



Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

Protección de Datos en el Ámbito de la
Administración de Justicia y de su
Transformación Digital

Trabajo fin de estudio presentado por:	Beltrán Moyano, Nicolás Eloy
Tipo de trabajo:	Trabajo Individual
Directora:	María Lidia Suárez Espino
Fecha:	13/7/2022

Resumen

El objetivo consiste en analizar aspectos centrales relativos a la implementación del derecho de protección de datos en la Administración de Justicia en España, particularmente, en su relación con el Derecho procesal, el principio de publicidad y la transformación digital. Al efecto, se desarrollan un conjunto de aproximaciones conceptuales que combinan aspectos normativos, doctrinales y técnicos, a fin de identificar características distintivas, núcleos tensión y posibles abordajes. En una primera etapa, se describe la relación existente entre protección de datos y Administración de Justicia, los conceptos centrales que rigen el tratamiento a nivel procesal y la vinculación con principio de publicidad. En una segunda etapa, se abordan aristas de la transformación digital de la Justicia y su impacto en la protección de datos y, en ese marco, se identifican oportunidades que brindan para la mejora de la Justicia, las tecnologías big data, inteligencia artificial y blockchain, y sus desafíos asociados.

Palabras clave: Protección de Datos-Justicia-Proceso-Transformación Digital-Big Data

Abstract

The objective is to analyze central aspects related to the implementation of the right to data protection in the Administration of Justice in Spain, in particular, in its relationship with procedural law, the principle of publicity and digital transformation. To this effect, a set of conceptual approaches is developed that combine normative, doctrinal and technical aspects, in order to identify distinctive characteristics, nuclei of tension and possible approaches. In a first stage, the relationship between data protection and the Administration of Justice is described, the central concepts that govern the treatment at the procedural level and the link with the principle of publicity. In a second stage, aspects of the digital transformation of Justice and its impact on data protection will be addressed and, within this framework, opportunities will be identified that will provide for the improvement of Justice, big data technologies, artificial intelligence and blockchain, and its associated challenges.

Keywords: Data Protection-Justice-Process-Digital Transformation-Big Data

Índice de contenidos

1. Introducción	1
1.1. Justificación del tema elegido.....	2
1.2. Problema y finalidad del trabajo.....	3
1.3. Objetivos	4
1.3.1 Objetivo general	4
1.3.2 Objetivos específicos	4
2. Marco teórico y desarrollo	5
2.1 Derecho a la protección de datos personales y Administración de Justicia	5
2.1.1 Derecho fundamental a la protección de datos en Europa	5
2.1.2 Derecho fundamental a la protección de datos en España	6
2.1.3 Administración de Justicia y protección de datos: Régimen Jurídico	7
2.1.4 Particularidades del derecho a la protección de datos a nivel judicial	9
2.2 Tratamiento de datos por la Administración de Justicia a nivel procesal	10
2.2.1 Tipos de ficheros.....	11
2.2.2 Datos “sensibles”	11
2.2.3 Responsables y encargados del tratamiento	12
2.2.4 Autoridades de control.....	12
2.2.5 Delegado de protección de datos	12
2.2.6 Bases jurídicas del tratamiento	13
2.2.7 Ejercicio de derechos.....	13
2.2.8 El problema de la legislación aplicable.....	14
2.3 Publicidad de las actuaciones y protección de datos	15
2.3.1 Regulación del principio de publicidad a nivel procesal	16

2.3.2	Acceso al expediente judicial y las sentencias en la LOPJ	17
2.4	Transformación digital de la Justicia: actualidad	18
2.4.1	Actualidad de la transformación digital	18
2.4.2	Asistencia telemática a las actuaciones judiciales	20
2.4.3	Acceso al expediente judicial electrónico (LexNET)	23
2.4.4	Acceso a sentencias contenidas en bases de datos públicas	25
2.5	Tecnologías disruptivas: oportunidades y desafíos	26
2.5.1	Big data (macro datos)	27
2.5.2	Inteligencia artificial	32
2.5.3	Blockchain (cadena de bloques)	35
3.	Conclusiones	38
	Referencias bibliográficas	41
	Listado de abreviaturas	52

1. Introducción

La aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD) y de la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante la LOPDGDD), representaron un avance muy significativo en la consolidación y garantía del derecho fundamental a la protección de datos tanto, en el ámbito de lo privado, como ante la Administración Pública en general. Sin embargo, estas disposiciones no prevén un conjunto específico de normas para la implementación integral de tal derecho, en el contexto de la Administración de Justicia.

Esto último, es relevante, pues la Justicia como Poder del Estado se rige por principios tales como la independencia en el ejercicio de sus funciones y la publicidad de las actuaciones, aspectos cuya singularidad, en ocasiones, pueden resultar difícilmente compatibles con el régimen de protección datos personales y la vigencia del sistema general de garantía y control.

Complementariamente, en el marco específico del proceso judicial, se da la característica que el derecho a la protección de datos se encuentra a la par de otros bienes jurídicos protegidos, como la tutela judicial efectiva o la publicidad procesal lo cual, en casos concretos, puede traducirse en una exigente labor de ponderación para los Juzgados y Tribunales a fin de establecer el equilibrio entre los diversos derechos e intereses en juego.

De igual manera, debe tenerse en cuenta que el proceso judicial es público por naturaleza, no obstante, no así todos los datos que en él se tratan, con la particularidad de que estos pueden no concernir de manera exclusiva a las partes y, por tanto, aludir a información personal de terceros vinculados al proceso (ej. testigos, peritos, víctimas indirectas, etc.).

Así, de las consideraciones enunciadas, se desprende en una primera aproximación el por qué se entiende relevante el abordaje del derecho a la protección de datos en el ámbito judicial, más aún, considerando que se trata de un sector del Estado en actual desarrollo y con múltiples desafíos por delante.

En este último sentido, a las complejidades que suscita la implementación procesal de la protección de datos, deben sumarse las emergentes de la transformación digital de la Justicia, aspecto de especial relevancia en el marco de la crisis generada por el COVID-19.

Así, la implementación de las nuevas tecnologías de la información y la comunicación (en adelante TIC) ha impuesto la necesidad de una adaptación tanto, de las categorías procesales, como de los medios materiales y humanos requeridos al efecto. Pues, a medida que avanza el desarrollo tecnológico, también se incrementan las oportunidades y desafíos asociados.

Al respecto, los Estados enfrentan el reto de construir un sistema de Justicia a la altura del Siglo XXI, capaz de integrar soluciones tecnológicas acompañadas de regulaciones normativas idóneas para limitar usos poco éticos o contrarios a libertades fundamentales y, al mismo tiempo, que permitan fortalecer el control de derechos de la ciudadanía.

En relación a esto último, cada día adquieren mayor relevancia las soluciones derivadas de la aplicación de sistemas big data, inteligencia artificial (en adelante IA) y tecnologías blockchain. No obstante, al tiempo que representan una oportunidad para la mejora de la Justicia, plantean interrogantes en relación a la protección de datos, situación que, precisamente, despierta un especial interés que inspira este trabajo.

1.1.JUSTIFICACIÓN DEL TEMA ELEGIDO

El interrogante que surge en este punto es ¿por qué se entiende importante el abordaje del derecho a la protección de datos en el ámbito de la Administración de Justicia?

En primer lugar, se da que la Justicia como sector, procesa una gran cantidad de información de carácter personal, incluyendo datos especialmente protegidos que son aportados por los justiciables de manera voluntaria o a solicitud del órgano competente, lo cual es propio de la naturaleza de los asuntos que en este ámbito se dirimen.

En segundo lugar, por aplicación del principio institucional de publicidad de las actuaciones, gracias a las TIC, se ha desarrollado lo que se conoce como difusión pública de la información judicial a través de internet.

Al respecto, se trata de un tema que despierta un creciente interés tanto, para los profesionales del Derecho, como también para sectores empresariales (particularmente, la

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital
rama de seguros) financieros (bancos, entidades de crédito, registros de información crediticia) editoriales, e incluso para las nuevas sociedades de la información¹, pues todos ellos comparten el entendimiento de que el manejo de la información, particularmente, de carácter judicial, puede aportar valor a sus productos y servicios (MIRA ROS 2012).

Asimismo, el acceso a expedientes judiciales a través de la red, expone los datos personales a los peligros del ciberespacio y a la posible vulnerabilidad de la infraestructura tecnológica de la Administración de Justicia, de ahí su importancia conforme a las graves consecuencias que pueden derivarse para los derechos y libertades de los ciudadanos.

Precisamente, en España, durante el año 2021 se produjeron una media de 40.000 ciberataques diarios, lo que supuso un incremento del 125 por ciento con respecto al año anterior, según informa Datos101².

Por último, en el marco de la transformación digital, pueden mencionarse al menos dos temas de relevancia rodeados de múltiples interrogantes. Por un lado, la utilización de sistemas big data e IA para la gestión masiva y automatizada de datos judiciales que, por ejemplo, ha dado lugar a lo que se conoce como Justicia predictiva, actualmente aplicable en España, dentro sector legal privado, pero en debate sobre su utilización en el ámbito de la Administración de Justicia. Y, por otro lado, la aplicación de tecnologías blockchain, que presentan importantes potencialidades en materia probatoria, integridad de documentos incorporados al expediente judicial electrónico, seguridad de la información, entre otras. En resumen, estos son algunos de los aspectos que permiten comprender la importancia del abordaje que se propone.

1.2.PROBLEMA Y FINALIDAD DEL TRABAJO

El problema de investigación puede describirse en relación a la siguiente pregunta: ¿cuáles son las principales características y núcleos de tensión que presenta la implementación del derecho a la protección de datos en el ámbito de la Justicia y de su transformación digital?

¹Por ejemplo, para el análisis de riesgos que puede engendrar una determinada operación económico-financiera.

²El año de los grandes ciberataques en España. Disponible en: <https://www.elmundo.es/tecnologia/2021/12/01/61a63b4ae4d4d8db5a8b4577.html> [Consulta: 1 de marzo de 2022].

Así, considerando lo descrito en la introducción, puede decirse que la falta de previsión en el RGPD y la LOPDGDD de una normativa específica integral, la incompatibilidad de ciertos principios institucionales que rigen a la Administración de Justicia y que se proyectan a nivel procesal, y las dificultades que plantea la transformación digital, son los algunos de los aspectos que integran el problema que se pretende abordar a través del presente trabajo.

En este marco, la finalidad se orienta a conocer desde diversas perspectivas el estado de actualidad de este tema, sus características singulares y principales núcleos de tensión para, posteriormente, aportar conclusiones los temas desarrollados.

1.3.OBJETIVOS

1.3.1 Objetivo general

El objetivo consiste en analizar la implementación del derecho a la protección de datos en el ámbito de la Administración de Justicia, particularmente, en su relación con el Derecho procesal, el principio institucional de publicidad de las actuaciones y la transformación digital.

1.3.2 Objetivos específicos

Conforme al objetivo general descrito, se proponen los siguientes objetivos específicos:

- a. Describir el marco de regulación del derecho a la protección de datos en el ámbito de la Administración de Justicia.
- b. Identificar características principales sobre el tratamiento de datos a nivel procesal y en relación al principio de publicidad de actuaciones.
- c. Describir características y riesgos para la protección de datos en el marco de la transformación digital de la Justicia.
- d. Indagar sobre posibles aplicaciones de sistemas big data, IA y tecnologías blockchain para la mejora de la Justicia e identificar desafíos que, en general, surgen para la protección de datos.
- e. Aportar conclusiones a los temas planteados.

2. Marco teórico y desarrollo

Conforme a lo desarrollado en la introducción, particularmente, los aspectos identificados como relevantes y que justifican este trabajo, se propone un abordaje del marco teórico en dos grandes etapas.

La primera, orientada a describir y analizar la relación existente entre el derecho a la protección de datos y la Administración de Justicia: su régimen jurídico, aspectos distintivos, conceptos centrales que rigen el tratamiento de datos a nivel procesal y particularidades que se dan en relación al principio de publicidad de las actuaciones judiciales. En esta primera etapa se toma referencia normativa de mayor importancia, a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante LOPJ).

Por su parte, la segunda etapa, se encauza al abordaje de ciertas aristas y dificultades que plantea la transformación digital de la Justicia a la protección de datos y, posteriormente, se identifican oportunidades que podrían surgir para la mejora del sistema judicial a través de la aplicación de sistemas big data, IA y tecnologías blockchain.

2.1 DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y ADMINISTRACIÓN DE JUSTICIA

2.1.1 Derecho fundamental a la protección de datos en Europa

A nivel de la Unión Europea (en adelante UE), fruto de un extenso proceso histórico de desarrollo normativo y jurisprudencial, el derecho a la protección de datos como derecho fundamental, se encuentra receptado en el artículo 8³ de la Carta de Derechos Fundamentales de la UE (en adelante CDFUE) aprobada en el año 2000 y que goza de efecto jurídico vinculante para los Estados miembro, desde el año 2009 en virtud de la entrada vigor del Tratado de

³Que establece que: “1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley [...] 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente” (CDFUE).

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital Lisboa (MARCOS AYJÓN 2013). En términos similares, se encuentra receptado en el artículo 16⁴ del Tratado de Funcionamiento de la UE (en adelante TFUE) del año 2010 (ARENAS 2006).

Así, del análisis de ambas disposiciones, se identifica la existencia de conjunto aspectos centrales que dan contenido al derecho a la protección de datos, como el tratamiento de “modo leal”, para “fines específicos”, “sobre la base del consentimiento u otro fundamento legítimo” y “sujeto al control de una autoridad independiente” (ÁLVAREZ HERNANDO 2020).

Cabe recordar que, a nivel de la UE, las disposiciones mencionadas se desarrollan en general, a través del RGPD.

2.1.2 Derecho fundamental a la protección de datos en España

En el ámbito español la recepción del derecho a la protección de datos surge implícita del artículo 18.4 de la Constitución Española⁵(en adelante CE), pues así lo entiende el Tribunal Constitucional que, a través de su jurisprudencia, lo desarrolla y le da forma como derecho fundamental e incluso, le reconoce autonomía e independencia en relación al derecho a la intimidad⁶ (RALLO LOMBARTÉ 2019).

En tal sentido, dicho órgano, lo define como “un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o un particular, o cuáles puede este tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o su uso. Su carácter de derecho fundamental le otorga determinadas características, como la de ser irrenunciable y el hecho de prevalecer sobre otros derechos no fundamentales” (FJ 7 STC 292/2000)⁷.

Así, del análisis de esta definición, se desprende que el derecho a la protección de datos se integra a su vez de un conjunto de facultades cuyo ejercicio impone ciertos deberes jurídicos

⁴Que establece que: “1. Toda persona tiene derecho a la protección de los datos [...]. 2. [...]. El respeto de dichas normas estará sometido al control de autoridades independientes [...]” (TFUE).

⁵Que establece que: “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” (CE).

⁶A diferencia, por ejemplo, de Alemania cuya jurisprudencia reconoce el derecho a la protección de datos, pero como integrante de otro derecho fundamental, como puede ser la vida privada, la dignidad humana, entre otros.

⁷Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332> [Consulta: 5 de marzo de 2022].

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

a terceros, sentido en el que se entienden los derechos de acceso, rectificación, supresión, oposición, en otros, que se efectivizan en el marco de determinados límites⁸ y que asumen diversas formas según el contexto de implementación (COTINO HUESO 2017), tal como sucede en el ámbito judicial.

Cabe recordar que en España, el derecho a la protección de datos se desarrolla a través de la LOPDGDD, legislación que converge en su aplicación con el RGPD⁹ (CANO GALÁN 2020).

2.1.3 Administración de Justicia y protección de datos: Régimen Jurídico

El régimen aplicable al tratamiento de datos personales en materia de protección de datos en el ámbito de la Administración de Justicia, se integra por un conjunto de disposiciones nacionales y a nivel de la UE, dentro de las que se destacan:

- RGPD y LOPDGDD.
- LOPJ¹⁰
- Directiva 2016/680/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos;
- Ley Orgánica 7/2021, de 26 de mayo¹¹, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales;
- Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial (en adelante el CGPJ), por el que se aprueba el Reglamento 1/2005¹², de los aspectos accesorios de las actuaciones judiciales;

⁸Ya que no son derechos absolutos.

⁹De carácter general, obligatorio y de aplicación directa en cada Estado miembro desde el 25 de mayo de 2018.

¹⁰Modificada en virtud de Ley Orgánica 7/2015, de 21 de julio.

¹¹Que traspone la Directiva 2016/680/UE al ordenamiento jurídico nacional.

¹²Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2005-15939> [Consulta: 25 de mayo de 2022].

- Acuerdo de 20 de septiembre de 2006, del Pleno del CGPJ, de creación de ficheros de carácter personal dependientes de los órganos judiciales;
- Real Decreto 937/2003, de 18 de julio, de modernización de archivos judiciales;
- Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen en el ámbito de la cooperación policial y de la cooperación judicial en materia penal; y
- Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos (ÁLVAREZ HERNANDO 2020).

Ahora bien, dentro de este marco general, asume especial interés lo establecido por el artículo 2.1.d del RGPD, que dispone que no quedan sometidos a sus disposiciones los tratamientos de datos *“por parte de autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención”*. Y, complementariamente, por el artículo 2.4 de la LOPDGDD, según el cual *“el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el RGPD y la presente ley orgánica, sin perjuicio de las disposiciones de la LOPJ que le sean aplicables”*.

Por tanto, conforme a ambas disposiciones, se puede distinguir el tratamiento de datos de naturaleza penal, del tratamiento del resto de datos de carácter personal. Así, los primeros, quedan regidos por Directiva 2016/680/UE y Ley Orgánica 7/2021, de 26 de mayo¹³, mientras que los segundos, por RGPD, LOPDGDD y, en cuanto fuere aplicable, por LOPJ.

¹³Y supletoriamente, por RGPD, LOPDGDD y LOPJ.

Así, esta distinción es relevante, pues el presente trabajo se centra en el abordaje de los tratamientos de datos que se dan, en general, con ocasión de la tramitación de procesos judiciales, mas no, de manera específica en el ámbito penal y tampoco en relación a aquellos que desarrollan en marco de la gestión de la Oficina Judicial, es decir, a través de la actividad no jurisdiccional de la Administración de Justicia, tal como se describe más adelante.

2.1.4 Particularidades del derecho a la protección de datos a nivel judicial

Como consecuencia de la naturaleza de ciertos tratamientos, desarrollados para el cumplimiento de los fines de la Administración de Justicia, el derecho a la protección de datos presenta en este ámbito, unas notas singulares tales como, no obligatoriedad de la designación del delegado de protección de datos (art. 37.1.a RGPD); excepción a la prohibición del tratamiento de datos especialmente protegidos (art. 9.2.f RGPD); modificación de competencia de las autoridades de control (arts. 55.3 RGPD; 53.3 LOPDGDD y 45 de Directiva 2016/680/UE); prescindencia del consentimiento como base jurídica del tratamiento (art. 236 ter. 3 LOPJ); admisión de restricciones al tratamiento a fin de garantizar la independencia judicial y de los procedimientos judiciales (arts. 23.1. f RGPD y 25. 1.e R (UE) 2018/1725); exclusión de competencia del Supervisor Europeo de Protección de Datos con respecto a los tratamientos efectuados por el Tribunal de Justicia en ejercicio de su potestad jurisdiccional (art. 57.1 inc. a R (UE) 2018/1725, de 23 de octubre); limitaciones al derecho de acceso en investigaciones y procesos penales (art. 83 del R (UE) 2018/1725), entre las más importantes¹⁴(RODRÍGUEZ ROCA 2020).

En este contexto, dos de los principios institucionales que mayor impacto tienen en la configuración del régimen particular que rige al derecho a la protección de datos a nivel judicial, son la publicidad de las actuaciones (arts. 120.3 3 CE y 229 LOPJ) y la independencia

¹⁴Aspectos también mencionados en Instrucción N° 2/2019, de 20 de diciembre, de la Fiscalía General del Estado, sobre protección de datos en el ámbito del Ministerio Fiscal: el responsable y el delegado de protección de datos. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-1003 [Consulta: 2 de abril de 2022].

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital de la Justicia¹⁵ (art. 117 CE), con la particularidad de que el primero, es un derecho, y a su vez, una garantía procesal del justiciable (ABAD ALCALÁ 2021).

Esto último, genera que la protección de datos asuma en el marco del proceso unas “notas singulares ligadas al derecho a la tutela judicial efectiva [...] la publicidad de actuaciones (procesales); o incluso puede llegar a afectar a principios básicos del Estado de Derecho como la independencia judicial” (DELGADO MARTÍN 2021, p.41).

Por su parte, dentro de este régimen singular, debe hacerse mención a la aplicación de las TIC en la Justicia, ya que también entran en juego con el principio de publicidad de las actuaciones e impactan en la configuración del derecho a la protección de datos (PLATERO ALCÓN 2020).

En este sentido, a través de “*medios técnicos, electrónicos, informáticos y telemáticos*” (art.230.1 LOPJ) se recogen, ordenan, almacenan, transmiten y difunden gran cantidad de datos personales que surgen de la actividad procesal y que, por regla, solo deberían ser accesibles para la propia organización judicial, o las partes. Sin embargo, con la digitalización de la Justicia, dichos datos también pueden quedar expuestos al conocimiento de terceros ajenos al proceso, por ejemplo, en el caso asistencia telemática al acto del juicio o de consultas online de expedientes electrónicos. De ahí, que la publicidad de las actuaciones judiciales a través de internet, también integra las particularidades del derecho a la protección de datos en el ámbito judicial (MIRA ROS 2012).

2.2 TRATAMIENTO DE DATOS POR LA ADMINISTRACIÓN DE JUSTICIA A NIVEL PROCESAL

Este apartado tiene como objetivo identificar los conceptos más importantes relativos al tratamiento de datos en el ámbito judicial. Al respecto, el análisis que se centra en los tratamientos efectuados por los Juzgados y Tribunales en los procesos y en ejercicio de su potestad jurisdiccional (ficheros jurisdiccionales) sin incluir, de manera específica, los que se

¹⁵Dos temas relacionados son la restricción para los demás Poderes del Estado de acceder a los datos personales recabados por la Administración de Justicia y el ejercicio de la función de verificación del cumplimiento de la normativa por parte de la autoridad de control.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

dan en el ámbito penal y tampoco los relativos a la gestión de Oficina Judicial (ficheros no jurisdiccionales).

Por su parte, a fines del desarrollo subsiguiente, dos conceptos centrales a tener en cuenta son: “dato personal”, es decir, toda información sobre una persona física identificada o identificable (art. 4.1 RGPD); Y, “tratamiento”, que alude a cualquier operación sobre datos personales a través de procedimientos automatizados o no, como la recogida, registro, conservación, transmisión, difusión, etc. (art. 4.2 RGPD) (MARCOS AYJÓN 2013).

2.2.1 Tipos de ficheros

Conforme a la LOPJ¹⁶, el tratamiento de datos por parte de los órganos judiciales, según sus fines, puede dar lugar a ficheros jurisdiccionales y no jurisdiccionales. Así, los primeros, se integran de datos personales incorporados a los procesos¹⁷ de que conozcan los Juzgados y Tribunales en ejercicio de su actividad jurisdiccional (art. 236. 1 Bis LOPJ)¹⁸. Mientras que los segundos, incluyen datos que derivan de los procedimientos gubernativos de la Administración de Justicia que refieren a la relación funcional o laboral de las personas que integran tales Juzgados y Tribunales (art. 88 LOPJ) (DELGADO MARTÍN 2019).

2.2.2 Datos “sensibles”

El proceso judicial genera una enorme cantidad de datos personales que, en su mayoría, tienen el carácter de sensibles, incluso a veces sin poseer una relación directa con las categorías que merecen tal consideración (arts. 9 RGPD y LOPDGDD), sino por el hecho de constar en dicho proceso, puesto que “adquieren una connotación potencialmente perjudicial para el afectado, si esa información resulta accesible a terceros fuera de las actuaciones judiciales” (GÓMEZ LOECHES 1999, p. 365).

Cabe resaltar que estos datos que constituyen los ficheros jurisdiccionales, pueden surgir del aporte voluntario de los justiciables, a requerimiento del órgano judicial competente (art. 236

¹⁶Capítulo I Bis sobre la “Protección de datos de carácter personal en el ámbito de la Administración de Justicia”.

¹⁷Referidos en el art. 87.2 de LOPJ.

¹⁸También se aplica a estos ficheros la regulación establecida por R. CGPJ 1/2005 de los aspectos accesorios de las actuaciones Judiciales (Título V, arts. 86 y ss.).

ter.3 LOPJ) o del intercambio de informaciones entre las diversas Administraciones u organismos públicos vinculados al proceso (CABEZUDO RODRÍGUEZ 2010).

2.2.3 Responsables y encargados del tratamiento

En este apartado, debe tenerse en cuenta de manera particular, lo establecido en el Anexo I del Acuerdo de 20 de septiembre de 2006 del Pleno del CGPJ.

Al respecto, para el caso de los ficheros jurisdiccionales, se establece que el responsable del tratamiento será el Juzgado o Tribunal que conoce en los procesos cuyos datos personales se incorporan al fichero, bajo la dependencia directa del Secretario Judicial. Mientras que el encargado del tratamiento será la Administración Pública competente en la dotación de medios materiales (equipos, sistemas, programas, etc.) para el funcionamiento de tales órganos. Por su parte, para los ficheros no jurisdiccionales, el responsable será la Oficina Judicial correspondiente al Juzgado o Tribunal con que se relacionen los datos que integran esos ficheros, mientras que el encargado, será la Administración Pública competente en los mismos términos mencionados en el párrafo anterior (ARIZA COLMENAREJO 2021).

2.2.4 Autoridades de control

Conforme a los artículos 55.3 del RGPD, 53.3 de LOPDGDD y 236 nonies de LOPJ, la autoridad competente¹⁹ para controlar las operaciones de tratamientos efectuadas en el marco de los ficheros jurisdiccionales es el CGPJ. Por su parte, en relación a los ficheros no jurisdiccionales, es la Agencia Española de Protección de Datos (en adelante AEPD) (236 octies.2 LOPJ) con la particularidad de que, entre ambas autoridades, existe un deber de colaboración mutua (art.43.3 LOPDGDD) en aras al adecuado desempeño de sus respectivas competencias (PUYOL MORENO 2018). Cabe subrayar que el Considerando 20 del RGPD alude de manera particular a este tema, y pondera su importancia en relación a la independencia del Poder Judicial.

2.2.5 Delegado de protección de datos

La Justicia en ejercicio de su función jurisdiccional, se encuentra exenta del deber de designar un delegado de protección de datos. Al respecto, el RGPD (art. 37. 1) alude a *“los tribunales*

¹⁹Se entiende por tal, a la autoridad pública independiente que supervisa la aplicación de la legislación vigente en la materia mediante el ejercicio de poderes de investigación y correctivos (arts. 4.16 y 51 a 59 RGPD).

que actúen en ejercicio de su función judicial”, de ahí es que se entiende aplicable en relación a los datos tratados en ficheros jurisdiccionales (MONTORO SÁNCHEZ 2019). Por tanto, en sentido contrario, cuando no desarrollen tales funciones, se puede entender la necesidad del nombramiento de un delegado de protección de datos (RODRÍGUEZ AYUSO 2019).

Cabe resaltar que en el año 2018, el CGPJ designó por primera vez un delegado de protección de datos para el desempeño de funciones específicas en relación a sus propios datos o ficheros²⁰ y, en abril del corriente año 2022, lo sustituyó por un nuevo delegado de protección²¹.

2.2.6 Bases jurídicas del tratamiento

Otro rasgo distintivo del derecho a la protección de datos en el ámbito judicial, es la base jurídica del tratamiento.

Al respecto, la LOPJ estipula que no es necesario el consentimiento (art. 6.1.a RGPD) del interesado para que proceda el tratamiento lícito de sus datos en el proceso, (art. 236 ter.1). De esta manera, se impone como base legitimadora “el ejercicio de poderes públicos conferidos al responsable” (art. 6.1.e del RGPD), en el sentido de que tal tratamiento es necesario para el ejercicio de la función jurisdiccional conferida a los Juzgados o Tribunales (responsable del tratamiento)²² (DELGADO MARTÍN 2019). Asimismo, esto no descarta que en determinados casos la base legitimadora pueda ser el consentimiento e incluso el interés público (ARIZA COLMAREJO 2021, pp. 108-109).

2.2.7 Ejercicio de derechos

En el ámbito judicial, los titulares de datos contenidos en ficheros jurisdiccionales gozan de todos los derechos reconocidos en el RGPD y LOPDGGD²³, es decir, acceso, rectificación, supresión, portabilidad, limitación y oposición al tratamiento y a no ser objeto de decisiones

²⁰Conforme Acuerdo del Pleno de 16 de mayo de 2018 Disponible en: <file:///C:/Users/Admin/Downloads/20220420%20BoletinesAcuerdosPleno.pdf> [Consulta: 11 de junio de 2022].

²¹Conforme Acuerdo del Pleno de 20 de abril de 2022. Disponible en: <https://www.poderjudicial.es/cgpj/es/Servicios/Atencion-Ciudadana/Delegado-de-Proteccion-de-Datos/> [Consulta: 11 de junio de 2022].

²²El artículo 8.2 LOPDGGG exige que la competencia atribuida al responsable para el ejercicio de poderes públicos emane de una norma con rango de ley que, en este caso, surge de manera general de LOPJ.

²³Regulados en los artículos 15 a 22 RGPD y 12 a 18 LOPDGGD.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital basadas únicamente en el tratamiento automatizado (DELGADO MARTÍN 2019). Sin embargo, respecto a su ejercicio, la LOPJ establece que deberá tramitarse de acuerdo *“a las normas que resulten de aplicación al proceso en que los datos fueron recabados”* (art. 236 septies.1 LOPJ).

De esta manera, se deja de lado la legislación general sobre protección de datos²⁴ y se impone la aplicación de normas procesales que deberán ser adaptadas al caso particular, situación que respecto a determinados derechos puede generar inconvenientes, por ejemplo, piénsese en el supuesto de que a través del derecho de acceso se pretenda tomar conocimiento de información declarada reservada o secreta donde, además, podría entrar en colisión con el principio de publicidad procesal, de ahí que en casos como estos, la aplicación de cualquier normativa sobre protección de datos podría verse limitada (ARIZA COLMAREJO, 2021).

2.2.8 El problema de la legislación aplicable

El tema de la legislación aplicable, es uno de los principales núcleos de tensión respecto a la implementación de la protección de datos a nivel judicial. Esto se da en relación al ejercicio de derechos y, en general, respecto al régimen aplicable a los ficheros jurisdiccionales.

Así, respecto al ejercicio de derechos, se ha dicho que la LOPJ remite al Derecho procesal, no obstante, este no contiene disposiciones específicas en la materia que, además, son anteriores en el tiempo al RGPD y LOPDGDD y no han sido diseñadas a estos fines (RODRÍGUEZ ROCA 2020).

Así las cosas, cada derecho debe recibir un tratamiento específico en cada caso, debiendo el juzgador adaptarlos a criterios procesales, tarea de por sí compleja si se tiene en cuenta que dentro del proceso se daría una superposición de normas de protección de datos, principios y normas procesales, que persiguen la satisfacción de diversos bienes jurídicos.

En este último sentido, es esencial que la norma procesal escogida por el juzgador, por ejemplo, para permitir el acceso a datos, respete el derecho de protección de datos en todo su alcance, pues de lo contrario, se estaría vulnerando un derecho fundamental.

²⁴A diferencia de los ficheros no jurisdiccionales que sí se rigen por la normativa general (art. 236 septies.3 LOPJ).

En segundo lugar, en el apartado del régimen jurídico (2.1.3) se ha mencionado que los tratamientos de datos en el marco del proceso se rigen, en general, por el RGPD (art.2.1 d) LOPDGDD (art.2.4) y en cuanto fuere aplicable, por LOPJ.

En este sentido, sucede que el RGPD, en palabras de RODRÍGUEZ ROCA “no contiene normas especiales sobre cómo implementar la protección de datos en la Administración de Justicia”²⁵, lo cual es relevante, pues como se ha dicho, en el proceso pueden entrar en juego diversos bienes jurídicos y no en todos los casos las diferencias pueden salvarse mediante un ejercicio de ponderación por parte del juzgador (RODRÍGUEZ ROCA 2020, p. 148).

Por su parte, lo mismo puede predicarse respecto a la LOPDGDD, la cual se limita a construir un sistema general de protección de datos y, en relación a la Justicia, solo incorpora normas puntuales sin tener en cuenta que no siempre las normas generales podrán traspolarse al ámbito judicial y a nivel procesal, pues, de hecho, existen extremos incompatibles con las características institucionales, organizativas y funcionales que rigen a la Justicia, tal como en ocasiones sucede con el principio de independencia judicial, la publicidad procesal o la tutela judicial efectiva (RODRÍGUEZ ROCA 2020).

2.3 PUBLICIDAD DE LAS ACTUACIONES Y PROTECCIÓN DE DATOS

En este apartado se analizan algunas interrelaciones reguladas en LOPJ entre el principio de publicidad y el derecho a la protección de datos, en particular, sobre el acceso al expediente y a sentencias por quienes no son parte en el proceso, dejando afuera, salvo alguna referencia puntual, el acceso a las actuaciones orales en los procedimientos, entendida como la presencia de terceros en la práctica de diligencias o del acto del juicio en carácter de público.

A estos fines, se entiende que el expediente judicial, se integra por todos los documentos aportados por las partes o terceros²⁶, y por las actuaciones procesales y demás resoluciones dictadas durante el proceso. Y, por sentencias, se alude a aquellas resoluciones por las que se finaliza un proceso y que tienen vocación de incorporarse a bases de datos públicas.

²⁵Cabe recordar que el Considerando 20 RGPD dice que sus normas son aplicables al ámbito judicial, no obstante, solo se limita establecer referencias sobre las autoridades de control.

²⁶Por escrito, medios electrónicos o telemáticos, conforme al artículo 1.4 de RDL 937/2003, de 18 de julio, de modernización de los archivos judiciales.

2.3.1 Regulación del principio de publicidad a nivel procesal

El proceso genera una enorme cantidad de datos personales que se incorporan a los ficheros y que surgen, del aporte voluntario de los justiciables, a requerimiento del órgano judicial competente (art. 236 ter.3 LOPJ) y del intercambio de informaciones entre las diversas Administraciones u organismos públicos participantes (CABEZUDO RODRÍGUEZ 2010).

Así, esta circulación de información debe respetar y resguardar el derecho a la protección de datos y al mismo tiempo encontrar un equilibrio con la publicidad de las actuaciones judiciales que, además de ser un principio guía de la Administración de Justicia (arts. 120 CE y 229 LOPJ), es un derecho y garantía procesal del justiciable (art. 24 CE) (ABAD ALCALÁ 2021).

En este último sentido, a nivel procesal, el principio de publicidad se desarrolla en la Ley de Enjuiciamiento Civil 1/2000 de 7 de enero (en adelante LECiv), principalmente, bajo las vertientes de publicidad de las actuaciones orales y celebración de juicios en audiencia pública (art. 138); acceso a documentos judiciales de procesos en curso; y acceso a sentencias de procesos concluidos, vertientes también contempladas en LOPJ.

Así tal distinción es relevante, pues originariamente la publicidad se entendía solo como presencia de la ciudadanía en el escenario del juicio y a fines estrictamente disuasorios de la arbitrariedad judicial o de la injerencia gubernamental en el proceso (MIRA ROS 2012).

Al respecto, cabe resaltar que la LOPJ (art.232) establece el carácter público de juicios, vistas y comparecencias y, excepcionalmente, permite limitar su publicidad e imponer el secreto de actuaciones, por razones de orden público o de protección de derechos y libertades de las personas, conforme a decisión motivada del órgano judicial competente (ABAD ALCALÁ 2021).

Ahora bien, más allá de esta vertiente general, la LOPJ presta especial atención al acceso al expediente judicial y a las sentencias, pues, en ellos, consta información confidencial de las partes y de terceros vinculados al litigio (testigos, peritos, etc.) que no adquiere la calidad de pública por el hecho de ventilarse en un proceso público (CABEZUDO RODRÍGUEZ 2010). Por tanto, su conocimiento por terceros ajenos al proceso, puede ser potencialmente perjudicial para sus derechos y libertades (GÓMEZ LOECHES 1999).

2.3.2 Acceso al expediente judicial y las sentencias en la LOPJ

En relación al expediente, la LOPJ establece que la Administración de Justicia, debe entregar a las partes o a cualquier interesado que no es parte pero *“que acredite un interés legítimo y directo”* (art. 234.2), cuanta información requieran, mediante exhibición, copias, testimonios o certificados²⁷, con el único límite de que las actuaciones no hayan sido declaradas secretas o reservadas (art. 234.1.2) en virtud de decisión motivada del órgano judicial competente²⁸.

Cabe resaltar que por “interesado”, siguiendo a HERRÁEZ MARTÍN, debe entenderse a “la persona afectada por los propios datos” que constan en el proceso y, por tanto, que integran los ficheros jurisdiccionales, y se diferencia del tercero, que es “la persona física o jurídica ajena a esos datos”. De ahí que debe exigirse una conexión concreta y específica con el objeto del proceso, a fin de habilitar su acceso al expediente (HERRÁEZ MARTÍN 2012, p. 42).

De esta manera, la LOPJ consagra como regla el acceso libre de las partes al expediente, y articula la conexión entre publicidad y protección de datos en base a tres filtros: el interés legítimo y directo (a acreditar por quien no es parte); el carácter reservado o secreto (que limita incluso el acceso de las partes); y la decisión motivada (MIRA ROS 2012).

Complementariamente, dicha legislación dispone que los datos personales que contengan las actuaciones procesales, documentos y otras resoluciones deben ser *“adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”* (art. 236 quinquies.1 LOPJ) y, en ese marco, faculta a los Juzgados y Tribunales a suprimir aquellos datos que no fueran indispensables para satisfacer el derecho a la tutela judicial efectiva (art. 236 quinquies.2 LOPJ).

Véase aquí la posible limitación a la publicidad y a la tutela judicial en pos de la protección de datos, de ahí la importancia del juicio de ponderación por parte del juzgador en el caso concreto, a fin de encontrar el equilibrio entre los intereses en pugna.

Por su parte, respecto al acceso a sentencias como medio de control de la actividad ad intra que desarrolla la Justicia (CALDERÓN CUADRADO 2000), la LOPJ establece que solo podrá

²⁷También receptado en art. 7 RDL 937/2003, de 18 de julio, sobre modernización de los archivos judiciales.

²⁸Conforme art. 140.3 LECiv y arts. 2,3 y 4 R. CGPJ 1/2005 de los aspectos accesorios de las actuaciones judiciales.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

llevarse a cabo por quienes no son parte en el proceso, previa disociación o anonimización de los datos personales contenidos en ellas (art. 235). Exigencia de carácter general, que se complementa a las limitaciones previstas para el acceso a resoluciones judiciales dictadas durante el proceso, según se menciona en párrafos anteriores (CANO GALÁN 2020).

Cabe destacar que, de manera complementaria, el artículo 266 de LOPJ dispone que el acceso al texto de las sentencias podrá ser restringido, toda vez que su publicidad pueda afectar la intimidad o derechos de personas que requieran de una especial tutela o garantía de anonimato, así como también, para evitar usos contrarios a las leyes.

Sobre el tema de la anonimización se retoma en el apartado dedicado a “Acceso a sentencias contenidas en bases de datos públicas y protección de datos” (2.4.4).

2.4 TRANSFORMACIÓN DIGITAL DE LA JUSTICIA: ACTUALIDAD

En esta segunda etapa del marco teórico, se abordan aspectos vinculados al impacto de las TIC en la Administración de Justicia, de manera particular, las principales formas que puede asumir la publicidad a través de internet como la asistencia telemática a las actuaciones, el acceso al expediente judicial electrónico y la difusión de sentencias a través de bases de datos de carácter público. Asimismo, se identifican a grandes rasgos, algunas oportunidades para la mejora del sistema judicial a través la aplicación de tecnologías derivadas de la denominada industria 4.0 y los desafíos que, en general, pueden presentarse para la protección de datos.

2.4.1 Actualidad de la transformación digital

La transformación digital de la Justicia alude a la integración de soluciones de tecnología digital al sistema judicial a fin mejorar la calidad y eficacia del servicio, modificando el funcionamiento interno de la Administración y la forma de relación con el ciudadano, y gestionando los riesgos que puedan surgir para las garantías procesales y derechos de las personas (DELGADO MARTÍN 2021, p.28).

Este concepto, aparece ligado a lo que se conoce como e-Justicia o Justicia electrónica, que es la Administración de Justicia cuya gestión se implementa con mediación de la tecnología digital y el uso de internet a fin de desmaterializar el proceso y mejorar el servicio de justicia (BUSTAMANTE RÚA y MARÍN TAPIERO 2021).

Al respecto, el principal hito de la transformación digital de la Justicia española se encuentra en la Ley 18/2011 de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, normativa que intensifica un proceso que actualmente es constante, transversal y multisectorial, en el sentido que está ligado al ritmo del avance tecnológico y depende e involucra a todos los actores públicos, el sector privado y a la ciudadanía (BEIRO MAGAN 2019). De ahí que para su desarrollo no basta con la aplicación de tecnología, sino que la misma debe ser acompañada de otras cuestiones como la adaptación integral de las categorías dogmáticas del Derecho procesal y su unificación normativa, la existencia los medios materiales e infraestructuras tecnológicas adecuadas al efecto y la presencia de recursos humanos suficientemente capacitados para estar a la altura de los cambios y oportunidades permanentes que se presentan (BUSTAMANTE RÚA y MARÍN TAPIERO 2021) (MIRA ROS 2012).

Ahora bien, junto a la mencionada Ley 18/2011, de 5 de julio, también aparecen como normativas de importancia, Real Decreto 84/2007, de 26 de enero, de creación del sistema de comunicaciones LexNET, Real Decreto 1065/2015, de 27 de noviembre, por el que se mejora dicho sistema, Ley 42/2015 de 5 de octubre, que reforma la LECiv y LOPJ, entre otras (PLATERO ALCÓN 2020).

Así, dentro de este contexto normativo sumado a otras disposiciones específicas²⁹ han surgido múltiples cambios en la actividad judicial imponiéndose una mayor tendencia a la oralidad, dentro de los que se destacan, asistencia telemática a actuaciones procesales, expediente electrónico, creación de bases de datos judiciales online de acceso público, prueba digital, creación de archivos de naturaleza audiovisual, textualización de declaraciones grabadas por medios audiovisuales, sistemas de videoconferencias, salas virtuales³⁰, almacenamiento de documentos en nube, firma electrónica, identificación a través de datos biométricos, realización de trámites electrónicos³¹, implantación de sistemas de gestión procesal de

²⁹Cuyo desarrollo excede los límites de este trabajo.

³⁰Carecen de bidireccionalidad de sonido y es imprescindible la presencia de un moderador que la gestione (efectuar invitaciones, anulación de sonido, conferir el uso de palabra, etc.).

³¹Por ejemplo, obtener información sobre el estado de trámites, descargar formularios, gestionar copias, certificados, entre otros (MIRA ROS 2012).

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital tramitación guiada³² y, en general, todas las aplicaciones desarrolladas en el marco de la Nueva Oficina Judicial Electrónica³³(MEDINA MORALES 2019) (BEIRO MAGAN, 2019).

Estos avances representan ventajas innegables para la Justicia y el proceso en su conjunto, no obstante, también generan riesgos potenciales para determinados derechos, por ejemplo, para la protección de los datos obrantes en ficheros jurisdiccionales ahora visibles a través de internet y, por tanto, expuestos a los peligros del ciberespacio y a las vulnerabilidades de la infraestructura tecnológica de la Administración de Justicia (MIRA ROS 2012).

Cabe resaltar que en el ámbito de gobernanza de la Administración Electrónica en España, desempeña funciones el Comité Técnico Estatal de la Administración Judicial Electrónica³⁴, no obstante, su tratamiento excede los objetivos del presente trabajo.

2.4.2 Asistencia telemática a las actuaciones judiciales

La transformación digital de la Justicia ha producido un desplazamiento del debate sobre la publicidad procesal, que ha dejado de estar en quienes pueden acceder físicamente al litigio o expediente y se ha centrado en la accesibilidad telemática y a su alcance a través de la red.

Desde esta perspectiva, por asistencia telemática se entiende “la intervención de una persona en un acto judicial, sin encontrarse físicamente en la sede del juzgado o tribunal, a través de videoconferencia u otro sistema similar que permita la comunicación bidireccional y simultánea de la imagen y el sonido y la interacción visual, auditiva y verbal entre dos personas o grupos de personas geográficamente distantes” (DELGADO MARTÍN 2021, p.36).

³²Según el Protocolo Marco de actuación de la Oficina Judicial, el sistema de gestión procesal es “un sistema de tramitación guiada, configurado sobre la base de unos esquemas de tramitación procesal que identifican claramente las fases o trámites del procedimiento que tendrán asignadas las distintas unidades de la oficina judicial y la distribución de competencias entre las mismas. Dicha identificación está totalmente configurada [...]” (BEIRO MAGAN 2019, p.2).

³³Objetivos de la oficina judicial. Disponible en: <https://www.mjusticia.gob.es/ca/justicia-espana/proyectos-transformacion/oficina-judicial/objetivos-oficina-judicial> [Consulta: 29 de abril de 2022].

³⁴Órgano de cooperación encargado de coordinar los esfuerzos de los diversos operadores de justicia a fin de lograr una adecuada incorporación de las TIC en el sector, particularmente, favorecer la interoperabilidad de los sistemas y aplicaciones que se utilicen. Sus funciones se encuentran receptadas en Real Decreto 396/13, de 7 de junio. Su sitio web se encuentra disponible en: <https://www.cteaje.gob.es/> [Consulta: 28 de mayo de 2022].

Normativamente, la implementación telemática de las actuaciones procesales se encuentra receptada en el artículo 229 de la LOPJ³⁵, modalidad que se estableció como preferente durante la pandemia en virtud de Real Decreto Ley 16/2020, de 28 de abril, luego derogado por la vigente Ley 3/2020, de 18 de septiembre, que regula las medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia. Al respecto, la particularidad de estos dos últimos preceptos es que, según se menciona en la Guía para la celebración de actuaciones judiciales telemáticas del CGPD³⁶ (en adelante GAJT), “ni uno ni otro precisan los criterios a seguir [...] ni la forma ni los requerimientos técnicos para esa aplicación” (apartado 3).

En tal sentido, dicha guía contempla la utilización de medios telemáticos tanto, para actuaciones internas, es decir, que hacen referencia a la actividad exclusiva de los Tribunales y su personal, como externas, en las que, además, participan ciudadanos y/o operadores jurídicos (abogados, peritos, etc.). Y, respecto a estas últimas, regula criterios de procedencia, según sea con participación exclusiva de ciudadanos o de operadores jurídicos. Asimismo, cabe destacar que esta modalidad permite que una o varias personas asistan telemáticamente a una actuación judicial llevada a cabo en sede judicial, como así también que todos los intervinientes asistan telemáticamente a dicha actuación (apartados 46 a 50 GAJT).

Lo más importante, a efectos del presente análisis es que, en relación a la celebración de actos telemáticos con trascendencia externa, la GAJT establece criterios para garantizar la confidencialidad, defensa y publicidad.

Así, respecto a la confidencialidad, se dispone que a través de los medios técnicos que se utilicen, se deberá impedir la realización grabaciones diferentes a las que correspondan para su documentación oficial y, en lo posible, deberán permitir el rastreo o trazabilidad de grabaciones diferentes a las autorizadas a fin de dejar constancia de la autenticidad e integridad de los datos (apartado 36 GAJT). Asimismo, deberán establecerse medidas para

³⁵Alude específicamente a declaraciones, testimonios, careos, interrogatorios, exploraciones, informes, ratificación de los periciales y vistas.

³⁶Disponible en: <https://www.poderjudicial.es/cgpj/es/Servicios/Informacion-COVID-19/Guias-y-Protocolos/Guia-para-la-celebracion-de-actuaciones-judiciales-telematicas> [Consulta: 5 de junio de 2022].

que las actuaciones se desarrollen en un entorno reservado, estando facultado el juez para verificar todos estos requisitos antes del inicio del acto y a suspenderlo, en caso de incumplimiento. De realizarse el acto, deberá mantener una actitud vigilante durante todo su desarrollo (apartado 37 GAJT).

Respecto a la defensa, se establece que en el supuesto de que el abogado y el acusado no se encuentren en el mismo lugar durante el juicio, debe garantizarse que mantengan contacto telemático constante y reservado³⁷. Igualmente, cuando por razones sanitarias se aconseje la toma de declaración del acusado en sede policial sin presencia del abogado, deberán adoptarse medidas que permitan la entrevista previa y reservada entre ambos y que sean pertinente para asegurar la efectividad de tal reserva (apartado 38 GAJT).

En relación a la publicidad, se dispone que cuando las actuaciones procesales deban celebrarse en audiencia pública, la forma más idónea de asegurar este principio vía telemática, es a través de la asistencia del público a la sala de vistas del Juzgado o Tribunal en que celebre el acto u otra dependencia judicial donde pueda ser observado en circuito cerrado, procurando la toma de medidas que impidan grabaciones clandestinas de lo que se visualice en los monitores. De esta manera se pretende facilitar técnicamente la satisfacción del principio de publicidad evitando el uso indebido de datos personales (ej. imágenes) de testigos u otros intervinientes (apartado 39 y 40 GAJT).

Por su parte, cuando tal asistencia del público a la sede del órgano judicial no sea posible, los datos sobre la audiencia³⁸ deberán hacerse constar todos en el “tablón de anuncios virtual” de la sede electrónica correspondiente y facilitarse para su transmisión telemática el uso de un programa que permita el acceso a terceros mediante clave o invitación, que se entregará una vez que se acrediten, física o virtualmente en sede judicial, oportunidad en la que se le informará de la prohibición de obtener copias de la sesión o de realizar grabaciones de la pantalla en que se transmita la sesión. Asimismo, el programa informático utilizado, debe

³⁷Respecto al juicio penal en particular, y hasta tanto el acusado preste declaración.

³⁸Fecha, hora, tipo de audiencia y número de procedimiento (art. 232.2 LOPJ).

contener medidas tendientes a impedir la grabación por los terceros invitados o que puedan compartir videos, audios o cualquier otro tipo de archivo (apartado 41 GAJT).

Cabe destacar que en relación a los requisitos técnicos de las actuaciones, la GAJT remite a su Anexo, el cual contempla aspectos relacionados a tecnologías aplicables (sistemas de gestión procesal, de grabación de vistas, de videoconferencias de calidad, salas virtuales, sedes judiciales electrónicas, etc.), seguridad³⁹, organización y verificación de cumplimiento⁴⁰.

En resumen, en relación a esta modalidad de actuaciones procesales, puede decirse que entre sus ventajas se destacan, la agilización de procedimientos y optimización de sus resultados, la reducción de costes y recursos para la Administración de justicia y las partes (ej. ligados al desplazamiento de las personas), la protección de personas en situación de especial vulnerabilidad (ej. evitar la asistencia presencial de menores de edad) como así también, ante potenciales riesgos para la salud (ej. rebrotes del COVID-19), el fortalecimiento de la garantía de publicidad de las actuaciones procesales, entre otras. Y, entre sus limitaciones se encuentran, el incremento de riesgos de hackeo y de afectación de los datos personales, tanto por el acceso no autorizado de terceros como por su potencial difusión posterior y la existencia de ciertas limitaciones en las infraestructuras tecnológicas de la Administración de Justicia en la actualidad, como falta de equipamientos y recursos técnicos, mala conexión a internet, escaso ancho de banda, entre otras. (GARCÍA SANZ y GONZÁLEZ GUIMARAES-DA SILVA 2020).

2.4.3 Acceso al expediente judicial electrónico (LexNET)

La aplicación de las TIC a la Administración de Justicia permite abrir nuevos canales de atención, comunicación e información accesibles para ciudadanos, como para operadores jurídicos. En este último sentido, uno de los más importantes a través de los que opera el expediente judicial electrónico, es el denominado sistema LexNET.

Al respecto, dicho sistema, es definido por Real Decreto 1065/2015 de 27 de noviembre, como “un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de

³⁹Autenticación de las partes y operadores jurídicos, control de acceso de los usuarios, encriptación de las comunicaciones, rastreo de fallo técnico intencionado, entre otras.

⁴⁰Aspectos cuyo análisis excede los límites del presente trabajo.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos. Asimismo, [...] garantiza el contenido íntegro de las comunicaciones y la identificación del remitente y destinatario de las mismas mediante técnicas de autenticación adecuadas⁴¹ [...]” (art.13).

En estos términos, LexNET constituye una red interna de utilización exclusiva para los operadores jurídicos⁴² que se relacionan con la Administración de Justicia. Su objetivo es lograr una política de “papel cero” en el sistema que se traduzca en la mejora de la eficiencia y calidad del servicio de justicia. Al efecto, entre sus finalidades, se destacan la presentación y transporte de escritos procesales, la gestión del traslado de copias, la realización de actos de comunicación procesal, la expedición de resguardos electrónicos, entre otros⁴³, todo ello, a través de un método de autenticación de modo que es posible controlar quien accede y asegurar que tal acceso, solo pueda ser efectuado por operadores jurídicos habilitados (BEIRO MAGAN 2019).

En este último sentido, como es de entender “si se trata de un medio de transmisión de datos seguro, debe respetar la normativa de protección de datos personales existente y no permitir el acceso a datos personales de otros usuarios [...] [Por tanto] debe reunir un requisito fundamental [...] como es la articulación de un sistema de custodia y cuidado de los datos personales de sus usuarios” (PLATERO ALCÓN 2020, p.35).

Sin embargo, en el año 2017, este requerimiento de seguridad fue incumplido, pues una falla de seguridad permitió que operadores habilitados accedieran al sistema con un usuario distinto del propio y consultaran informaciones y documentos ajenos (notificaciones, traslados, demandas, partes hospitalarios, entre otros) lo que derivó en la interrupción del servicio, el cierre del sistema por varios días y en la incoación de un procedimiento sancionador por parte de la AEPD en contra del Ministerio de Justicia. Al respecto, la

⁴¹En la actualidad, a través de certificado digital y firma electrónica (art 6). No obstante, en 2019 el Ministerio de Justicia anunció la incorporación al expediente electrónico de una aplicación para participantes del proceso sin firma electrónica obligatoria que incluiría datos biométricos (BEIRO MAGAN 2019, p.8).

⁴²Enunciados en el Anexo II RDL 1065/2015 de 27 de noviembre.

⁴³Conforme al artículo 17 RDL 1065/2015 de 27 de noviembre.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

investigación determinó que 284 usuarios accedieron a 692 buzones ajenos y visualizando 1438 mensajes de forma no autorizada⁴⁴.

Evidentemente, esta situación derivó en cambios y esfuerzos continuos por parte del Ejecutivo Nacional en coordinación con el CGPJ, a fin de mejorar el sistema. No obstante, los inconvenientes continuaron en los años subsiguientes, pues tal como señala MEDINA MORALES, basta navegar por la prensa para verificar que en repetidas ocasiones se han producido filtraciones de documentos, accesos no autorizados o caídas del sistema que han hecho saltar las alarmas de los operadores de la justicia. Cabe resaltar, que hablar de accesos no autorizados supone un claro peligro para la privacidad y los datos personales de quienes se vinculan con la Administración de Justicia y, entre otras infracciones, supone la violación del deber de secreto (MEDINA MORALES 2019, p. 90). Cabe resaltar, que la última actualización de LexNET se ha producido en el corriente año 2022 y supone, según el Ministerio de Justicia, una mejora sustancial en las prestaciones tecnológicas del sistema⁴⁵.

2.4.4 Acceso a sentencias contenidas en bases de datos públicas

La vigencia del principio de publicidad procesal en el marco de la transformación digital, también ha dado lugar a la creación de grandes bases de datos de búsqueda online de jurisprudencia de acceso libre, tal como sucede con el Centro de Documentación Judicial⁴⁶ del CGPJ (en adelante CENDOJ).

Al respecto, el CENDOJ es administrado por el CGPJ (art. 619 LOPJ), de ahí que una de sus principales ventajas es que, Tribunal Supremo, Audiencia Nacional, Tribunales Superiores de Justicia, Audiencias Provinciales y el resto de Tribunales cuando sean requeridos, se encuentran obligados a remitirle sus sentencias, lo que ha permitido el registro de antecedentes jurisprudenciales desde el año 2003 a la fecha (MARCOS AYJON 2020).

⁴⁴La AEPD opina que el Ministerio de Justicia infringió la LOPD con el caso Lexnet. Disponible en: <https://protecciondatos.conversia.es/aedp-opiniones-lexnet-ministerio-justicia/> [Consulta: 3 de mayo de 2022].

⁴⁵Justicia mejora las prestaciones tecnológicas del sistema de comunicaciones electrónicas Lexnet. Disponible en: <https://www.mjusticia.gob.es/ca/ElMinisterio/GabineteComunicacion/Paginas/220506-NP-Ampliacion-funcionalidades-de-LexNET.aspx> [Consulta: 6 de mayo de 2022].

⁴⁶Acceso disponible en: <https://www.poderjudicial.es/search/indexAN.jsp> [Consulta: 22 de abril de 2022].

Al respecto, previo a la publicación, el CENDOJ “se encarga de la anonimización de las sentencias” (art 235 LOPJ) (ÁLVAREZ HERNANDO 2020, p. 1359), tarea técnica que consiste en enmascarar o suprimir aquella información que permita identificar a los particulares intervinientes en el proceso a fin de proteger su intimidad y datos personales obrantes. Según la RAE “anonimizar” consiste en “expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad” (CANO GALÁN 2020, p.42).

No obstante, este procedimiento no constituye una garantía absoluta sino una medida de privacidad y de protección de datos ya que “en el momento en que del conjunto de otros datos periféricos pueda identificarse a la persona, la anonimización pierde su eficacia”. Asimismo, “la difusión a través de medios de comunicación de procesos de relevancia mediática, hace que del relato de hechos de la sentencia se logre identificar a la persona y poner en riesgo su intimidad personal y familiar” (ARIZA COLMENAREJO 2021, p. 110).

Por tanto, se entiende que el gran reto es lograr un equilibrio pleno entre todos los derechos en juego, de ahí el importante rol del CGPJ para construir y proponer parámetros uniformes y seguros para la protección de los datos obrantes en sentencias, y demás resoluciones judiciales que se publiquen (ARIZA COLMENAREJO 2021).

2.5 TECNOLOGÍAS DISRUPTIVAS: OPORTUNIDADES Y DESAFÍOS

La enorme transformación digital y tecnología de este Siglo ha dado lugar a lo que algunos autores denominan cuarta revolución industrial (SCHWAB 2016) y otros, industria 4.0 (AYNETO GUBERT 2019) como concepto que pretende englobar el mismo fenómeno.

Así, tomando como referencia este último, puede decirse que la industria 4.0 representa un modo de producción caracterizado por la digitalización y automatización de procesos, el uso de tecnologías de la información y la electrónica, la personalización de la producción y la interacción y el intercambio de información entre máquinas y personas, entre otros aspectos (YNZUNZA CORTÉS, IZAR LANDETA, y BOCARANDO CHACÓN 2017). En este marco, las tecnologías empleadas por este nuevo modo de producción son muy variadas y entre ellas se encuentran las denominadas “tecnologías facilitadoras” como “Internet de las Cosas, análisis de datos y big data, inteligencia artificial, computación cognitiva, sistemas ciberfísicos,

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital
robotización, realidad virtual, drones, “machine learning”, blockchain o ciberseguridad, entre otras” (GARCÍA JIMÉNEZ 2021, p.311).

Precisamente, se denominan “facilitadoras” porque al trabajar de forma conjunta, están produciendo cambios trascendentales en todos los ámbitos de la vida humana, desde la industria, los negocios, el mercado, las relaciones de consumo, el ámbito laboral, profesional e incluso hasta el gubernamental (YNZUNZA CORTÉS *et al.* 2017).

En este último sentido, el uso de tecnologías “facilitadoras” en la Administración de Justicia ha dado lugar al planteamiento de temas tales como, gestión pública y masiva de datos judiciales a través de sistemas big data a fines estadísticos, asistencia de software basado en inteligencia artificial para atención al ciudadano, incorporación de tecnología de encriptación matemática o blockchain a fines probatorios, entre otros (BEIRO MAGAN 2019).

Ahora bien, todas estas soluciones tecnológicas a la par de presentarse como oportunidades emergentes para la mejora del sistema, también plantean interrogantes en relación a la protección de datos (HERNÁNDEZ ÁLVAREZ 2020). En este último sentido, interesa indagar sobre posibles aplicaciones de big data, IA y tecnologías blockchain.

2.5.1 Big data (macro datos)

Se entiende por big data al sistema o conjunto de tecnologías que permiten tratar a gran velocidad, cantidades ingentes de datos que pueden ser organizados de manera tal, que proporcionen valor. Es decir, permite convertir grandes cantidades de datos en bruto, en información aplicable que se traduce en beneficios (BALLESTAR, RIBEIRO y SAINZ 2018).

En este sentido, no se trata de una tecnología en sí misma, sino un método de trabajo (GIL GONZÁLEZ 2015) que, a través del tratamiento de datos de diversas formas⁴⁷ y fuentes⁴⁸, persigue descubrir un conocimiento que estaba oculto (COTINO HUESO 2017). De ahí que lo relevante no es la cantidad, fuente o naturaleza de los datos, sino el valor potencial que estos

⁴⁷Estructurados (cuantitativos), no estructurados (cualitativos) o parcialmente estructurados (COTINO HUESO 2017).

⁴⁸Imágenes, vídeos, datos web (redes sociales y de navegación en internet), transacciones electrónicas, dispositivos móviles, comunicaciones 3G, 4G, 5G y GPS, sensores de internet de las cosas, entre otras (PUYOL MORENO 2014).

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

adquieren al ser tratados por un conjunto de tecnologías como el big data, capaces de convertirlos en un corto periodo de tiempo, en información aplicable de valor (PUYOL MORENO 2014).

Desde esta perspectiva, el big data brinda a las instituciones y empresas la oportunidad de que grandes cantidades de datos en principio, sin posible utilidad, puedan ser recogidos y utilizados para mejorar la toma de decisiones, resolución de problemas y optimización de respuestas, en definitiva, de ser más competitivas en términos de productividad, costes y calidad de bienes y servicios (ÁLVAREZ VALLE 2013).

Cabe resaltar que, al hablar de datos en principio sin posible utilidad, se alude a que estos no pueden ser almacenados, procesados o analizados mediante tecnologías o herramientas convencionales de gestión de datos, o no pueden serlo dentro del tiempo necesario para que sean útiles (COLLADO CALVO 2019).

En relación a esto último, el big data se caracteriza por ser aplicable a datos difíciles de manejar y utilizar, sea por su volumen (tamaño), variedad (de fuentes y naturaleza) o velocidad de crecimiento (COTINO HUESO 2017).

Por su parte, debe tenerse en cuenta que el big data como sistema no se agota en el almacenamiento y procesamiento de datos, sino que sobre ellos se aplican algoritmos que conducen a conclusiones. En este sentido, se integra por tecnologías que permiten capturar datos, integrarlos en conjuntos adecuados o estructurados, almacenarlos, analizarlos y presentarlos en su forma de aplicación (AEPD y ISMS FORUM SPAIN 2018).

Así, el big data puede utilizarse a fines descriptivos, es decir, a efectos de explicar lo que ha sucedido o está sucediendo (analítica 1.0)⁴⁹; predictivos, a fin de expresar con la mayor certidumbre posible (en base a datos) que puede llegar a suceder (analítica 2.0)⁵⁰; y prescriptivos, modalidad que en base a las predicciones sugiere acciones a seguir para obtener beneficios (analítica 3.0) (QUINTERO *et al.* 2018).

⁴⁹Fortalece las prácticas de las denominadas bodegas de datos o “data warehouse” (QUINTERO, MOLLAR VILLANUEVA y GÓMEZ MONTAYA 2018).

⁵⁰Da lugar a la minería de datos o “data mining” y se complementa con modelos de predicción basados en estadísticas, matemáticas y aprendizaje artificial automático o “machine Learning” (QUINTERO *et al.* 2018).

Ahora bien, si se analiza lo que está sucediendo con la aplicación de estas tecnologías en el ámbito de la Justicia, puede decirse que existe un número creciente de experiencias y estudios sobre posibles funcionalidades para la mejora del sistema.

En este sentido, se puede mencionar la conocida estadística judicial, donde la aplicación de sistemas big data (e IA) podría contribuir a una interconexión entre bases de datos de diversos organismos públicos lo que generaría una transformación radical en el tratamiento unificado de datos que podría fortalecer los fines dispuestos por LOPJ (art. 461)⁵¹ y Real Decreto 1184/2006, de 13 de octubre⁵² y, por tanto, la propia misión institucional de la Comisión Nacional de Estadística Judicial (BEIRO MAGAN 2019) .

Por su parte, en el ámbito de la investigación normativa, doctrinal y jurisprudencial, la utilización de estos sistemas en combinación con IA ha dado lugar a la denominada Justicia predictiva de las resoluciones judiciales (BEIRO MAGAN 2019, p. 9) que, en España, hasta el momento, es utilizada en el sector legal privado a través de aplicaciones como jurimetría⁵³.

Esta utilización de la analítica predictiva del big data, permite generar gran cantidad de información relevante en torno a procesos judiciales específicos (posible duración, predicción de su resultado, factibilidad de recurso, antecedentes del juez, líneas de decisión más comunes en torno al tema de litigio, argumentaciones con más probabilidades de éxito, etc.) y a partir de ello, predecir cómo van a fallar los jueces.

Sin embargo, los beneficios de estas aplicaciones, han puesto sobre la mesa el debate sobre el posible “efecto sustitución” de los juristas tal como se está dando en el sector privado⁵⁴, según el cual comienza a valorarse la posibilidad de que el que los juicios puedan resolverse en base a algoritmos (GARCÍA JIMÉNEZ 2021), es decir, que el juez -abogado sea sustituido por el juez-robot (BEIRO MAGAN 2019).

⁵¹Relativo a la estadística judicial y al rol de la Comisión Nacional de Estadística Judicial.

⁵²Sobre la estructura, composición y funciones de la Comisión Nacional de Estadística Judicial.

⁵³Aplicación disponible en: <https://jurimetria.laleynext.es/content/QueEs.aspx> [Consulta: 2 de marzo de 2022].

⁵⁴Los bufetes admiten que los robots ya suplen a algunos abogados. Disponible en: https://cincodias.elpais.com/cincodias/2019/12/03/legal/1575388049_051347.html [Consulta: 25 de junio de 2022].

En este sentido, se trata de máquinas (software) que, a partir de enormes cantidades de datos (legales, doctrinales, etc.) introducidos en sus sistemas y dotados de IA, pueden ejecutar procesos de razonamiento con capacidad de aprender y mejorar su capacidad por la experiencia, sin necesidad de ser expresamente programadas al efecto, que es lo que se conoce como “machine learning” (o aprendizaje automatizado) (MANRIQUE ROJAS 2020).

Al respecto, se detectan experiencias del estilo, sobre todo, para la resolución de reclamaciones judiciales de menor cuantía. Un ejemplo de ello se da en Estonia, donde se aplica para conflictos de montos inferiores a siete mil euros y dentro de la etapa de iniciación de la controversia. Asimismo, se identifican proyectos similares, aunque con carácter más incipiente, en Estados Unidos y China (GARCÍA JIMÉNEZ 2021, p. 315).

También se encuentra dentro de este supuesto la Plataforma ODR para la resolución de conflictos en línea⁵⁵, sitio web interactivo y multilingüe que facilita gratuitamente a empresas y consumidores, un punto de acceso para la solución extrajudicial de litigios contractuales derivados de contratos de compraventa o prestación de servicios celebrados en línea⁵⁶.

Lo cierto, es que más allá de esta posible aplicación del juez-robot en términos sustitutivos del juez-humano, si podrían generarse a través de estas tecnologías, importantes beneficios en su carácter de herramienta complementaria de la labor de los juristas, por ejemplo, para consultar bases de datos, filtrar información, organizarla, asistir para la toma de decisiones complejas, entre otras. Es decir, ya no como amenaza, sino como apoyo al razonamiento del jurista y en su caso, como reto a su capacidad intelectual (GARCÍA JIMÉNEZ 2021, p. 316).

Por último, en relación a los desafíos que, en general, trae aparejado el tratamiento de datos a través de sistemas big data, pueden mencionarse, entre otros, la necesidad de garantizar una absoluta transparencia sobre la información que se recaba, cómo se procesa, su finalidad, etc. En este sentido asume especial relevancia el principio de finalidad y minimización de datos (art.5.1 RGPD) ya que uno de los inconvenientes de los proyectos big data frente a la

⁵⁵ Acceso disponible en: <http://ec.europa.eu/odr> [Consulta: 26 de junio de 2022].

⁵⁶ Plataforma ODR para la resolución de conflictos en línea. Disponible en: <https://www.consumo.gob.es/es/consumo/plataforma-odr-para-la-resoluci-n-de-conflictos-en-l-nea#:~:text=Se%20trata%20del%20sitio%20web,de%20servicios%20celebrados%20en%20l%C3%ADnea>. [Consulta: 26 de junio de 2022].

protección de datos suele ser “que no siempre se conoce desde el comienzo el alcance del proyecto” (ÁLVAREZ HERNANDO 2020, p. 1574), pues los conocimientos que potencialmente pueden ser revelados por estos sistemas pueden extender los límites de la finalidad original⁵⁷ e incluso modificarla⁵⁸(MORALES CÁCERES 2021).

En segundo lugar, y en relación a lo anterior, también plantea desafíos el requisito del consentimiento, particularmente para el caso de que se requiera un tratamiento que no se preveía cuando se recogieron los datos (MORALES CÁCERES 2021). Al respecto, COTINO HUESO señala que el derecho a la protección de datos ha girado fundamentalmente hasta la actualidad, en relación al consentimiento del titular de esos datos. No obstante, en la práctica, ese consentimiento viene dado casi por defecto, de ahí que no es realista creer en la efectividad del control de la información personal a través del consentimiento y sus derechos complementarios, mucho menos ante la ola arrolladora del big data. De ahí, es que ante estas garantías meramente subjetivas dependientes de la acción del interesado, deben reforzarse las obligaciones preventivas derivadas de los principios de privacidad en el diseño y por defecto y de evaluación de impacto a la privacidad (COTINO HUESO 2017, p. 145).

En tercer lugar y para finalizar, es imprescindible que los perfiles de ciudadanos que puedan generarse a través de la gestión inteligente de datos carezcan de sesgos discriminatorios, especialmente, en relación a sectores poblacionales más vulnerables que podrían ser aún más excluidos en base a los resultados obtenidos, pues esto se convertiría en la “dictadura de los datos” (AEPD y ISMS FORUM SPAIN 2018, p. 4).

Un ejemplo de ello puede identificarse en Países Bajos, Estado que, de acuerdo al Informe “Xenophobic Machines”⁵⁹ elaborado por Amnistía Internacional (2021), diseñó un algoritmo

⁵⁷En este ámbito se entiende indispensable que exista un cierto equilibrio entre la información que ostentan los poderes públicos que tratan datos personales a través de big data y aquella que poseen las personas cuyos datos son tratados.

⁵⁸Tal como sucede con la reutilización de datos obtenidos para la primera finalidad (MORALES CÁCERES 2021).

⁵⁹Máquinas xenóforas. Discriminación a través del uso no regulado de algoritmos en el escándalo de los beneficios del cuidado infantil holandés. Disponible en: https://doc.es.amnesty.org/ms-opac/search?fq=msstored_fld99&fv=*&doc-return=search&advanced=true&mandatoryTerms=&mandatoryPhrase=&optionalTerms=&prohibitedTerms=&fq=mssearch_geographics&fv=*&msstored_mltgeographics=&fq=mssearch_materials&fv=*&msstored_materials=&fq=mssearch_doctype&fv=*&fq=mssearch_typology&fv=*&dateFrom=&dateTo=&fq=mssearch_fld13&fv=EU R35468621 [Consulta: 2 de julio de 2022].

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

xenófobo basado en la configuración de perfiles raciales que impidió a progenitores y familias, particularmente de ingresos bajos y minorías étnicas, recibir subvenciones para el cuidado infantil, bajo la falsa acusación de fraude tributario.

2.5.2 Inteligencia artificial

La IA es “la disciplina dentro de la informática o la ingeniería cuyo objetivo es el desarrollo de sistemas computacionales (no biológicos) inteligentes, tomando como referencia la inteligencia humana” (OLIVER RAMÍREZ 2019, p.10)⁶⁰. En este sentido, persigue la creación de algoritmos para diseñar y desarrollar máquinas que puedan imitar capacidades del ser humano como, su aprendizaje, razonamiento, optimización de decisiones, mejora por la experiencia, entre otras. En pocas palabras, se trata de la inteligencia de máquinas que son creadas para ejecutar acciones que emulan la inteligencia humana⁶¹ y pueden superarla (ORTEGA RUÍZ y BECERRA 2021).

Ahora bien, considerando explicar el funcionamiento técnico de la IA excede las finalidades de este modesto trabajo, interesa una breve descripción de sus características y posibles aplicaciones en la Administración de Justicia.

Al respecto, se trata de una disciplina caracterizada por ser transversal, es decir, aplicable a cualquier ámbito del conocimiento o social, multidisciplinar⁶², compleja, invisible y actualizable (ya que es un software) con capacidad de explicar el pasado, el presente y predecir el futuro (OLIVER RAMÍREZ 2019).

En este último sentido, la IA mantiene una íntima relación con el big data⁶³, particularmente, cuando los sistemas computacionales son capaces de tratar, aprender, solucionar y adoptar decisiones en base a grandes cantidades de datos, es decir, cuando a estos datos se les aplican

⁶⁰Hacia una Inteligencia Artificial por y para la sociedad. Disponible en: <https://umhsapiens.com/hacia-una-inteligencia-artificial-por-y-para-la-sociedad/> [Consulta: 26 de junio de 2022].

⁶¹También puede entenderse a la IA como un “sistema de datos humanos que generan subdatos artificiales” (ORTEGA RUÍZ y BECERRA 2021, p. 219).

⁶²Ya que intervine la computación junto a otras áreas de conocimiento como la ingeniería, la matemática, la lingüística, la filosofía etc. (ÁLVAREZ HERNANDO 2020, p. 1582).

⁶³Los sistemas big data constituyen una base fundamental para el funcionamiento de la IA (ORTEGA RUÍZ y BECERRA 2021).

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital
algoritmos, patrones de razonamiento y redes neuronales artificiales que conducen a conclusiones (COTINO HUESO 2017, p. 132).

Al respecto, al desarrollar el tema de big data se hizo referencia al “machine learning” que no es auto programación, sino auto aprendizaje de datos y experiencia para generar patrones y resolver nuevas tareas (MANRIQUE ROJAS 2020, p. 587).

Al respecto, el “machine learning” es una rama de la IA cuyos tipos son el aprendizaje supervisado (algoritmos que aprenden de datos clasificados o etiquetados introducidos por la intervención humana y genera datos de salida a fin de aplicarse en un análisis); el no supervisado (algoritmos que funcionan con datos no clasificados o etiquetados y se orientan a descubrir patrones o relaciones entre ellos, más conocido como modelo predictivo); y reforzado (en el cual no se trabaja en base a datos clasificados o no clasificados, sino que el sistema aprende a través de acciones y de los resultados obtenidos, y se refuerza luego de resolver un problema, por la experiencia)(MANRIQUE ROJAS 2020).

Cabe destacar que autores como ÁLVAREZ HERNANDO incluyen al “machine learning” como una técnica de IA a las que se suman, la minería de datos “data mining”, redes neuronales, lógica difusa, redes de creencia, procesamiento de lenguaje natural, sistema de expertos, vida artificial, entre otras (ÁLVAREZ HERNANDO 2020, pp. 1584-1585).

Ahora bien, considerando los tipos y técnicas de IA mencionadas, interesan sus posibles aplicaciones en el ámbito de la Administración de Justicia a cuyo respecto ya se ha hecho referencia a la denominada gestión inteligente de datos a fines de la estadística judicial y Justicia predictiva, a las que podrían agregarse una mayor automatización de los tramites del proceso judicial, asistencia al juez durante el proceso de decisión y en la propia toma decisión⁶⁴, mediación electrónica, valoración de prueba digital (DELGADO MARTÍN 2021, pp. 40-41), asistencia en la búsqueda y elaboración de documentación oficial, asistencia a trabajadores judiciales en la automatización de tareas y elaboración de borradores de documentos oficiales, traducción de documentos y atención a la ciudadanía, entre otras.

⁶⁴Particularmente útil en supuestos de homogeneidad de acciones entabladas, contestación de demandas similares, resolución de casos de escasa complejidad, litigación en masa en materia de derecho de consumo, entre otros.

Cabe resaltar que uno de los software con los que más se está experimentando en proyectos con interacción humana, como la atención a la ciudadanía, son los denominados robots de conversación (chatbots) y asistentes virtuales inteligentes cuyas funcionalidades van, desde respuestas preestablecidas, hasta la capacidad para mejorar por sí mismos, sea a través de su conexión con bases de datos externas, mediante la incorporación de nuevos datos obtenidos por la experiencia, o en virtud del entrenamiento constante con sus programadores. De ahí, es que se entiende que estas iniciativas podrían generar un cambio trascendental para facilitar el acceso a la Justicia por parte de la ciudadanía (BEIRO MAGAN 2019, p. 12).

Por último, respecto a los desafíos ante la protección de datos, además de los supuestos en que se utilice IA para tratar datos masivos (como se ha visto al desarrollar el tema big data), existen distintos escenarios que deben ser considerados. En este sentido, es de especial interés la guía elaborada por la AEPD relativa a la “Adecuación al RGPD de tratamientos que incorporan IA”⁶⁵ ya que presenta un desarrollo integral sobre este tema.

En este marco, primero debe tenerse en cuenta que no todas las soluciones de IA tratan datos personales (ej. sistemas de control de calidad de productos), segundo, que hay casos en las aplicaciones de IA elaboran de manera automatizada perfiles (ej. de potenciales consumidores) o adoptan decisiones sobre ellos, supuestos en donde evidentemente deberá respetarse la normativa de protección de datos. A su vez, puede darse que a través de IA se traten datos de interesados (ej. políticas de marketing de una empresa en base a preferencias de sus clientes) o que los interesados adquieran un producto o servicio con IA que trate sus datos personales (pulsera deportiva inteligente). Véase aquí la importancia que asumen en uno u otro caso el consentimiento y la información de que dispone el interesado.

Por su parte, también el denominado “sesgo de algoritmo” plantea desafíos, particularmente al principio de licitud según el cual, entre otros aspectos, deben implementarse medidas que prevengan tratamientos que puedan afectar derechos fundamentales. Precisamente, aun cuando el algoritmo en sí, sea una fórmula matemática, en principio, objetiva y neutral, puede

⁶⁵La AEPD publica una guía para adaptar al RGPD los productos y servicios que utilicen IA. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-una-guia-para-adaptar-al-rgpd-los-productos-y> [Consulta: 27 de junio de 2022].

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital
reflejar valores humanos que estuvieron presentes en su codificación y en la recolección de datos para su entrenamiento, por ejemplo, género y raza⁶⁶(MORALES CÁCERES 2021).

Por último, cabe resaltar que el “machine learning” asociado al big data, también puede desafiar al principio de finalidad y la base legitimadora del tratamiento, ya que se trata de una tecnología basada en lo inesperado de su resultado (MORALES CÁCERES 2021).

En resumen, todas estas variantes y particularidades evidencian el amplio marco de desafíos que plantea la utilización de IA al derecho de protección de datos personales.

2.5.3 Blockchain (cadena de bloques)

En términos generales, el blockchain como tecnología de encriptación, es un procedimiento de carácter matemático que permite ordenar un conjunto de datos en bloques, de modo tal que solo se puede modificar la información contenida en un bloque, alterando los posteriores, es decir, la cadena de bloques (BEIRO MAGAN 2019, p. 10). La información así generada y compartida, constituye un estilo de verdad consensuada con características de irreversibilidad, que ofrece un alto nivel de integridad y autenticidad de la información limitando su manipulación (ÁLVAREZ HERNANDO 2020).

Desde esta perspectiva y sin entrar al campo estrictamente técnico, puede decirse que uno de los conceptos centrales para comprender el funcionamiento la cadena de bloques es, precisamente, el de bloque. Al respecto, se trata de un software que registra un conjunto de datos de manera cronológica, por tanto, cada bloque que forma la cadena contiene dos códigos⁶⁷, uno el del bloque que le precede⁶⁸ y otro que explica cuál es el que le sigue, es decir, se encuentran entrelazados entre sí y además, son distribuidos de forma replicada a través de

⁶⁶También el documento de la Comisión Europea “Directrices éticas para una IA fiable” (2019) destaca la importancia de que los ciudadanos tengan control de sus datos y que estos no sean utilizados para discriminarlos o perjudicarlos. Disponible en: <https://data.europa.eu/doi/10.2759/14078> [Consulta: 29 de mayo].

⁶⁷Salvo que sea el primero (bloque génesis).

⁶⁸Además, contiene un resumen de ese bloque, que permite verificar que no sido modificado (MELA y CEDEÑO HERRERA 2019).

un conjunto de nodos que conforman redes descentralizadas⁶⁹. Cabe destacar que a estos bloques entrelazados, se les aplica una firma criptográfica⁷⁰(MELA y CEDEÑO HERRERA 2019).

Esta tecnología ha tenido su auge en el marco de las criptomonedas, inicialmente en Bitcoin, no obstante, en la actualidad, se aplica a áreas como contratos inteligentes, almacenamiento en la nube, sistemas de registro documental, transacciones bancarias etc. Asimismo, se la considera idónea para mejorar procesos en entornos big data, en el sentido de que puede proporcionar robustez, transparencia y seguridad a cantidades ingentes de bases datos, fortaleciéndolas ante múltiples amenazas, desde fugas de información hasta manipulación maliciosa de su contenido y toda clase de ciberdelincuencia en general (DOLADER RETAMAL, BEL ROIG y MUÑOZ TAPIA 2017, p. 33)⁷¹.

Por su parte, a nivel judicial, además de su posible aplicación para el fortalecimiento de sistemas de gestión masiva e inteligente de datos, (donde trabajaría junto a sistemas big data e IA), se destacan virtudes en materia procesal e integridad del expediente judicial electrónico, entre otros⁷².

Así, a nivel procesal puede brindar, por ejemplo, un importante aporte en materia de fiabilidad de la prueba digital. En este sentido, la cadena de bloques permitiría acreditar la integridad y autenticidad de un documento o su contenido en relación a su existencia en un momento determinado. Por tanto, en el proceso no habría que probar la cadena de bloques, sino que esta sería la fuente de prueba que acredita que un contenido registrado por ella, goza de autenticidad e integridad. Asimismo, y de manera consecuente como tecnología de encriptación, favorece la protección de los datos obrantes en esos documentos (DELGADO MARTÍN 2021, p.30).

Por su parte, también puede implementarse en relación al expediente judicial electrónico. En este sentido, cada vez que se incorpore un documento al expediente, se le puede aplicar una

⁶⁹Que con carácter general pueden ser públicas, privadas o semiprivadas.

⁷⁰Que da lugar al denominado código “hash” de carácter alfanumérico y que se constituye por la aplicación de un código matemático sobre los datos del bloque.

⁷¹También puede ser útil a efectos de controlar la ubicación de pruebas mediante registro (ej. en materia penal) o favorecer la trazabilidad de transacciones económicas, entre otras (PASCUAL GARCÍA 2021).

⁷²Por ejemplo, la mediación electrónica, fundamentalmente para favorecer la trazabilidad del procedimiento y la protección de los datos personales que se vuelcan en él.

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

cadena de bloques lo que limitaría posibles alteraciones. Asimismo, permitiría registrar accesos a dichos documentos o comunicaciones y notificaciones entre los operadores judiciales que participan del proceso disuadiendo así, potenciales accesos indebidos o modificaciones documentales deliberadas (PASCUAL GARCÍA 2021).

Para finalizar, en relación a algunos de los desafíos de estas tecnologías generan para la protección de datos, se considera de especial interés el Informe del Observatorio y el Foro de la UE “Blockchain y RGPD”⁷³ del año 2018.

Al respecto, debe partirse de que en los proyectos blockchain puede existir un tratamiento de datos personales, sobre todo en el contenido de los bloques⁷⁴.

En este marco, según el mencionado Informe, uno de los mayores desafíos se da respecto a la identificación del responsable del tratamiento, ya que como red descentralizada no existiría un actor único (o nodo) que adopte decisiones sobre ella o la ordene unilateralmente⁷⁵. Este aspecto, a su vez, trae aparejado como consecuencia, que también surjan desafíos para efectivizar el ejercicio del derecho de acceso, pues sin responsable, no podría determinarse ante quien requerirlo. Asimismo, en relación a los demás derechos (rectificación, supresión, oposición, etc.) (MÉNDEZ 2019).

Por último, otro de los desafíos mencionados en el documento, gira en torno a la determinación de la base legitimadora. En tal sentido, el requisito principal para introducir datos en blockchain, consiste en descargar el denominado software “cliente”, sin embargo, ante la ausencia de un responsable identificado, surge la dificultad de ante quien otorgaría el usuario su consentimiento para legitimar el tratamiento, o con que información contaría al efecto, entre otros aspectos vinculados (MÉNDEZ 2019).

⁷³Disponible en: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [Consulta: 2 de julio de 2022].

⁷⁴Asimismo, respecto a los actores intervinientes dentro de las redes descentralizadas (mineros y participantes), particularmente, cuando disponen de una clave identificativa de usuario, permitiéndoles participar de este sistema. Aspecto que no se aborda atento a que excede los límites del presente trabajo.

⁷⁵Aspecto que puede relajarse según se trate de redes públicas, privadas o semiprivadas.

3.Conclusiones

Tras este breve recorrido sobre algunos aspectos centrales relativos a la implementación del derecho a la protección de datos en el ámbito de la Administración de Justicia en España, es posible extraer las siguientes conclusiones:

Primera: La Justicia trata una enorme cantidad de datos “sensibles” en los procesos, lo que representa un riesgo para diversos derechos fundamentales, entre ellos, el de protección de datos, con la particularidad de que la base jurídica del tratamiento, no es necesariamente el consentimiento de los interesados, sino preponderantemente, el ejercicio de poderes públicos. De ahí es que, acorde a su rol garante de derechos, es indispensable que su funcionamiento, regido por normas y principios singulares, se adecue a las pautas establecidas por el RGPD y LOPDGDD. No obstante, del análisis del régimen jurídico, se observa que ambas legislaciones se limitan a extender la aplicabilidad de sus normas al ámbito de la Administración de Justicia, pero sin consideración a las especificidades propias de su organización y del ejercicio de sus funciones.

Segunda: Ante la falta de previsión de una normativa específica e integral en el RGPD y LOPDGDD, se abre paso a un régimen jurídico amplio y fragmentado, encabezado por la LOPJ, pero acompañada de multiplicidad de normas complementarias. Un ejemplo de ello es que, a fines de analizar las singularidades de la protección de datos a nivel judicial y en particular, en el marco del proceso y del tratamiento de ficheros jurisdiccionales, se hace necesario recurrir a diversidad de normas y reglamentaciones. En este sentido, se evidencia una regulación casuística, dispersa y no libre de vaguedades, por lo que se entiende que encajar el sistema de protección de datos al funcionamiento del proceso judicial es una tarea pendiente de desarrollar para el legislador.

Tercera: Parece poco adecuada la remisión de la LOPJ a la ley procesal a fines de permitir el ejercicio de los derechos que integran el sistema de protección de datos. Pues, del análisis del régimen jurídico, no surge un Derecho procesal con categorías dogmáticas diseñadas al efecto, por lo que el rol de juzgador y el valor del caso concreto, terminan asumiendo un protagonismo tal, que subyace evidente la limitación al derecho de protección de datos. En otras palabras, si se acepta la remisión al Derecho procesal, urge que el legislador actualice y

Protección de Datos en el Ámbito de la Administración de Justicia y de su Transformación Digital

rediseñe sus categorías dogmáticas para evitar la construcción ad hoc por el juzgador, atento a la inseguridad jurídica que esto conlleva para los ciudadanos ante la Administración Judicial.

Cuarta: Un aspecto que no puede soslayarse del análisis del régimen jurídico, es el relativo al rol del CGPD como autoridad de control de los ficheros jurisdiccionales, competencia asignada en aras al respeto de la independencia judicial. No obstante, aun cuando se trate de un aspecto no analizado en detalle, queda el interrogante sobre la efectividad de su función, pues en definitiva actúa como juez y parte, en el sentido de aquel que se controla a sí mismo. Quedaría pensar, si no existen otras formas de regulación que, respetando la independencia judicial, aseguren un control con mayor legitimación de cara a la ciudadanía y demás Poderes del Estado. Y, asimismo, capaces de imitar el nivel de especialización en el ejercicio de funciones de que goza la AEPD, algo que, a día de hoy, no ostenta el CGPD.

Quinta: A partir del análisis efectuado, se entiende la necesidad de abordar cambios en la materia y avanzar hacia un corpus iuris único que regule de manera integral y unificada el derecho de protección de datos en todo su alcance, capaz de responder a las preguntas que plantea la práctica procesal y acorde a las reglas y principios que rigen el funcionamiento de la Administración de Justicia y, en particular, su función jurisdiccional.

Sexta: Al analizar la relación con la publicidad procesal se puede observar, casi por intuición, que las normas de protección de datos entran en tensión con las garantías emergentes de este principio, particularmente, en lo relativo al acceso de terceros interesados al expediente judicial, ya que, en él, pueden confluir datos protegidos e información accesible al público. En este sentido, se entiende que el desafío consiste en delimitar con claridad qué información se protege y de qué modo, pues del análisis de los filtros para la protección de datos establecidos por LOPJ, junto a la facultad de supresión conferida a los Tribunales, surge evidente la preponderancia del criterio discrecional del juzgador, con la consecuencia de que, al otro lado, se encuentra un principio central del Estado de derecho y que hace a la tutela judicial efectiva. Por tanto, siguiendo con la idea un corpus iuris integral, puede pensarse en que las excepciones al principio de publicidad estén claramente unificadas, acompañadas de criterios claros de valoración e identificación de categorías de datos accesibles o restringidos. Asimismo, que establezca un régimen agravado de responsabilidad ante accesos injustificados, violación del deber de secreto o divulgación indebida de información.

Séptima: Es evidente que la asistencia telemática, el expediente electrónico y la publicidad online de sentencias, han traído múltiples ventajas para el sistema judicial. No obstante, ello exige que se presten cuidados especiales al tratamiento de datos a través de la red, pues la modernización no puede implementarse a costa de un incremento de perjuicios o potenciales violaciones a derechos. Se impone así, una regulación normativa en constante actualización, capaz de lograr que la aplicación de las TIC, en cualquier caso, sea conciliable con las garantías procesales y derechos fundamentales ya que, de lo contrario, se trataría de un retroceso y limitación al servicio de la tecnología.

Octava: Para la plena efectividad de la transformación digital, la regulación específica, debe estar acompañada de dos aspectos claves: la calidad de la infraestructura tecnológica (hardware y software), que sea capaz de garantizar la seguridad de la información y el respecto a los principios procesales de publicidad, oralidad, intermediación y contradicción (ej. sonido, imagen, interacción en tiempo real, etc.); Y, la capacidad de los recursos humanos para lograrlo. En este sentido, se impone la necesidad de un cambio cultural hacia la adaptación constante. Cabe resaltar que, en ambos aspectos, el respaldo presupuestario y la gobernanza del sistema de implementación de esta transformación, serán fundamentales.

Novena: Las tecnologías disruptivas ha invadido la vida diaria y como se ha visto, su desembarco en la Justicia ya ha comenzado. Su potencial es increíble, una justicia más transparente, ágil, eficiente y eficaz, e incluso, más cercana al ciudadano, parece posible. No obstante, ante un exceso de optimismo, subyacen importantes desafíos legales, técnicos y morales. Al respecto, se entiende que el primer paso es acordar los valores y reglas éticas que han de guiar la creación e implantación de estos sistemas y su regulación y, en este sentido, una premisa se considera fundamental: las tecnologías no reemplazan personas solo sustituyen tareas y, en ningún caso, pueden utilizarse con fines discriminatorios o en contra de la dignidad de las personas, pues, de ser así, se configuraría “la dictadura del sistema tecnológico”. Queda, por tanto, en tarea del legislador junto a la doctrina y la jurisprudencia, ir perfilando soluciones capaces de encontrar un sano equilibrio entre el aprovechamiento de las oportunidades emergentes, la vigencia de los pilares del Estado de Derecho y el pleno respeto a los derechos fundamentales de las personas.

Referencias bibliográficas

Bibliografía básica

ABAD ALCALÁ, L. «El principio constitucional de publicidad procesal y el derecho a la información». *Cuadernos Constitucionales* [en línea]. 2021, núm. 2, pp. 9-30 [consulta: abril 2022]. ISSN 2660-9231. Disponible en: <https://doi.org/10.7203/cc.2.21527>

ÁLVAREZ HERNANDO, J. *Practicum en Protección de Datos 2021*. 1ª ed. Pamplona: Aranzadi, S.A.U., 2020.

ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos en Europa*. 1ª ed. Valencia: Tirant lo Blanch, 2006.

ARIZA COLMAREJO, M. «Principio de publicidad procesal y protección de datos», 491-510. En GONZÁLEZ GRANDA, P. (ed). *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional*. 1ª ed. Madrid: Dykinson, 2021.

ARIZA COLMAREJO, M. «Tratamiento de datos en la tramitación judicial». En PÉREZ-LUÑO ROBLEDO, E. y DOMÍNGUEZ BARRAGÁN, M. (ed). *La administración de justicia en España y en América: José Martín Ostos, Liber amicorum*. 1ª ed. Sevilla: Astigi, 2021.

AYNETO GUBERT, X. «La industria 4.0, el nuevo motor de la innovación industria». *Revista Dirección y Organización (DyO)* [en línea]. 2019, núm. 69, pp. 99-110 [consulta: junio de 2022]. ISSN 2171-6323. Disponible en: <https://doi.org/10.37610/dyo.v0i69.563>

BALLESTAR, M.T., RIBEIRO, D. y SAINZ, J. «¿Es el Big Data el siguiente paso en la digitalización de la empresa?». *Revista economía industrial* [en línea]. 2018, núm. 409, pp. 47-56 [consulta: mayo de 2022]. ISSN 0422-2784. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6650446&orden=0&info=link>

BEIRO MAGAN, J. «Retos tecnológicos de la administración de justicia española para la tercera década del siglo XXI». *Pensamiento crítico. Cuaderno digital de opinión*. 2019 [Consulta: junio de 2022] Disponible en: <https://pensamientocritico.sisej.com/retos-tecnologicos-de-la-administracion-de-justicia-espanola-para-la-tercera-decada-del-siglo-xxi/>

BUSTAMANTE RÚA, M. y MARÍN TAPIERO, J. «Justicia digital, acceso a internet y protección de datos personales». *Revista internacional de derecho* [en línea]. 2021, vol. 2, núm. 1, pp. 5-22 [consulta: junio de 2022]. ISSN 2788-7448. Disponible en: <https://doi.org/10.37768/unw.rid.02.01.001>

CABEZUDO RODRÍGUEZ, N. «Ficheros automatizados y registros centrales de la Administración de Justicia: la obtención de los datos y de la gestión de las informaciones», 153-194. En PEDRAZ PENALVA, E. (ed). *Protección de datos y proceso penal*. 1ª ed. Madrid: La Ley-Actualidad, 2010.

CALDERÓN CUADRADO, M. P. «El acceso a libros, registros y archivos judiciales (publicidad de las actuaciones concluido el proceso)». *Boletín de Información del Ministerio de Justicia* [en línea]. 2000, núm. 1872, pp. 2159-2188 [consulta: marzo de 2022]. ISSN 0211-4267. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/78659.pdf>

CANO GALÁN, Y. «La seudonimización y la anonimización de datos personales en las sentencias del orden jurisdiccional social». *Documentación Laboral* [en línea]. 2020, núm. 119, pp. 31-56 [consulta: abril 2022]. ISSN 0211-8556. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/7544416.pdf>

COLLADO CALVO, M. A. «El comercio de datos: el oro negro del siglo XXI». *Revista de Estudios Económicos y Empresariales* [en línea]. 2019, núm. 31, pp. 89-142 [consulta: junio de 2022]. ISSN: 0212-7237. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=7444484&orden=0&info=link>

COTINO HUESO, L. «Big data e inteligencia artificial: Una aproximación a su tratamiento jurídico desde los derechos fundamentales». *Dilemata* [en línea]. 2017, núm. 24, pp. 131-150 [consulta: abril 2022]. ISSN: 1989-7022. Disponible en: <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104>

DELGADO MARTÍN, J. «Reflexiones sobre el estado actual de la transformación digital de la justicia». *Revista Acta Judicial* [en línea]. 2021, núm. 8, pp. 27-43 [consulta: abril de 2022]. ISSN 2603-7173. Disponible en: <https://revistaactajudicial.letradosdejusticia.es/index.php/raj/article/view/58>

DELGADO MARTÍN, J. «Reflexiones sobre la protección de datos personales en la Administración de Justicia». *Diario La Ley* [en línea]. 2019, núm. 9363 [Consulta: abril de 2022]. ISSN 1989-6913.

DOLADER RETAMAL, C. BEL ROIG, J. y MUÑOZ TAPIA, J. «La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas». *Revista Economía industrial* [en línea]. 2017, núm. 405, pp. 33-40 [consulta: mayo de 2022]. ISSN 0422-2784. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6207510&orden=0&info=link>

GARCÍA JIMÉNEZ, A. «Las nuevas tecnologías y la Administración de Justicia. Un nuevo paradigma para los juristas, en especial los jueces». *Revista Tribuna de actualidad* [en línea]. 2021, núm. 2, pp. 309-317 [consulta: mayo de 2022]. ISSN 1138-8870. Disponible en: <https://doi.org/10.24310/rejlss.vi2.12459>

GARCÍA SANZ, J. y GUIMARAES-DA SILVA J. «Las vistas telemáticas en el proceso civil español: visión comparada, regulación y cuestiones prácticas que suscita su celebración». *Diario La Ley* [en línea]. 2020, núm. 9659 [Consulta: abril de 2022]. ISSN 1989-6913. Disponible en: <https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbF1CTEAAmNDIwMTC7Wy1KLizPw827DM9NS8klQAYoIO6SAAAAA=WKE>

GIL GONZÁLEZ, E. *Big Data, privacidad y protección de datos*. 1ª ed. Madrid: Boletín Oficial del Estado (BOE), 2016.

GÓMEZ LOECHES, L. «La publicidad de las actuaciones judiciales: Teoría y práctica del derecho de acceso». *Revista Boletín de la ANABAD* [en línea]. 1999, Tomo 49, núm. 3-4, pp. 359-370 [consulta: abril de 2022]. ISSN 0210-4164. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/51169.pdf>

MANRIQUE ROJAS, E. «Machine Learning: análisis de lenguajes de programación y herramientas para desarrollo». *Revista Ibérica de Sistemas y Tecnologías de Información* [en línea]. 2020, núm. E28, pp. 586-599 [consulta: junio de 2022]. ISSN 1646-9895. Disponible en: <http://www.risti.xyz/issues/ristie28.pdf>

MARCOS AYJÓN, M. «La protección de datos en el ordenamiento europeo y en España». *Revista de derecho penal y criminología*, [en línea]. 2013, núm. Extra 1, pp. 81-117 [consulta:

abril 2022]. ISSN 1132-9955. Disponible en:
<https://revistas.uned.es/index.php/RDPC/article/view/25012>

MARCOS AYJÓN, M. *La protección de datos de carácter personal en la justicia penal*. 1ª ed. Barcelona: J. M. BOSCH, 2020

MEDINA MORALES, D. «Las nuevas tic y la administración de justicia LexNET, el soporte español». *Journal of Ethics and Legal Technologies* [en línea]. 2019, vol. 1, núm. 1, pp. 77-94 [consulta: junio de 2022]. ISSN 2612-4920. Disponible en:
<https://jelt.padovauniversitypress.it/system/files/papers/jelt-01-01-05.pdf>

MELA N., J., y CEDEÑO HERRERA, E. «Tecnologías Blockchain y sus aplicaciones». *Revista Visión Antataura* [en línea]. 2019, vol. 3, núm. 2, pp. 110-126 [consulta: junio de 2022]. ISSN 2309-6373. Disponible en: <https://revistas.up.ac.pa/index.php/antataura/article/view/1061>.

MIRA ROS, C. «la tutela judicial en el ciberespacio: nuevos interrogantes en el ámbito de las comunicaciones electrónicas». *Anales de la Real Academia de Doctores de España* [en línea]. 2012, vol. 16, núm. 1, pp. 05-116 [consulta: abril 2022]. ISSN: 1138-2414. Disponible en:
<https://www.radoctores.es/doc/1V16N1-mira%20ros-tutelajudicialenciberespacio.pdf>

MIRA ROS, C. *Algunas reflexiones sobre la protección de datos personales en el ámbito judicial*. En: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional). Los desafíos del Poder Judicial ante la sociedad globalizada [en línea]. 2012. pp. 581-594. A Coruña: Universidade da Coruña [consulta: 12 de abril de 2022]. Disponible en: <http://hdl.handle.net/2183/9172>

MONTORO SÁNCHEZ, J. «El delegado de la protección de datos en la Administración de Justicia: ¿Una figura recomendable o incompatible?», 1177-1190. En MARTÍN RODRÍGUEZ, J. y GARCÍA ÁLVAREZ, L. *El mercado único en la Unión Europea. Balance y perspectivas jurídico-políticas*. 1ª ed. Madrid: Dykinson, 2019.

MORALES CÁCERES, A. «El impacto de la inteligencia artificial en el Derecho». *Revista Advocatus* [en línea]. 2021, núm. 39, pp. 39-71 [consulta: abril de 2022]. ISSN 1996-4773
 Disponible en:
<https://revistas.ulima.edu.pe/index.php/Advocatus/article/download/5117/4930/>

OLIVER RAMÍREZ, N. «Hacia una inteligencia artificial por y para la sociedad» *Revista Bit* [en línea]. 2019, núm. 214, pp. 8-13 [consulta: junio de 2022]. ISSN 0210-3923. Disponible en: <https://www.coit.es/archivo-bit/bit-214/hacia-una-inteligencia-artificial-por-y-para-la-sociedad>

ORTEGA RUÍZ, L. y BECERRA, J. «La Inteligencia Artificial en la decisión jurídica y política». *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales* [en línea]. 2022, vol. 24, núm. 49, pp. 217,238 [consulta: junio de 2022]. ISSN 1575-6823. Disponible en: <https://doi.org/10.12795.10>

PLATERO ALCÓN, A. «Lexnet como máximo exponente del sistema de justicia electrónica en España: Especial referencia a su tratamiento de datos personales». *Revista de Ciencias Jurídicas* [en línea]. 2020, núm. 152, pp. 13-42 [consulta: junio de 2022]. ISSN 0034-7787. Disponible en: <https://revistas.ucr.ac.cr/index.php/juridicas/article/view/42568/42825>

PUYOL MORENO, J. «Una aproximación a Big Data». *Revista De Derecho De La UNED*, [en línea]. 2014, núm. 14, pp. 471–506 [consulta: marzo de 2022]. ISSN 1886-9912. Disponible en: <https://doi.org/10.5944/rduned.14.2014.13303>

QUINTERO, J., MOLLAR VILLANUEVA, M. y GÓMEZ MONTAYA, F. «Analítica de datos para sistemas de costos basados en actividades en la era de big data». *Revista del Instituto Internacional de Costos* [en línea]. 2018, núm. Extra 1, pp. 64-82 [consulta: mayo de 2022]. ISSN 1646-6896. Disponible en: <https://dialnet.unirioja.es/download/articulo/7457929.pdf>

RALLO LOMBARTÉ, A. «El nuevo derecho de protección de datos». *Revista Española de Derecho Constitucional* [en línea]. 2019, núm. 116, pp. 45-74 [consulta: marzo de 2022]. ISSN 0211-5743. Disponible en: <https://doi.org/10.18042/cepc/redc.116.02>

RODRÍGUEZ AYUSO, J. F. *El delegado de protección de datos en la Administración de Justicia*. En: Actas del I Congreso Internacional “La Administración de Justicia en España y en América” [en línea]. pp. 521-530. Sevilla: Astigi, 2019 [consulta: junio 2022]. Disponible en: <https://hdl.handle.net/11441/132209>

RODRÍGUEZ ROCA, A. *La Protección de Datos Personales en la Administración de Justicia*. Director: Miguel Rodríguez Blanco. Universidad Internacional de la Rioja, Logroño, 2020.

SCHWAB, K. *La cuarta revolución industrial*. 1ª ed. Barcelona: Editorial Debate. 2016.

YNZUNZA CORTÉS, C., IZAR LANDETA, J. y BOCARANDO CHACÓN, G. «El entorno de la industria 4.0: Implicaciones y perspectivas futuras». *Revista Conciencia Tecnológica* [en línea]. 2017, núm. 54, pp. 33-45 [consulta: junio de 2022]. ISSN 1405-5597. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/6405835.pdf>

Bibliografía complementaria

Artículos periodísticos y blogs

ÁLVAREZ VALLE, J. «El Big Data: Una Gran Oportunidad». La Nueva España. 11 de noviembre de 2013. Disponible en: <http://www.lne.es/opinion/2013/11/10/big-data-una-gran-oportunidad/1497242.html>

HERRÁEZ MARTÍN, G. y OTROS. «Aplicación de la Ley de Protección de Datos en los juzgados y tribunales». 2012 [consulta: junio de 2022]. Disponible en <http://www.privacidadlogica.es/wp-content/uploads/downloads/2012/09/CEJ-LOPD-en-Juzgados-y-Tribunales.pdf>

MÉNDEZ, V. «Blockchain y RGPD ¿Destinados a entenderse? Parte II». Áudea. 17 de febrero de 2019. Disponible en: <https://www.informatica-juridica.com/trabajos/proteccion-de-datos/blockchain-y-rgpd-destinados-a-entenderse-parte-ii/>

OLIVER RAMÍREZ, N. «Hacia una Inteligencia Artificial por y para la sociedad». UMH sapiens. 20 de mayo de 2021. Disponible en: <https://umhsapiens.com/hacia-una-inteligencia-artificial-por-y-para-la-sociedad/>

PASCUAL GARCÍA, A. «La evidencia digital: ¿cómo ayuda el blockchain en un juicio?». UNIR. 15 de diciembre de 2021. Disponible en: <https://www.unir.net/derecho/revista/evidencia-digital-blockchain-legaltech/>

PUYOL MORENO, J. «¿Cómo es la protección de datos en el ámbito de la Administración de Justicia? (I)». CONFILEGAL. 22 de julio de 2018. Disponible en: <https://confilegal.com/20180722-como-es-la-proteccion-de-datos-en-el-ambito-de-la-administracion-de-justicia-i/>

TRINCADO AZNAR, B. «Los bufetes admiten que los robots ya suplen a algunos abogados». El País. 8 de diciembre de 2019. Disponible en: https://cincodias.elpais.com/cincodias/2019/12/03/legal/1575388049_051347.html

«El año de los grandes ciberataques en España». El Mundo. 1 de diciembre de 2021. Disponible en: <https://www.elmundo.es/tecnologia/2021/12/01/61a63b4ae4d4d8db5a8b4577.html>

«El escándalo de los subsidios para el cuidado infantil en Países Bajos, una alerta urgente para prohibir los algoritmos racistas». Amnistía Internacional. 25 de octubre de 2021. Disponible en: <https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/el-escandalo-de-los-subsidios-para-el-cuidado-infantil-en-paises-bajos-una-alerta-urgente-para-prohibir-los-algoritmos-racistas/>

«Justicia mejora las prestaciones tecnológicas del sistema de comunicaciones electrónicas Lexnet». Ministerio de Justicia. 6 de mayo de 2022. Disponible en: <https://www.mjusticia.gob.es/ca/ElMinisterio/GabineteComunicacion/Paginas/220506-NP-Ampliacion-funcionalidades-de-LexNET.aspx>

«La AEPD opina que el Ministerio de Justicia infringió la LOPD con el caso Lexnet». Conversia. 31 de mayo de 2018. Disponible en: <https://protecciondatos.conversia.es/aedp-opiniones-lexnet-ministerio-justicia/>

Informes y dictámenes

AEPD y ISMS FORUM SPAIN. «Código de buenas prácticas en protección de datos para proyectos Big data». 25 de mayo de 2018. Disponible en: <https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>

ANEXO DE LA GUÍA PARA LA CELEBRACIÓN DE ACTUACIONES JUDICIALES TELEMÁTICAS. Consejo General del Poder Judicial. 11 de febrero de 2021. Disponible en: <https://www.poderjudicial.es/cgpj/es/Servicios/Informacion-COVID-19/Guias-y-Protocolos/Guia-para-la-celebracion-de-actuaciones-judiciales-telematicas>

COMISIÓN EUROPEA y GRUPA EKSPERTÓW WYSOKIEGO SZCZEBLA DS. SZTUCZNEJ INTELIGENCJI. «Directrices éticas para una inteligencia artificial fiable». 11 de agosto de 2019. Disponible en: <https://data.europa.eu/doi/10.2759/14078>

CONSEJO GENERAL DEL PODER JUDICIAL. Acuerdo de 20 de septiembre de 2006, del Pleno del Consejo General del Poder Judicial, de creación de ficheros de carácter personal dependientes de los órganos judiciales. Boletín Oficial del Estado, núm. 244, de 12 de octubre de 2006, páginas 35360 a 35362. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2006-17867

CONSEJO GENERAL DEL PODER JUDICIAL. Acuerdo del pleno de 15 de septiembre de 2005, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales. Boletín Oficial del Estado, núm. 231, de 27 de septiembre de 2005. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2005-15939>

FISCALÍA GENERAL DEL ESTADO. «Instrucción N° 2/2019, de 20 de diciembre, sobre la protección de datos en el ámbito del Ministerio Fiscal: el responsable y el delegado de protección de datos». Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-1003

GUÍA PARA LA CELEBRACIÓN DE ACTUACIONES JUDICIALES TELEMÁTICAS. Consejo General del Poder Judicial. 11 de febrero de 2021. Disponible en: <https://www.poderjudicial.es/cgpj/es/Servicios/Informacion-COVID-19/Guias-y-Protocolos/Guia-para-la-celebracion-de-actuaciones-judiciales-telematicas>

LYONS, T., COURCELAS, I., y TIMSIT, K. «Blockchain y RGPD». Observatorio y Foro Blockchain de la UE, 2018. Disponible en: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Legislación citada

Normativa internacional

Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de las Comunidades Europeas*, 11 de diciembre de 2000. Disponible en:

Directiva 2016/680/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. *Diario Oficial de la Unión Europea*, 4 de mayo de 2016. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES>
http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *Diario Oficial de las Comunidades Europeas*, 4 de mayo de 2016, núm. 119. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (Texto pertinente a efectos del EEE.). *Diario Oficial de las Comunidades Europeas*, 21 de noviembre de 2018, núm. 295. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1725&from=ES>

Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión. *Diario Oficial de las Comunidades Europeas*, 7 de diciembre de 2018, núm. 312. Versión consolidada al 8 de marzo de 2021. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1862&from=EN>

Tratado de Funcionamiento de la Unión Europea, firmado en Lisboa el 13 de diciembre de 2007. *Diario Oficial de las Comunidades Europeas*, 17 de diciembre de 2007, pp. 1-344.

Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=es>

Normativa nacional

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. *Boletín Oficial del Estado*, 8 de enero de 2000, núm. 7. Disponible en: <https://www.boe.es/eli/es/l/2000/01/07/1/con>

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. *Boletín Oficial del Estado*, 6 de julio de 2011, núm. 160. Disponible en: <https://www.boe.es/eli/es/l/2011/07/05/18/con>

Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia. *Boletín Oficial del Estado*, 19 de septiembre de 2020, núm. 250. Disponible en: <https://www.boe.es/eli/es/l/2020/09/18/3/con>

Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. *Boletín Oficial del Estado*, 6 de octubre de 2015, núm. 239, pp. 90240 a 90288 Disponible en: <https://www.boe.es/eli/es/l/2015/10/05/42>

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294. Disponible en: <https://www.boe.es/eli/es/lo/2018/12/05/3>

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *Boletín Oficial del Estado*, 2 de julio de 1985, núm. 157. Última actualización a 29 de junio de 2022. Disponible en: <https://www.boe.es/eli/es/lo/1985/07/01/6/con>

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. *Boletín Oficial del Estado*, 27 de mayo de 2021, núm. 126. Disponible en: <https://www.boe.es/eli/es/lo/2021/05/26/7/con>

Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET. *Boletín Oficial del Estado*, 1 de diciembre de 2015, núm. 287. Disponible en: <https://www.boe.es/eli/es/rd/2015/11/27/1065/con>

Real Decreto 1184/2006, de 13 de octubre, por el que se regula la estructura, composición y funciones de la Comisión Nacional de Estadística Judicial. *Boletín Oficial del Estado*, 31 de octubre de 2006, núm. 260. Disponible en: <https://www.boe.es/eli/es/rd/2006/10/13/1184>

Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica. *Boletín Oficial del Estado*, 19 de junio de 2013, núm. 146. Disponible en: <https://www.boe.es/eli/es/rd/2013/06/07/396>

Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos. *Boletín Oficial del Estado*, 13 de febrero de 2007, núm. 38. Disponible en: <https://www.boe.es/eli/es/rd/2007/01/26/84>

Real Decreto 937/2003, de 18 de julio, de modernización de los archivos judiciales. *Boletín Oficial del Estado*, 30 de julio de 2003, núm. 181. Disponible en: <https://www.boe.es/eli/es/rd/2003/07/18/937/con>

Real Decreto-ley 16/2020, de 28 de abril, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia. *Boletín Oficial del Estado*, 29 de abril de 2020, núm. 119. Disponible en: <https://www.boe.es/eli/es/rdl/2020/04/28/16/con>

Jurisprudencia referenciada

Sentencia del Tribunal Constitucional Español 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, de 4 de enero de 2001, núm. 4. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332>

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos

CDFUE: Carta de Derechos Fundamentales de la Unión Europea

CE: Constitución Española

CENDOJ: Centro de Documentación Judicial

CGPJ: Consejo General del Poder Judicial

GAJT: Guía para la celebración de actuaciones judiciales telemáticas

IA: Inteligencia Artificial

LECiv: Ley de Enjuiciamiento Civil

LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales

LOPJ: Ley Orgánica del Poder Judicial

RGPD: Reglamento General de Protección de Datos

TFUE: Tratado de Funcionamiento de la Unión Europea

TIC: Tecnologías de la Información y la Comunicación

UE: Unión Europea