusado, podrá solicitar condiciones y garantías específicas en cuanto a la recogida de testimonios o la declaración de la persona, o prever notificaciones o solicitudes de medidas procesales sobre esta persona. El Segundo Protocolo también permite la posibilidad de aplicar estas disposiciones a la audioconferencia (artículo 11.7).

CAPÍTULO 1

AUTOMATIZACIÓN, ROBOTIZACIÓN E INTELIGENCIA ARTIFICIAL

1. INTRODUCCIÓN Y ELEMENTO CONCEPTUALES
2. NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES
3. REGULACIÓN EN LA LEY ORGÁNICA DEL PODER JUDICIAL
4. NORMATIVA PROCESAL
5. NORMATIVA SOBRE EFICIENCIA PROCESAL

1. INTRODUCCIÓN Y ELEMENTO CONCEPTUALES

1.1. Objeto

Independientemente de las diferentes concepciones de la inteligencia artificial, nosotros nos vamos a referir a la **utilización de tecnologías que automatizan la decisión o ayudan a la decisión en el proceso judicial, tanto en la tramitación del procedimiento como en las resoluciones de fondo**.

1.2. Delimitación conceptual

Automatizar es aplicar la automática a un proceso, es decir, aplicar en un proceso un elemento que funciona por sí solo sin intervención humana[(1)]. Pues bien, dentro de esta concepción general caben distintas tecnologías: la automatización de procesos; la automatización robótica de procesos (RPA); las diferentes modalidades de sistemas expertos; y la inteligencia artificial basada en redes neuronales (Natural Networks), Aprendizaje Automatizados (Machine Learning) y/o Procesamiento de Lenguaje Natural (Natural Language Processing).

La **inteligencia artificial** (IA) es un conjunto de tecnologías de rápida evolución[(2)] que permite dotar a las máquinas de la posibilidad de resolver problemas de manera similar a un cerebro humano. Desde este perspectiva general, la ciencia y la técnica han de desarrollado una serie de herramientas, entre las que destacan: las redes neuronales (Neural Networks), inspiradas en la estructura y funcionamiento del cerebro humano, y que son utilizadas para reconocer patrones en conjuntos de datos complejos, el Aprendizaje

(1) Carles RAMIÓ MATAS destaca que «*la inteligencia artificial y la robótica pueden ser la gran oportunidad para implantar una renovación institucional y organizativa radical de las instituciones públicas y contribuir a su adaptación, a su relevancia y a su supervivencia en un contexto complejo de gobernanza*»; en *Inteligencia artificial, robótica y modelos de Administración pública*, CLAD, 2018, https://www.redalyc.org/journal/3575/357559243001

(2) Considerando 1 de la DECISIÓN DE LA COMISIÓN de 24 de enero de 2024 por la que se crea la Oficina Europea de Inteligencia Artificial.

Automatizados (Machine Learning), que posibilita a los sistemas informáticos aprender y mejorar automáticamente a partir de la experiencia; y el Procesamiento de Lenguaje Natural (Natural Language Processing) que permita a los sistemas informáticos entender, interpretar y generar lenguaje humano.

La **automatización robótica de procesos** (RPA o robótica de *software*) es un método para automatizar procesos transaccionales basados en reglas específicas, mediante la utilización de robots de *software* virtuales, también conocidos como robots digitales o bots, para que realicen tareas o trabajos manuales que consumen tiempo. Un bot de *software* es un programa de computadora diseñado para realizar acciones específicas; creados para realizar actividades simples o complejas, los bots automatizan procesos que implican tareas repetitivas. Entre los beneficios que aporta la implantación de RPA destaca[3]:

- Automatización de tareas simples y repetitivas que por su naturaleza conducen a errores, permitiendo a los órganos judiciales dedicar su tiempo a otras tareas donde sus capacidades pueden aportar un mayor valor.
- Implantación ligera y rápida, siendo una tecnología no invasiva y que no requiere de adaptación en la arquitectura tecnológica, sino que se relacionan como una capa superior sin necesidad de adaptar y/o modificar las aplicaciones subyacentes.
- Mejora general del rendimiento en los procesos, al eliminarse los cuellos de botella en procesos arduos y manuales y la capacidad de emplearse 24/7.

En el ámbito judicial, se está empleando RPA en la automatización de procesos de distinta naturaleza y con beneficio en diversos agentes del ecosistema judicial. Entre los procesos en los cuales ya están implantadas soluciones automatizadas destacan[4]:

- Transmisión automatizada de resguardos de operaciones entre el Sistema de Cuentas de Depósitos y Consignaciones Judiciales (CDCJ) y el Sistema de Gestión Procesal Minerva para distintas operaciones de las CDCJ.
- Automatización del registro y reparto de iniciadores de asuntos de monitorios civiles en las Oficinas de Registro y Reparto.

(3) https://www.administraciondejusticia.gob.es/-/robotizacion-de-procesos-judiciales
(4) https://www.administraciondejusticia.gob.es/-/robotizacion-de-procesos-judiciales

• Apoyo automatizado en la tramitación de procedimientos de monitorios civiles en los órganos judiciales.

• Automatización de la satisfacción extraprocesal para procedimientos de recursos contencioso-administrativos ante la Audiencia Nacional de denegaciones de nacionalidad por residencia.

• Automatización del registro, reparto y tramitación de las solicitudes derivadas de la Ley 8/2021 de revisión de las medidas de discapacidad en los procedimientos judiciales.

• Automatización de la gestión de las subastas electrónicas en la Unidad de Subastas Electrónicas de Murcia.

• Procedimiento automático de las peticiones que proceden de órdenes europeas de investigación (OEI) a través del Sistema Europeo de Información de Antecedentes Penales (Portal eDES) y traspaso de las peticiones al Portal CJI-Cris para su tramitación.

Hay que tener en cuenta que mientras la RPA se fundamenta en procesos, la IA se basa en datos. Los bots de RPA solo pueden seguir los procesos que define un usuario final, mientras que los bots de IA utilizan machine learning para reconocer patrones en los datos, en particular en datos no estructurados, y aprenden con el tiempo. Dicho de otra manera, la IA está destinada a simular la inteligencia humana, mientras que la RPA sirve únicamente para replicar tareas dirigidas por humanos. Si bien el uso de herramientas de inteligencia artificial y RPA minimiza la necesidad de intervención humana, la forma en que automatizan los procesos es diferente[5]. Aunque la RPA y la IA tienen un amplio margen de complemento entre ellas. La IA puede ayudar a la RPA a automatizar tareas de un modo más completo y gestionar casos de uso más complejos. Además, la RPA puede servir para agilizar la respuesta ante la información obtenida mediante IA, en lugar de tener que esperar a las implementaciones manuales.

1.3. Normativa aplicable

En la actualidad, el paraguas normativo de la aplicación a la justicia de sistemas de automatización y de IA está compuesto por los siguientes elementos:

• Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (RIA).

• Reglamento General de Protección de Datos (RGPD).

(5) https://www.ibm.com/es-es/topics/rpa

- RDL 6/23 sobre Eficiencia Digital.
- Normas complementarias aprobadas por el Comité Técnico Estatal de Administración Judicial Electrónica (CTEAJE).

2. NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Resulta plenamente aplicable la normativa de protección de datos personales relativa a las decisiones automatizadas: el artículo 22 del Reglamento (UE) 2016/679 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), y el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[6]; en cuanto no se oponen a las especificidades contenidas en la LOPJ. Ambas normativas tienen un contenido muy similar.

El Reglamento General de Protección de Datos (RGPD), en sus Considerandos 71 y 71 así como en su artículo 22, limita y establece los derechos de los sujetos relativos a que los datos no sean sometidos a decisiones exclusivamente automatizadas que tengan efectos jurídicos o que afecten significativamente al interesado. En este sentido, la elaboración de perfiles de forma automática se incluye en este marco de decisiones automatizadas; en todo caso ha de tenerse en cuenta que las decisiones automatizadas pueden llevarse a cabo con o sin elaboración de perfiles, mientras que la elaboración de perfiles puede darse sin realizar decisiones automatizadas. Las Directrices del Grupo de Trabajo del artículo 29 citan el siguiente ejemplo: la imposición de multas por exceso de velocidad únicamente sobre la base de las pruebas

(6) El artículo 14 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, establece lo siguiente:
1. *Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.*
2. *Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*
3. *Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13*.

de los radares de velocidad es un proceso de decisiones automatizadas que no implica necesariamente la elaboración de perfiles; sin embargo, puede convertirse en una decisión basada en la elaboración de perfiles si los hábitos de conducción de la persona se supervisan a lo largo del tiempo y, por ejemplo, la cuantía de la multa impuesta es el resultado de una evaluación que implique otros factores, como si el exceso de velocidad es un caso de reincidencia o si el conductor ha cometido otras infracciones de tráfico recientemente.

Como principio general, el artículo 22.1 RGPD reconoce que «*todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*». De esta manera, viene a **prohibir la decisión basada únicamente en el tratamiento automatizado** que produzca efectos jurídicos en la persona o le afecte significativamente de modo similar. **Aunque lo permite cuando la decisión**:

a) es necesaria para la celebración o la ejecución de un **contrato** entre el interesado y un responsable del tratamiento;

b) está **autorizada por el Derecho de la Unión o de los Estados miembros** que se aplique al responsable del tratamiento y que establezca asimismo **medidas adecuadas** para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o

c) se basa en el **consentimiento explícito del interesado**.

En los casos en que sean posibles las decisiones automatizadas (letras a, b y c mencionadas), las mismas no se basarán en las **categorías especiales de datos personales** contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado (artículo 22.4 RGPD).

Por último, en los casos a que se refieren letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el **derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión**.

En este sentido, el Artículo 18 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,

dispone que «*el derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679*».

Según las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, elaboradas por el Grupo de Trabajo sobre protección de datos del artículo 29 (3 de octubre de 2017 y revisadas), estas decisiones automatizadas pueden basarse en cualquier tipo de datos, citando los ofrecidos directamente por las personas afectadas (como las respuestas a un cuestionario); o los observados acerca de las personas (como los datos sobre la ubicación recogidos a través de una aplicación); o bien los derivados o inferidos como, por ejemplo, un perfil ya existente de la persona (por ejemplo, una calificación crediticia). En todo caso, las decisiones automatizadas adoptadas en el seno de un proceso judicial han de basarse únicamente en los datos o informaciones obrantes en el proceso, que se hayan incorporado al mismo con pleno respeto de los derechos de las partes y las garantías procesales.

3. REGULACIÓN EN LA LEY ORGÁNICA DEL PODER JUDICIAL

La LOPJ no contiene referencia alguna a la inteligencia artificial, pero sí realiza dos alusiones a las actuaciones automatizadas:

3.1. IA para la gestión de recursos y el seguimiento de las actuaciones del sistema de justicia

El primer inciso del artículo 236 sexies.4 LOPJ dispone que «el Ministerio de Justicia y las Comunidades Autónomas con competencias en la materia, dentro de las políticas de apoyo a la Administración de Justicia y desarrollo de la gestión electrónica de los procedimientos, podrán realizar el tratamiento de datos no personales para el ejercicio de sus competencias de gestión pública…». De esta manera, las Administraciones prestacionales pueden utilizar sistemas IA para la adecuada gestión de los medios materiales y personales de la Administración de Justicia; y ello «permitirá a las Administraciones implicadas utilizar sistemas de IA que se nutran de los datos que dispongan en los respectivos aplicativos que dan soporte a los juzgados y tribunales, con la finalidad de llevar a cabo políticas de gestión públicas, basadas en la información que aporten el uso de estas herramientas de IA como puede ser, el conocimiento de la incidencia de criminalidad de una determinada zona para que, en atención a ello, se refuercen los órganos

jurisdiccionales, así como adelantarse a posibles colapsos de las jurisdicciones, o, valorar el posible impacto de una normativa específica en relación a la carga de trabajo de las sedes judiciales, entre muchas otras» (7).

Y, por otro lado, el último párrafo del artículo 461.3 dispone que «los sistemas informáticos de gestión procesal de la Administración de Justicia permitirán en todo caso la extracción automatizada de la totalidad de los datos exigidos en los correspondientes boletines estadísticos». Ello posibilitará la realización de un seguimiento de la evolución de la actividad de los juzgados y tribunales y de la oficina judicial, y facilitará la propia labor de inspección.

3.2. IA para la clasificación documental en el procedimiento

Por otro lado, el mismo artículo se refiere a los sistemas automáticos de **clasificación documental** orientados a la tramitación procesal. La clasificación documental es el proceso mediante el cual se organiza la información contenida en los documentos, otorgándoles una ubicación específica en un sistema creado para tal fin, agrupándolos por conceptos o asuntos concretos. En definitiva, se trata de aplicar sistemas automatizados y/o de IA para clasificar los diferentes documentos del proceso con la finalidad de facilitar su uso en la tramitación de los procedimientos (8), abarcando tres funciones materiales (todos ellas con un amplio margen de automatización o robotización):

1. Examen del documento para conocer sus contenidos.
2. Realización de una síntesis de los citados contenidos en un tema principal.
3. Contrastar este tema principal o materia con un lenguaje clasificatorio, para establecer qué específica categoría es la más próxima; y representar el documento mediante la notación propia de la clasificación; posibilitando tanto el almacenamiento ordenado como la recuperación del documento.

(7) Román GARCÍA-VARELA IGLESIAS, «La (futura) legislación sobre IA: cuestiones sobre la prueba y la responsabilidad derivada de su uso», *LA LEY Probática* n.º 7, enero-marzo 2022, N.º 7, 1 de enero de 2022, página 8.

(8) Rodrigo SÁNCHEZ JIMÉNEZ, «*Se puede definir la Clasificación Automática de Documentos, también denominada categorización de textos o topic spotting, como la tarea de asignar automáticamente un conjunto de documentos a una o más categorías preexistentes a través de un conjunto de documentos clasificados por expertos sobre los que el sistema lleva a cabo un proceso de aprendizaje supervisado*»; en «La documentación en el proceso de evaluación de Sistemas de Clasificación Automática», Documentación de las Ciencias de la Información 2007, vol. 30, 25-44.

CAPÍTULO 1

COLABORACIÓN CON LAS AUTORIDADES PENALES EN EL REGLAMENTO DE SERVICIOS DIGITALES (DSA)

1. SOBRE EL DSA
2. ÓRDENES DE ENTREGA DE INFORMACIÓN
3. NOTIFICACIÓN DE SOSPECHAS DE DELITOS

1. SOBRE EL DSA

El Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales[1] (Reglamento de Servicios Digitales-DSA) es aplicable desde el día 17 de febrero de 2024.

El DSA resulta de aplicación a las entidades prestadoras de servicios de intermediación, es decir, que tienen como objeto la mera puesta a disposición de información o la puesta en contacto de usuarios: facilitan el servicio de acceso a Internet; trasmiten datos por redes de telecomunicaciones; realizan copias temporales de las páginas de Internet solicitadas por los usuarios; o bien alojan en sus propios servidores datos, aplicaciones o servicios suministrados por otras personas o entidades. Su característica principal radica, con carácter general, en su falta de responsabilidad por los contenidos de los usuarios, sin perjuicio del deber de cumplimiento de las condiciones y obligaciones impuestas por el DSA[2].

1.1. Ámbito de aplicación: prestadores de servicios afectados

El DSA afecta a los **servicios intermediarios** ofrecidos a **destinatarios del servicio que tengan su lugar de establecimiento o estén situados en la Unión**, con independencia de donde los prestadores de dichos servicios intermediarios tengan su lugar de establecimiento (artículo 2).

---

(1) Lourdes ORTEGA, «El nuevo reglamento europeo de mercados digitales: regulación de las plataformas digitales en el nuevo entorno tecnológico», *Revista General de Derecho de los Sectores Regulados 10,* 2022.

(2) Como afirma Estrella TORAL LARA, se consagra el principio de «ausencia de responsabilidad» por las actuaciones de terceros, por lo que la responsabilidad de los intermediarios podrá establecerse solo cuando concurra su propia y no diligente actuación frente a las conductas examinadas. Es decir, cuando a pesar de conocer su ilicitud no la evitan ni la impiden, según su posición; en *Obligaciones de los proveedores de servicios*, *Práctica de Derecho de Daños* n.º 153, Sección Consulta de los suscriptores, Cuarto trimestre de 2022, LA LEY.

Su Artículo 3 g) define «servicio intermediario» como uno de los siguientes servicios de la sociedad de la información:

> i) **un servicio de «mera transmisión»,** consistente en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones,
>
> ii) **un servicio de «memoria caché»**, consistente en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, prestado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos,
>
> iii) **un servicio de «alojamiento de datos»**, consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este.

Entre estos servicios de intermediación, los que probablemente tengan más incidencia en el ámbito objeto de estas reflexiones son las llamadas **plataformas en línea**, como pueden ser las redes sociales o los mercados online que ofrecen los productos de terceros. Téngase en cuenta que estos mercados online almacenan información proporcionada por los destinatarios del servicio a petición suya, y además la difunden al público también a petición de los destinatarios del servicio.

Según el Considerando 13 DSA, los prestadores de servicios de alojamiento de datos no deben ser considerados plataformas en línea cuando la difusión al público sea tan solo una característica menor o meramente accesoria que esté inextricablemente unida a otro servicio o una funcionalidad menor del servicio principal, y dicha característica o funcionalidad no pueda utilizarse, por razones técnicas objetivas, sin ese otro servicio o servicio principal, y la integración de dicha característica o funcionalidad no sea un medio para eludir la aplicabilidad de las disposiciones del DSA aplicables a las plataformas en línea. Por ejemplo, la sección de comentarios de un periódico en línea podría ser una característica de esta índole, cuando no quepa duda de que es auxiliar al servicio principal constituido por la publicación de noticias bajo la responsabilidad editorial del editor. En cambio, el almacenamiento de comentarios en una red social debe ser considerado un servicio de plataforma en línea cuando quede claro que no es una característica menor del servicio ofrecido, aunque sea accesorio a la publicación de las entradas de los destinatarios del servicio.

A efectos del DSA, los servicios de computación en nube o de alojamiento web no deben ser considerados plataformas en línea cuando la difusión al público de información específica constituya una característica menor y auxiliar o una funcionalidad menor de dichos servicios.

1.2. Colaboración voluntaria

El artículo 7 DSA, referido a las investigaciones voluntarias por iniciativa propia y cumplimiento del Derecho, dispone lo siguiente: «*No se considerará que los prestadores de servicios intermediarios no reúnen las condiciones para acogerse a las exenciones de responsabilidad a que se refieren los artículos 4, 5 y 6 por la única razón de que realicen, de buena fe y de modo diligente, investigaciones por iniciativa propia de forma voluntaria, o adopten medidas con el fin de detectar, identificar y retirar contenidos ilícitos, o bloquear el acceso a estos, o adoptar las medidas necesarias para cumplir los requisitos del Derecho de la Unión y del Derecho nacional en cumplimiento del Derecho de la Unión, incluidos los requisitos establecidos en el presente Reglamento*».

1.2.1. Relevancia

Como puede observarse, el DSA permite que los prestadores de servicios de intermediación realicen investigaciones voluntarias para detectar contenidos ilícitos; así como que procedan a la retirada de dichos contenidos de forma también voluntaria.

Estas actuaciones vienen realizándose por determinados prestadores de servicios de comunicaciones interpersonales, como el correo web, los servicios de mensajería y/o de servicios de redes sociales (Microsoft, Facebook, Twitter-X, Adobe….), de conformidad con su propia política corporativa. Se trata del uso de determinados instrumentos automatizados para filtrar contenidos, metadatos y/o datos de tráfico de comunicaciones con la finalidad de detectar contenidos sospechosos de ser constitutivos de delito. Cabe destacar especialmente que utilizan de forma voluntaria tecnologías específicas con el fin de detectar el abuso sexual de menores en línea cometido en sus servicios y denunciarlo a las autoridades policiales y a las organizaciones que actúan en interés público contra los abusos sexuales de menores, escaneando el contenido, incluidas imágenes y texto, o los datos de tráfico de las comunicaciones, mediante el uso, en algunos casos, de datos históricos. Una vez detectado el material ilícito, se pone en conocimiento de autoridades policiales o judiciales del Estado competente.

Como afirma el Considerando 8 del Reglamento (UE) 2021/1232, de 14 de julio, a pesar de que su objetivo sea legítimo, las actividades voluntarias de los proveedores para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos representan una injerencia en los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales de todos los usuarios de servicios de comunicaciones interpersonales independientes de la numeración. Ninguna limitación del ejercicio del derecho fundamental al respeto a la vida privada y familiar, incluida la confidencialidad de las comunicaciones, puede encontrar justificación en el mero hecho de que los proveedores empleasen determinadas tecnologías en un momento en el que los servicios de comunicaciones interpersonales independientes de la numeración no estaban comprendidos en la definición de «servicios de comunicaciones electrónicas». Dichas limitaciones son posibles únicamente en determinadas circunstancias. En virtud del artículo 52, apartado 1, de la Carta, dichas limitaciones deben estar establecidas por la ley y respetar el contenido de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. Y cuando tales limitaciones impliquen con carácter permanente el seguimiento y análisis general e indiscriminado del contenido de las comunicaciones de todos los usuarios, constituyen una injerencia en el derecho a la confidencialidad de las comunicaciones.

1.2.2. Afectación a derechos fundamentales

Los tipos de tecnologías utilizadas deben ser los menos intrusivos para la intimidad a la vista del estado de la técnica en el sector. Dichas tecnologías no deben emplearse para filtrar y escanear sistemáticamente el texto de las comunicaciones, salvo con el fin de detectar pautas que apunten a posibles razones concretas para sospechar de abuso sexual de menores en línea, y no deben poder deducir la sustancia del contenido de las comunicaciones. En el caso de la tecnología utilizada para identificar el embaucamiento de menores, tales razones concretas de sospecha deben basarse en factores de riesgo identificados objetivamente, como la diferencia de edad y la probable participación de un menor en la comunicación escaneada[(3)].

Teniendo en cuenta que estas actuaciones voluntarias representan una restricción de los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales de los usuarios de servicios

(3) Considerando 16 del Reglamento (UE) 2021/1232, de 14 de julio.

de comunicaciones interpersonales, cabe aludir al Reglamento (UE) 2021/1232 de 14 de julio de 2021 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración[4] para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea. Este Reglamento tiene como objeto permitir a determinados proveedores de servicios de comunicaciones interpersonales usar, sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, tecnologías específicas para el tratamiento de datos personales y de otro tipo en la medida estrictamente necesaria para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y para retirar el material de abuso sexual de menores en línea de sus servicios (art. 1.1). Esta excepción es aplicable hasta el 3 de abril de 2026[5].

1.2.3. Modalidades

Una primera posibilidad de actuaciones se centra sobre **los motores de búsqueda** (Google, Yahoo o Bing), utilizando sistemas de bloqueo de información mediante el control de términos empleados en motores de búsqueda, mediante la detección de hasta 100.000 vocablos[6].

También cae destacar el seguimiento de la huella digital mediante la comparación del hash de los archivos ilícitos (especialmente en materia de pornografía infantil) en **redes P2P**, que fue admitida por la jurisprudencia y posteriormente recogida por el artículo 588 ter k LECRIM[7]. Sin embargo, esta actividad policial determinó que los investigados por pornografía infantil

(4) Servicio de comunicaciones interpersonales independientes de la numeración: «*servicio de comunicaciones interpersonales que no conecta a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permite la comunicación con un número o números de los planes de numeración nacional o internacional*» (artículo 2.7 de la Directiva 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas).

(5) El Reglamento (UE) 2024/1307 del Parlamento Europeo y del Consejo, de 29 de abril de 2024, ha modificado el Reglamento (UE) 2021/1232 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE, de tal manera que éste será aplicable hasta el 3 de abril de 2026.

(6) José Luis RODRÍGUEZ LAINZ, «Reflexiones sobre el tratamiento de datos personales por prestadores de servicios de comunicaciones vía internet para la lucha contra abusos sexuales de menores en línea en el Reglamento (UE) 2021/1232», *Diario La Ley* n.º 9974, 20 de diciembre de 2021.

(7) El artículo 588 ter k LECRIM, referido a la identificación mediante número IP, dispone lo siguiente: «*Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una*

trasladaran el intercambio de materiales a repositorios virtuales compartidos[8].

De esta manera, la actividad de investigación se centra en **repositorios virtuales** con la utilización de tecnología de funciones de resumen (hashing) para imágenes y vídeos: se compara el hash de los archivos (base de datos con material verificado de abuso sexual de menores) con los hashes de otros archivos de los repositorios virtuales[9].

En último lugar, se están desarrollando **clasificadores e inteligencia artificial para el análisis de textos o datos de tráfico**. Se trata de la clasificación por procedimientos de inteligencia artificial (aprendizaje automático) para evaluar y predecir si un determinado archivo contiene elementos de pornografía infantil o abuso de menores[10].

---

dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso».

(8) José Luis RODRÍGUEZ LAINZ, «Reflexiones sobre el tratamiento…», trabajo citado.

(9) Juan Carlos ORTIZ PRADILLO explica de forma amplia que este tipo de tecnología es usada por los servicios de Microsoft (incluidos Bing y Onedrive) y por otros prestadores de servicios como Facebook, Twitter, Adobe y Gmail de Google; que Apple ha decidido desarrollar una herramienta llamada NeuralHash para escanear cuentas de iCloud de sus usuarios para la busca y captura de contenido pedófilo; y que Youtube cuenta con sistemas automatizados de detección de videos con imágenes de explotación sexual infantil o de extremismo terrorista; en «Inteligencia artificial, macrodatos y metadatos en las investigaciones policiales y en el proceso penal»; en: *La tecnología y la inteligencia artificial al servicio del proceso*. Pilar Martín Ríos y otros. Editorial Colex, A Coruña, 1.ª ed., 2023, pág. 252.

(10) José Luis RODRÍGUEZ LAINZ se refiere al *CSAM Image Classifier*. Explica que «esta herramienta, facilitada por la *Fundación Thorn —Digital Defenders of Children—*, se sustenta en una clasificación de aprendizaje automático, por procedimientos de inteligencia artificial, que permite evaluar y predecir si un determinado archivo contiene imágenes de pornografía infantil o abuso de menores. La comparativa se realiza sobre conjuntos de datos correspondientes a cientos de miles de imágenes, incluida la pornografía para adultos, CSAM y varias *imágenes benignas*; con lo que el abanico de posibilidades de detección se expande más allá de hashes plenamente identificados o pequeñas variantes de los mismos, hasta alcanzar a imágenes hasta entonces desconocidas. El procedimiento genera hashes criptográficos y perceptivos para imágenes; comparando éstos con hashes CSAM conocidos. El hashing, al igual que sucede en el *CSAMDetection System* de Apple, se lleva a cabo en la infraestructura propia del cliente asociado para mantener en la medida de lo posible su privacidad. El sistema cuenta asimismo con la misma herramienta comparativa aplicada a archivos de vídeo, el *Video Hash Matching*; a la vez que un sistema de compartición de información, el *SaferList for Detection*, que permite comparar los hashes aportados por los distintos clientes asociados, ampliando así las capacidades de detección»; en «Reflexiones sobre el tratamiento…», trabajo citado.

Esta obra pretende ofrecer a los profesionales del Derecho las herramientas necesarias para enfrentarse a los problemas que plantea la aplicación de las tecnologías en el proceso judicial, desde una perspectiva procesal.

Está plenamente adaptada a las numerosas reformas normativas e iniciativas regulatorias que afectan al proceso, tanto nacionales como de la Unión Europea: e-justicia, presencia telemática en vistas y juicios, expediente judicial electrónico y eficiencia digital (RDL 6/23); confianza y seguridad digital mediante identificación electrónica, firma electrónica… (Reglamento eIDAS y su modificación por el Reglamento 2024/1183 llamado eIDAS2); protección de datos personales (RGPD, LO 7/21…); digitalización de la cooperación judicial internacional (Reglamento 2023/2844, e-CODEX, Tratado de Medellín…); inteligencia artificial (Reglamento IA); nuevos instrumentos internacionales de lucha contra la ciberdelincuencia (Reglamento e-Evidence, Convenio de Budapest y su Segundo Protocolo…); retirada de contenidos ilícitos y colaboración de prestadores de servicios (Reglamento de Servicios Digitales-DSA y Directiva 2024/1385 sobre la lucha contra la violencia contra las mujeres).

ISBN: 978-84-19905-98-7

AENOR ER Empresa Registrada ISO 9001 ER-0280/2005
IQNet
AENOR Gestión Ambiental ISO 14001 GA-2005/0100

LA LEY