



Tercera época

Revista editada por Ilustre Colegio Nacional

ACTA JUDICIAL

de Letrados de la Administración de Justicia

N.º 10. Julio-Diciembre 2022

<http://www.letradosdejustizia.es/revistaactajudicial>

Sumario

	Págs.
HACIA UNA REGULACIÓN INTEGRAL DE LA MEDIACIÓN PENAL Por Estefanía Navarrete Corral	03-19
INCORPORACIÓN DE LOS WHATSAPP Y OTRAS APLICACIONES SEMEJANTES DE MENSAJERÍA ELECTRÓNICA AL PROCESO PENAL EN LA FASE DE INSTRUCCIÓN Por Alfredo Martínez Guerrero	20-36
LOS PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL Y SUS IMPLICACIONES EN EL PROCESO PENAL Por Juan Alejandro Montoro Sánchez	37-73

Licencia de las obras Pág. 74
Consejo editorial y Comité científico Pág. 75
Normas de publicación Pág. 76

Págs.

Edición semestral

ISSN 2603-7173

Editado en Madrid
(España)

por

Ilustre Colegio
Nacional de Letrados
de la Administración
de Justicia

HACIA UNA REGULACIÓN INTEGRAL DE LA MEDIACIÓN PENAL

Towards a comprehensive regulation of criminal mediation

Por Estefanía Navarrete Corral

Profesora de Derecho Penal. Universidad Pablo de Olavide
enavcor@upo.es

Artículo recibido: 01/12/21 | Artículo aceptado: 27/01/22

RESUMEN

El presente artículo anticipa los principales retos que se plantean respecto de una necesaria y futura regulación integral de desarrollo del procedimiento de mediación penal. La configuración del acceso o eventual derivación a los servicios de mediación penal debe entenderse desde la insuficiente regulación prevista en el art. 15 de la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito. Misma identidad de razón respecto del desarrollo de las sesiones de mediación penal y la propia delimitación de los principios aplicables que presentan unos caracteres propios diferenciables respecto de lo previsto en materia de mediación civil y mercantil. Lo anterior, además, debe armonizarse con las previsiones normativas que puedan resultar aplicables tanto en materia penal como procesal penal.

ABSTRACT

This article anticipates the main challenges that may be faced by a necessary and future comprehensive regulation of development of the criminal mediation procedure. The configuration of the access or eventual referral to the criminal mediation services must be understood from the insufficient regulation provided by article 15 of Law 4/2015, of April 27, of the Statute of the victim of the crime. Same identity of reason with respect to the development of the criminal mediation sessions and the delimitation of the applicable principles. The above, in addition, must be harmonized with the regulatory provisions that may be applicable both in criminal and criminal procedural matters.

PALABRAS CLAVE

Mediación, Penal, Principios, Derivación, Acceso, Procedimiento, Acuerdo, Medial.

KEYWORDS

Mediation, Criminal, Principles, Derivation, Procedure, Access, Agreement, Medial.

Sumario: 1. Introducción. 2. La insuficiente previsión normativa de los servicios de Justicia Restaurativa. 3. El acceso a los servicios de mediación. Desarrollo de las sesiones de mediación. 5. La derivación a los servicios de justicia restaurativa. 6. Los principios de actuación aplicables en el procedimiento de mediación penal. 7. Conclusiones. 8. Bibliografía.

1. Introducción

La mediación puede definirse, siguiendo a BARONA VILAR¹, como “un procedimiento extrajudicial, en virtud del cual víctima e infractor, voluntariamente, se reconocen capacidad para participar en la resolución de su conflicto penal, que existe, con intervención de un tercero, al que llamamos mediador, reestableciendo la situación previa al delito y el respeto al ordenamiento jurídico, amén de dar satisfacción a la víctima y el reconocimiento de tal actividad por el victimario”. Asimismo, para GONZÁLEZ CANO², se trataría de un “sistema de gestión de conflictos, aquel en el que una parte neutral, con carácter técnico y en posesión de conocimientos adecuados, independiente de los actores institucionales del proceso penal, e imparcial, ayuda a dos o más personas implicadas en un delito o falta, en calidad de víctima e infractor, a comprender el origen del conflicto, sus causas y consecuencias, a confrontar sus puntos de vista ya a elaborar acuerdos sobre el modo de reparación, tanto material como simbólica”.

Por tanto, la solución al conflicto se produce por el acuerdo voluntario e informado de las partes, mediando la intervención no vinculante de un tercero en la conformación de dicho acuerdo.

No obstante, las específicas circunstancias que plantea tanto la producción como la eventual composición del conflicto penal favorecen la delimitación de parámetros propios de la mediación penal y, en cierta medida, diferenciables, en comparación con otros modelos de mediación que se proponen en el ámbito de las relaciones privadas, particularmente en lo que respecta a la mediación en los ámbitos civil y mercantil.

¹ BARONA VILAR, S., *Mediación penal: fundamento, fines y régimen jurídico*, Tirant lo Blanch, Valencia, 2011, pp. 257 a 318.

² GÓNZALEZ CANO, I., «La mediación penal en España», en *La mediación penal para adultos una realidad en los ordenamientos jurídicos: (experiencia en España, EEUU, Inglaterra y Gales, Países Escandinavos, Francia, Alemania, Portugal, Brasil y Chile)*, Tirant lo Blanch, Valencia, 2017, p. 25.

Como refiere SÁNCHEZ GÓMEZ³, “en la materia procesal penal que nos ocupa, el conflicto presenta entonces una vertiente intersubjetiva y una vertiente social. La primera de estas hace referencia al conflicto que se plantea entre víctima y victimario, cuya composición tendrá un contenido y unos límites específicos. En el ordenamiento jurídico español, la vertiente intersubjetiva del conflicto encuentra su acomodo en las propias leyes de enjuiciamiento criminal, al disponerse el instituto de la acusación no oficial, es decir, mediante el ejercicio de la acusación particular, ejercitada por la propia víctima o quien legítimamente ocupe tal posición, y la acción popular, en defensa de los intereses generales. De otro lado, la vertiente social del conflicto refiere la existencia de una controversia entre el victimario y la propia Sociedad, interesada en la prevención y represión de los delitos. Ambas vertientes, intersubjetiva y social, han de vincular la composición del conflicto”⁴.

Asimismo, las consecuencias del acuerdo alcanzado entre las partes y su posterior eficacia procesal en el ámbito de la mediación penal distan mucho de la realidad de la ejecución de los acuerdos mediales en la composición del conflicto concreto que se somete al procedimiento de mediación civil o mercantil.

Entre las razones que informan tales argumentos es posible ahora afirmar, la naturaleza de los derechos que se ventilan en un proceso penal, la posición de las partes, principalmente respecto del sostenimiento de las pretensiones acusadoras y los propios efectos procesales que se derivan del acuerdo de mediación en cuanto a la determinación de la eventual pena que pudiera acordarse en la sentencia.

Como se dijo, el pretendido impulso legislativo propuesto respecto de la mediación⁵, tampoco ha conseguido alcanzar las deseadas cotas de implementación de los servicios de mediación en el plano penal. La consideración de la Estadística judicial publicada por el Consejo General del Poder Judicial es un claro ejemplo al respecto.

A tal fin, llama poderosamente la atención cómo las razones expuestas en la Exposición de Motivos del propio Anteproyecto de Ley de Impulso de la Mediación para justificar la falta de éxito en la implementación del procedimiento de mediación en materia civil y mercantil resultan también

³ SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, Tirant lo Blanch, Valencia, 2017, pp. 1153 y ss.

⁴ Véase GIMENO SENDRA, V., *Fundamentos de Derecho Procesal (jurisdicción, acción y proceso)*, Civitas, Madrid, 1981, pág. 21.

⁵ Al menos respecto del Anteproyecto de Ley de Impulso de la Mediación, mientras que, respecto del Anteproyecto de Ley de Medidas de Eficiencia Procesal del Servicio Público de Justicia, aun estar por ver.

trasladables al ámbito de la mediación penal. Entre estas, destaca la falta de una «cultura» de la mediación en los Estados miembros, conforme el Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre la aplicación de la Directiva 2008/52/CE, de 26 de agosto de 2016.

No obstante, no es posible compartir plenamente tales argumentos, debiendo situar al mismo nivel tanto la referida falta de cultura como la ausencia, precisamente, del suficiente impulso estatal para consolidar unos servicios de mediación, con independencia de su naturaleza, en directa conexión con la propia Administración de Justicia⁶.

Suficiencia en el pretendido impulso que debería acompañarse de un inicial y adecuado respaldo presupuestario, la definitiva incorporación orgánica de los servicios de mediación, si se quiere en el marco de la propia Oficina Judicial o su encaje en las diferentes Leyes de Enjuiciamiento.

En efecto, como se puso de relieve, los servicios de mediación sean de naturaleza pública o privada, no han calado como habría sido deseable en el conjunto de la ciudadanía a la hora de decidir la fórmula más adecuada para la resolución de sus derechos subjetivos, de naturaleza disponible. Tampoco se ha producido, en el concreto supuesto que nos ocupa, una consolidación efectiva de la oferta institucional de composición pública de conflictos efectiva, más allá de los tradicionales contornos del proceso jurisdiccional.

2. La insuficiente previsión normativa de los servicios de Justicia Restaurativa

El art. 15 Ley 4/2015, de 27 de abril, del estatuto de la víctima del delito (en adelante LEVD⁷), regula parcamente cómo deberán articularse los servicios de mediación penal, entendemos que, en el marco de la Administración de Justicia, mediante la creación de las Oficinas de Justicia Restaurativa, del siguiente tenor:

1. Las víctimas podrán acceder a servicios de justicia restaurativa, en los términos que reglamentariamente se determinen, con la finalidad de obtener una adecuada reparación material y moral de los perjuicios derivados del delito, cuando se cumplan los siguientes requisitos:

⁶ En similares términos, véase SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, referencia 3, págs. 1153 y ss.

⁷ La citada normativa trae causa en la transposición al ordenamiento jurídico español del contenido de la Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y por la que se sustituye la Decisión Marco 2001/220/JAI del Consejo.

- a) el infractor haya reconocido los hechos esenciales de los que deriva su responsabilidad;*
- b) la víctima haya prestado su consentimiento, después de haber recibido información exhaustiva e imparcial sobre su contenido, sus posibles resultados y los procedimientos existentes para hacer efectivo su cumplimiento;*
- c) el infractor haya prestado su consentimiento;*
- d) el procedimiento de mediación no entrañe un riesgo para la seguridad de la víctima, ni exista el peligro de que su desarrollo pueda causar nuevos perjuicios materiales o morales para la víctima; y*
- e) no esté prohibida por la ley para el delito cometido.*

2. Los debates desarrollados dentro del procedimiento de mediación serán confidenciales y no podrán ser difundidos sin el consentimiento de ambas partes. Los mediadores y otros profesionales que participen en el procedimiento de mediación estarán sujetos a secreto profesional con relación a los hechos y manifestaciones de que hubieran tenido conocimiento en el ejercicio de su función.

3. La víctima y el infractor podrán revocar su consentimiento para participar en el procedimiento de mediación en cualquier momento.

La insuficiencia del contenido del precepto para poder articular tales servicios de Justicia Restaurativa es notoria.

El ámbito de aplicación del procedimiento de mediación se plantea de manera negativa, por referencia a aquellas materias expresamente prohibidas en el ordenamiento jurídico, como, por ejemplo, lo previsto en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, en la modificación propuesta respecto del art. 87 ter de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial⁸.

Por tanto, es posible afirmar que allí donde no exista expresa prohibición normativa al respecto podrá proponerse someter el conflicto penal al procedimiento de mediación, limitándose la norma a afirmar que su finalidad radica en la obtención de una adecuada reparación material y moral de los perjuicios derivados del delito.

Sin embargo, como sostiene BARONA VILAR⁹, la mediación penal “puede centrarse en la reparación, y por eso se habla de justicia reparadora (entendiendo reparación tanto la moral como la económica, empero también la simbólica), y también se ha extendido a lo que, especialmente en ciertos ámbitos

⁸ Crítico con la prohibición absoluta se muestra SÁNCHEZ GÓMEZ R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, referencia 3, pp. 1153 a 1163 y la doctrina científica allí citada.

⁹ BARONA VILAR, S., «Mediación y acuerdos reparatorios en la metamorfósica justicia penal del siglo XXI», en *Boletín Mexicano de derecho comparado*, 2020, Vol. 1, núm. 155, pp. 698 y 699.

(políticos y complejos) se ha denominado «justicia reconstructiva»; en esta última, existe un objetivo esencial: alcanzar la paz social”.

La finalidad de la mediación penal trasciende, entonces, el mero conflictivo intersubjetivo en que la propia víctima también es parte.

La limitada finalidad propuesta permite afirmar una posición parcial de partida donde se atiende alguno de los parámetros que puede perseguir la víctima cuando decide, voluntariamente, acudir a un procedimiento de mediación.

En efecto, la reparación puede ser un medio de pacificar el conflicto porque permite aliviar la tensión emocional de la víctima, prevenir la reiteración de hechos violentos similares y lograr, en su caso, el desapasionamiento del agresor hacia su víctima. Y ello porque atiende a dos dimensiones fundamentales: la reparación psicológica y material de la víctima y la responsabilización del autor¹⁰.

A tal fin, la Guía para la práctica de la mediación intrajudicial del Consejo General del Poder Judicial pone de relieve las ventajas que proporcionaría la conformación de unos servicios (públicos) de mediación en el ámbito penal:

Para la víctima: le hace participar activamente y de forma voluntaria en la resolución del conflicto que le afecta. Le permite ser reparada por los daños y perjuicios tanto morales como materiales sufridos y la recuperación de la tranquilidad personal.

Para el encausado: le facilita la concienciación y el responsabilizarse de las propias acciones y consecuencias, así como la posibilidad de entender el delito y obtener beneficios previstos en el Código Penal.

Para la justicia: le proporciona una nueva concepción, nuevas formas de respuesta penal con sentido educativo, promoviendo actitudes hacia la responsabilización y la reparación.

Para la sociedad: le da a conocer otras formas de reacción de la justicia, acercando la justicia a los ciudadanos; puede facilitar una disminución de la conflictividad social.

¹⁰ SAÉZ VALCARCEL, J., «La mediación penal, una metodología judicial para ocuparse de la reparación y de la resocialización», en Boletín del Ministerio de Justicia, 2008, Año 62, núm. 2060, pág. 1763. Asimismo, el propio Consejo General del Poder Judicial propone los siguientes fines respecto de los servicios de mediación: asegurar una efectiva protección a la víctima mediante la reparación o disminución del daño causado por el delito. Si no existe víctima, la reparación podrá tener carácter simbólico ante la comunidad social; responsabilizar al infractor sobre las consecuencias de su infracción; puede atenuar la pena; procurar medios para la normalización de su vida; restablecer la convivencia y el diálogo comunitario; devolver protagonismo a la sociedad civil; conocer las causas reales y las consecuencias del conflicto, buscando la fórmula más idónea para satisfacer las necesidades personales de víctima e infractor.

De otro lado, especialmente significativas resultan la ausencia de una específica regulación que delimite el estatuto básico del mediador, con competencias en materia penal. En tal sentido refiere BARONA VILAR¹¹, entre otras cuestiones, “sobre la necesaria configuración del estatuto básico del mediador que opera en el ámbito penal mediante el desarrollo de un estatuto del mediador y su correspondiente actividad de control, a través de la formación de este nuevo sector profesional, que debe capacitarse para el desempeño de esta función en el marco del sistema punitivo; y asimismo, la necesidad de establecer garantías al ejercicio de esta función, a través de registros, asociaciones profesionales, etc”.

Así mismo, resulta necesario delimitar las normas aplicables al procedimiento de mediación penal o la eficacia procesal que dispondrán los acuerdos mediación en sede ejecución¹².

Como refiere la autora es imprescindible conectar la mediación con el proceso penal, de manera que, además de regular en la ley sobre mediación el acuerdo que se alcance y la posible eficacia jurídica del mismo, debe incorporarse a la LECrim alguna norma que permita:

a) la regulación de la posible suspensión del proceso, sea cual sea la fase en la que se encuentre, con el fin de remitir a la víctima y al victimario al procedimiento de mediación, fijando, en su caso, un plazo máximo de suspensión del mismo, lo que conectará con una posible norma en la ley de mediación que regula la duración máxima del mencionado procedimiento. Todo ello sin perjuicio de posibles prórrogas cuando concurren circunstancias que lo justifiquen.

b) los momentos en que la mediación puede llevarse a cabo pendiente una causa penal. No se trata de que exista una norma que en la LECrim haga referencia a esta posibilidad, dado que se trata esta más bien de una norma que se recoja en la ley de mediación, sino de la regulación específica de la eficacia jurídica procesal de la mediación vinculada a la fase de investigación, a la fase de juicio oral y, en su caso, a la fase de ejecución penal.

c) En la fase de investigación parece que se darán las situaciones más comunes para derivar a mediación, máxime cuando se está en la fase incipiente

¹¹ BARONA VILAR, S., *Mediación penal: fundamento, fines y régimen jurídico*, referencia 9. cit., pp. 148 y 152.

¹² Sobre la aplicabilidad de los arts. 21.5 CP, sobre la atenuante de reparación del daño, o los arts. 80 y 84 sobre la suspensión de la penal mediando la concurrencia de un acuerdo mediación, y su relación a efectos de conformidad puede consultarse BARONA VILAR, S., *Mediación penal: fundamento, fines y régimen jurídico*, referencia 9, pp. 250 Y 251 y SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, referencia 3, pp. 1162 a 1163.

del proceso. Evidentemente no existe duda alguna de que si con la mediación se alcanza un acuerdo que evita la continuación del proceso, esta es la fase más eficiente para la misma.

Por el contrario, todas estas materias se encuentran firmemente positivizadas en la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles (en adelante LMACM), y su correspondiente desarrollo normativo previsto en el Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles que regula, a grandes rasgos, las relaciones de los profesionales de la mediación y la aplicación de medios electrónicos al procedimiento de mediación.

Por todo lo anterior, sería necesario entonces proponer la tan ansiada normativa de desarrollo del precepto analizado donde se regulen, entre otras, las materias comentadas, más aún, si tenemos en cuenta que las normas que disciplinan la mediación en asuntos civiles y mercantiles expresamente prohíben su aplicación a la mediación que pudiera sucederse en materia penal (art. 2 LMACM), por lo que su inicial aplicación supletoria puede plantear serias dudas al respecto.

3. El acceso a los servicios de mediación

La escueta referencia a cómo debe producirse el acceso a los servicios de Justicia Restaurativa prevista en el citado art. 15 LEVD se centra, en buena lógica, en la posición de la víctima, apostando precisamente por la reparación del conflicto intersubjetivo existente entre víctima y victimario.

Como se dijo, la finalidad de acceso al servicio se residencia en la obtención de una adecuada reparación material y moral de los perjuicios derivados del delito.

Ello abre el debate sobre si es posible introducir pretensiones acusatorias por parte de la víctima o su eventual representación procesal en el marco de las sesiones de mediación penal.

A diferencia de la norma procesal de referencia, Ley de Enjuiciamiento Criminal, que se articula mayoritariamente en torno a la figura del sujeto pasivo del proceso penal, los servicios de Justicia Restaurativa previsto en la LEVD, y la propia norma en su conjunto, se configuran en torno a la víctima.

Ello permite entender las escasas referencias normativas existentes tanto respecto de la intervención del victimario en las sesiones de mediación penal como respecto de los propios efectos procesales que podrían sucederse con un eventual acuerdo medial.

Por tanto, es posible sostener, vistos además los requisitos que informan la conformación inicial del procedimiento de mediación penal, que la intención subyacente en la propuesta normativa de mínimos que plantea el precepto, se

correspondería con una composición no estrictamente jurídica del conflicto penal intersubjetivo existente entre víctima y victimario.

Tales extremos deberán entonces valorarse en el propio proceso jurisdiccional que conozca de la causa, teniendo presente los resultados del acuerdo mediador que pudiera haberse alcanzado, a los efectos, precisamente, de determinar las consecuencias jurídicas que se derivarían del hecho delictivo sometido a enjuiciamiento.

A mayor abundamiento, la indicación de que el acceso a los servicios de justicia restaurativa por parte de las víctimas se regulará en un futuro reglamento, del que siete años después aún no se tienen noticias, permite afianzar los argumentos planteados.

Seguidamente, se plantean dos requisitos de procedibilidad respecto del acceso de la víctima al procedimiento de mediación, vista la finalidad descrita respecto de la obtención de una adecuada reparación material y moral de los perjuicios derivados del delito.

En primer lugar, se reconoce el libre acceso y permanencia de la víctima en el procedimiento de mediación, debiendo prestar su consentimiento al respecto para el acceso, pudiendo revocarlo en cualquier momento del desarrollo de las actuaciones. La libertad de permanencia es absoluta no estando obligada, ni víctima ni infractor, a justificar las razones que fundamentan su negativa a iniciar o proseguir un procedimiento de mediación.

Dicho consentimiento debe prestarse de manera informada, tanto con carácter previo al inicio del procedimiento de mediación, como al inicio de las actuaciones, en la denominada sesión informativa, donde el mediador debe poner de relieve los principios aplicables al procedimiento informando a las partes sobre las condiciones y el modo en que van a desarrollarse las diferentes sesiones y los correspondientes debates.

Asimismo, se requiere que dicha información previa sea exhaustiva e imparcial, refiriendo de una manera innecesariamente anticipada los posibles resultados que pudieran alcanzarse y los procedimientos existentes para hacer efectivo el cumplimiento de un eventual acuerdo mediador.

En segundo lugar, como se puso de manifiesto, se supedita el recurso a la justicia restaurativa a que el procedimiento de mediación no entrañe un riesgo para la seguridad de la víctima, ni exista el peligro de que su desarrollo pueda causar nuevos perjuicios materiales o morales para la víctima.

La competencia para valorar tales riesgos lógicamente se reside en la propia Oficina de Asistencia a las Víctimas, atendidas las resultados de la investigación gubernativa y judicial en curso.

No obstante, la introducción del elemento prospectivo en la denegación de justicia restaurativa, desde la perspectiva tanto de un posible perjuicio material como moral para la víctima, supone introducir un criterio casuístico

más allá de una enumeración exhaustiva de los conflictos penales susceptibles de composición mediante fórmulas autocompositivas.

En dicho enfoque, la delimitación predictiva realizada por tercero respecto de la concurrencia de un posible perjuicio moral puede situarse razonablemente en la esfera intersubjetiva del conflicto penal¹³.

Sin embargo, respecto cómo deberá producirse el acceso del victimario a los servicios de mediación tan solo se recogen dos requisitos de procedibilidad que informarían la apertura del procedimiento de mediación y su eventual continuación.

En primer lugar, el infractor ha de reconocer los hechos esenciales de los que se deriva su responsabilidad, lógicamente, de naturaleza penal pero no circunscrita exclusivamente a dicho ámbito.

Ello podría generar serias disfunciones en sus derechos procesales en los supuestos que el procedimiento de mediación cesase sin éxito, debiendo abrirse el correspondiente proceso penal sin acuerdo medial.

La alegación de una previa asunción de responsabilidad penal por parte del victimario en el procedimiento de mediación o la simple comunicación en sede judicial de que el procedimiento se inició, siendo requisito de procedibilidad dicho previo reconocimiento, puede situar al victimario ante una complicada situación procesal que afecte, entre otros, su derecho a la presunción de inocencia.

En tal sentido, como refiere BARONA VILAR¹⁴, “la confidencialidad y el secreto a que se someten los sujetos que intervienen en el procedimiento de mediación, plasmado en el inicial del procedimiento de mediación, tras conocer el significado de la misma y sus posibles efectos jurídicos, debería implicar la asunción, con firma de los participantes, de que en modo alguno está aceptando culpabilidad el sujeto posible infractor. Esto sobre todo debe garantizarse para los supuestos en los que no se llega a un acuerdo y se produce la incorporación en el proceso penal de los sujetos que intervinieron en el procedimiento de mediación; no es posible a estos efectos que “lo” afirmado en mediación pueda tener naturaleza inculpativa, lo que se garantiza mediante la imposibilidad de trasvasar el contenido de la mediación al proceso penal. En la ley de mediación debiera por tanto impedirse, en garantía del derecho a la presunción de inocencia, que el documento generado en mediación se incorpore como prueba al proceso penal, so pena de incurrir en responsabilidad. Y debe quedar

¹³ Sobre el desarrollo de las vertientes intersubjetiva y social presentes en la conformación del conflicto penal puede consultarse SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, referencia 3, pp. 1153 y ss.

¹⁴ BARONA VILAR, S., *Mediación penal: fundamento, fines y régimen jurídico*, referencia 9, p. 248.

asimismo en la ley de mediación garantizada la imposibilidad de que el mediador sea llamado como testigo o perito al proceso”.

En segundo lugar, se interesa que el infractor haya prestado su consentimiento para la celebración del procedimiento de mediación, lo que en conexión con el desarrollo de los principios fundamentales que informan el modelo autocompositivo, permite afirmar la naturaleza libre y voluntaria de sometimiento al procedimiento de mediación, tanto por parte de la víctima como del victimario.

Por último, parece que el acceso informado al procedimiento de mediación solo será predicable respecto de la propia víctima, debiendo hacerse extensible también al victimario pues la propia dinámica de las actuaciones mediales así lo requiere.

El acceso informado del victimario al procedimiento de mediación no debe descansar en su representación letrada, por más que al inicio de las sesiones el mediador deba informar sobre tales aspectos de manera detallada.

4. Desarrollo de las sesiones de mediación

El apartado segundo del precepto objeto de análisis plantea la articulación del principio de confidencialidad en el desarrollo de los debates que componen el procedimiento de mediación.

De esta forma, la regla general informa la naturaleza confidencial de los debates desarrollados, y por ende, no podrán ser objeto de difusión sin el previo consentimiento de ambas partes.

Así, al inicio del procedimiento, más concretamente en la sesión informativa, el mediador pondrá de manifiesto dicha naturaleza confidencial respecto de los pormenores que se sucedan en el procedimiento de mediación, si bien, resultaría preferible trasladar la confidencialidad y prohibición de difusión respecto del procedimiento de mediación en su conjunto y no solo respecto de los debates que se sucedan.

La naturaleza confidencial del procedimiento de mediación puede ser excepcionada por expresa acuerdo entre las partes, siendo preferible que el mediador documente tales extremos en la correspondiente acta.

Lógica consecuencia de la naturaleza confidencial del procedimiento de mediación resulta en la afirmación de que la actuación de los mediadores y demás profesiones que participen en el procedimiento de mediación estarán sometidas a secreto profesional en relación tanto con los hechos como las manifestaciones de que hubieran tenido conocimiento en el ejercicio de sus funciones.

Esta parca regulación nos obliga a transponer el contenido de algunos preceptos de la Ley de Enjuiciamiento Criminal, principalmente respecto de la

genérica obligación de denunciar y la posibilidad de eximir la declaración como testigo de según que personas o profesionales.

Sin embargo, la aplicabilidad de los diferentes regímenes que plantea la Ley de Enjuiciamiento Criminal dependerá en gran medida de la naturaleza pública o privada de los servicios de mediación penal, cuestión que en materia penal parece resolverse a favor de la configuración de unos servicios públicos, aunque pudieran estar servidos por entidades privadas.

El primer supuesto de hecho que se plantea es asumible pueda concurrir en la praxis forense, es decir, en el desarrollo de los debates el mediador tiene constancia de la posible comisión de nuevos hechos delictivos.

A tal fin, el art. 262 LECrim regula la obligación de denuncia inmediata de aquellos que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, planteando además la eventual responsabilidad que la falta de cumplimiento de dicha obligación pueda generar en el orden administrativo.

Ahora bien, el art. 263 LECrim excepciona a los Abogados y Procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes. Tampoco vincula dicha obligación a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio.

No parece que el mediador pueda equipararse con las excepciones comentadas, debiendo resultar de aplicación la regla general que informa la obligación de denunciar los nuevos hechos delictivos de que tuviera conocimiento en el marco del procedimiento de mediación, a pesar de las consecuencias que ello pueda generar para con las actuaciones mediales.

En el segundo supuesto, el art. 416 LECrim establece la excepción de prestar testimonio del abogado defensor respecto a los hechos que éste le hubiese confiado en su calidad de defensor, así como respecto de los traductores e intérpretes de las conversaciones y comunicaciones mantenidas en el marco de la preparación de la defensa y en relación con los hechos a que estuviera referida su traducción o interpretación. Refuerza dicha excepción el art. 417 LECrim cuando dispone que no podrán ser obligados a declarar como testigos:

1.º Los eclesiásticos y ministros de los cultos disidentes, sobre los hechos que les fueren revelados en el ejercicio de las funciones de su ministerio.

2.º Los funcionarios públicos, tanto civiles como militares, de cualquiera clase que sean, cuando no pudieren declarar sin violar el secreto que por razón de sus cargos estuviesen obligados a guardar, o cuando, procediendo en virtud de obediencia debida, no fueren autorizados por su superior jerárquico para prestar declaración que se les pida.

3.º Los incapacitados física o moralmente.

Como puede apreciarse la materia testifical, sin embargo, difiere de lo argumentado en el primero de los supuestos visto el reconocimiento explícito que realiza la norma comentada respecto del reconocimiento del secreto profesional que vincula al mediador en lo que se refiere a los hechos y manifestaciones de que hubiera tenido conocimiento en el ejercicio de su función. En otras palabras, el mediador dispondrá de la debida confidencialidad respecto de las actuaciones mediales y en función del objeto que informa el procedimiento de mediación, hasta ahí su alcance, si bien, sobrevenidos nuevos hechos delictivos de los que se tiene conocimiento en el propio procedimiento de mediación, el mediador no se encuentra entre las excepciones previstas en la norma procesal respecto de la obligación de denunciar, aunque sería preferible que dispusiera de un margen de actuación más flexible al respecto.

Por su parte, el art. 9 LMACM establece los estándares de confidencialidad aplicables a la mediación civil y mercantil desde una óptica quizás más amplia que lo previsto respecto de la mediación penal al establecer la reserva tanto del propio procedimiento de mediación como de la documentación utilizada.

Dicha obligación de confidencialidad se extiende al mediador, que quedará protegido por el secreto profesional, a las instituciones de mediación y a las partes intervinientes de modo que no podrán revelar la información que hubieran podido obtener derivada del procedimiento.

Consecuencia de dicho reconocimiento inicial, los mediadores o las personas que participen en el procedimiento de mediación no están obligados a declarar o aportar documentación en un procedimiento judicial o en un arbitraje sobre la información y documentación derivada de un procedimiento de mediación o relacionada con el mismo.

Dicha regla general, admite las siguientes excepciones:

- a) Cuando las partes de manera expresa y por escrito les dispensen del deber de confidencialidad.
- b) Cuando, mediante resolución judicial motivada, sea solicitada por los jueces del orden jurisdiccional penal.

Por ende, es posible afirmar las diferencias existentes entre el desarrollo del principio de confidencialidad, particularmente en materia testifical, según nos situemos en la órbita de la mediación civil, mercantil o penal.

5. La derivación a los servicios de justicia restaurativa

El procedimiento de mediación en materia civil y mercantil admite la posibilidad de disponer de ámbitos de actuación diferenciados en lógica conexión con la naturaleza de los conflictos y derechos subjetivos que se plantean.

A grandes rasgos, el procedimiento de mediación puede producirse en varias instancias.

Una primera instancia preprocesal, es decir, el procedimiento de mediación se sucede con anterioridad al ejercicio de cualquier acción judicial, si bien, si se traduce en el correspondiente acuerdo medial entre las partes, quedará expedita la posibilidad de solicitar la ejecución de lo previamente acordado. Téngase presente la naturaleza de título ejecutivo que, generalmente, presentan los acuerdos mediales.

Una segunda instancia, que se produce de manera coetánea a la accionabilidad de las pretensiones en sede procesal.

Iniciado el proceso civil, las partes solicitan su suspensión para acudir a un procedimiento de mediación, en cualquier momento de la primera instancia o de los recursos o de la ejecución de sentencia (art. 19.3 de la Ley de Enjuiciamiento Civil). La solicitud de suspensión será acordada por el Letrado de la Administración de Justicia mediante decreto siempre que no perjudique al interés general o a tercero y que el plazo de la suspensión no supere los sesenta días (art. 19.4 de la Ley de Enjuiciamiento Civil). En tales supuestos, el procedimiento de mediación podrá celebrarse bien de manera extraprocesal, acudiendo a los servicios privados de una entidad de mediación, o bien, solicitando los servicios públicos de mediación, vinculados o no, a la Administración de Justicia, allí donde existan¹⁵.

Una tercera instancia, que también se produce una vez iniciado el proceso civil que corresponda, donde el procedimiento de mediación se inicia por voluntad de las partes, previa derivación judicial.

Una última instancia, precisamente, en ejecución de lo previamente resuelto, sea por acuerdo medial sea por decisión jurisdiccional.

Dicho esto, resultan notorias las sensibles diferencias que se plantean respecto del procedimiento de mediación en el ámbito penal y su desconexión con la propia Ley de Enjuiciamiento Criminal.

En efecto, las posibilidades de acudir a tales servicios podrán producirse bien por iniciativa de las partes bien por derivación de los diferentes operadores jurídicos pertenecientes a la Administración de Justicia. Incluso por las propias Fuerzas y Cuerpos de Seguridad con competencias en la materia.

Como refiere el Protocolo de funcionamiento del servicio de mediación intrajudicial de la Dirección de Justicia, Departamento de Justicia y Administración Pública, del Gobierno Vasco, en principio no existe limitación en cuanto al órgano jurisdiccional con posibilidad de derivación, salvo los

¹⁵ Por ejemplo, en la provincia de Sevilla, tales servicios públicos de mediación se ofrecen, en determinados supuestos, desde el área de cohesión social de la Diputación de Sevilla.

expresamente prohibidos (asuntos que traen origen en Violencia contra la Mujer), por lo que cabe la remisión desde todos los órganos de la jurisdicción penal, tanto unipersonales –Juzgados de Instrucción (incluidos los Juzgados Mixtos) y Juzgados de lo Penal– como colegiados –Audiencias Provinciales–. Tampoco está limitado a priori el momento procesal en el que pueden derivarse los asuntos a los servicios de mediación, siempre que se estime oportuno conforme a los criterios anteriormente enunciados.

6. Los principios de actuación aplicables al procedimiento de mediación penal

A continuación, se describen los principios específicos del procedimiento de mediación penal desde la lógica perspectiva de su naturaleza voluntaria y confidencial, incorporando unos estándares concretos respecto de la articulación del secreto profesional. El precepto no incorpora algunos de los regulados en la Ley 5/2012, de mediación en asuntos civiles y mercantiles, limitándose a afirmar la concurrencia de los citados anteriormente.

Como se dijo, la naturaleza voluntaria de participación en el procedimiento de mediación se hace depender, entonces, del consentimiento informado de la víctima. No así respecto del victimario, que meramente podrá prestar su consentimiento al respecto. En ambos supuestos, el consentimiento para participar en el procedimiento de mediación podrá ser revocado en cualquier momento.

No se introducen, sin embargo, los parámetros contractuales del art. 6 LMACM previstos para aquellos supuestos en que exista un pacto por escrito que exprese el compromiso de someter a mediación las controversias surgidas o que puedan surgir, se deberá intentar el procedimiento pactado de buena fe, antes de acudir a la jurisdicción o a otra solución extrajudicial, en consonancia con la naturaleza generalmente pública del conflicto penal.

Respecto de la aplicación del principio de igualdad que debe regir el procedimiento de mediación, en cualesquiera de sus modalidades materiales, es necesario advertir su omisión expresa en el contenido del precepto comentado.

Las particulares circunstancias en que se desarrolla el conflicto penal, han provocado una tendencia a excluir, en según qué supuestos, el recurso al procedimiento de mediación, precisamente sobre la base de que no es posible garantizar la concurrencia del principio de igualdad entre las partes.

No obstante, es preciso advertir que, si la existencia de un conflicto penal puede implicar una posición desigual entre víctima y victimario, ninguna duda cabe que su composición en sede procesal se plantea desde la estricta aplicación

del principio de igualdad en cuanto a las posibilidades de alegación y prueba de las partes¹⁶.

Misma identidad de razón puede plantearse respecto del procedimiento de mediación. La regulación prevista en el art. 7 LMACM, precisamente, detalla la garantía de intervención de las partes en el procedimiento de mediación con plena igualdad de oportunidades, manteniendo el equilibrio entre sus posiciones y el respeto hacia los puntos de vista por ellas expresados, sin que el mediador pueda actuar en perjuicio o interés de cualquiera de ellas.

La igualdad en el procedimiento mediador también se garantiza en cuanto a las facultades de intervención equilibrada entre las partes y la debida imparcialidad de las personas mediadoras.

El art. 8 LMACM, regula precisamente la neutralidad que debe informar el procedimiento de mediación y, consecuentemente, la actuación de las personas mediadoras, conectándose con los criterios que deben regir su actuación, informada por la debida imparcialidad, establecidos en el art. 13 LMACM.

Respecto del principio de imparcialidad se prevé que el mediador antes de iniciar o de continuar su tarea, y durante todo el procedimiento de mediación, ponga de relieve cualquier circunstancia que pueda afectar a su imparcialidad o bien generar un conflicto de intereses. Tales circunstancias incluirán, en todo caso:

- a) Todo tipo de relación personal, contractual o empresarial con una de las partes.
- b) Cualquier interés directo o indirecto en el resultado de la mediación.
- c) Que el mediador, o un miembro de su empresa u organización, hayan actuado con anterioridad a favor de una o varias de las partes en cualquier circunstancia, con excepción de la mediación.

De esta forma, los subsiguientes principios que sí son objeto de regulación deben ser conectados, entre otros, con el de imparcialidad.

En efecto, como se ha puesto de relieve *ut supra*, la confidencialidad deberá predicarse respecto de los debates que se susciten dentro del procedimiento de mediación, pero también respecto de los hechos y

¹⁶ Crítico con tales planteamientos se muestra SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, referencia 3, pp. 1162 y 1163, para quien “el principio de igualdad en el proceso penal se garantiza disponiendo iguales medios de ataque y de defensa para las partes, desde la perspectiva que aporta la defensa de los derechos e intereses legítimos a través del juicio jurisdiccional. Más aún, dicha situación no necesariamente conlleva descartar la institución de la mediación penal, sino que la cuestión de fondo radicaría en fomentar un adecuado equilibrio entre las partes, para que voluntariamente, puedan someter la composición de su controversia a las tareas mediadoras, especialmente informadas por la confidencialidad de su práctica”.

manifestaciones de que hubieran tenido conocimiento las personas mediadoras, que se encuentran amparadas por el secreto profesional (art. 416 y 417 LECrim). Se exceptúa la posibilidad de que las partes presten ambas su consentimiento para poder revelar las informaciones que se suceden en el curso del procedimiento de mediación.

7. Conclusiones

Del tenor del texto principal caben destacar las siguientes conclusiones:

1. La falta de desarrollo normativo respecto del procedimiento de mediación previsto en el art. 15 LEVD puede generar una implementación desigual de los servicios y procedimientos aplicables.

2. La escueta finalidad propuesta respecto del acceso a los servicios de mediación debe ampliarse conforme los parámetros descritos.

3. Entre las principales ausencias normativas respecto del procedimiento de mediación penal destacan la ausencia de una específica regulación que delimite el estatuto básico del mediador, con competencias en materia penal, así como las normas aplicables al procedimiento de mediación penal o la eficacia procesal que dispondrán los acuerdos mediación en sede ejecución. Por tanto, vistas las citadas competencias de las Oficinas de Justicia Restaurativa, cómo se produce el acceso a tales servicios, así como el desarrollo de los principios que informan el procedimiento de mediación a seguir, es posible afirmar que tales servicios deberán estar servidos por mediadores públicos o cuya actuación sea retribuida con cargo a fondos públicos. Tales cuestiones, abrirían también el subsiguiente debate acerca de la idoneidad de los profesionales de la mediación en el ámbito penal y la ausencia de una regulación que establezca los parámetros habilitantes y formativos necesarios para el desarrollo de sus funciones profesionales como personas mediadoras, como por ejemplo si ocurre en materia civil y mercantil (art. 11 LMACM y arts. 3 a 7 del Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles).

4. Los principios aplicables al procedimiento de mediación penal presentan una configuración propia y diferenciable respecto de la regulación aplicable en materia de mediación civil y mercantil.

5. Una futura normativa de desarrollo respecto del procedimiento de mediación penal deberá armonizarse con las normas previstas en materia penal y procesal penal.

8. Bibliografía.

BARONA VILAR, S., *Mediación penal: fundamento, fines y régimen jurídico*, Tirant lo Blanch, Valencia, 2011.

BARONA VILAR, S., «Mediación y acuerdos reparatorios en la metamorfósica justicia penal del siglo XXI», en *Boletín Mexicano de derecho comparado*, 2020, Vol. 1, núm. 155.

GIMENO SENDRA, V., *Fundamentos de Derecho Procesal (jurisdicción, acción y proceso)*, Civitas, Madrid, 1981.

GÓNZALEZ CANO, I., «La mediación penal en España», en *La mediación penal para adultos una realidad en los ordenamientos jurídicos: (experiencia en España, EEUU, Inglaterra y Gales, Países Escandinavos, Francia, Alemania, Portugal, Brasil y Chile)*, Tirant lo Blanch, Valencia, 2017, pág. 25.

SAÉZ VALCARCEL, J., «La mediación penal, una metodología judicial para ocuparse de la reparación y de la resocialización», en *Boletín del Ministerio de Justicia*, 2008, Año 62, núm. 2060.

SÁNCHEZ GÓMEZ, R., «Mediación Penal y Violencia de Género. Un adecuado sistema de resolución de conflictos», en *Construyendo la igualdad. La feminización del Derecho privado*, Tirant lo Blanch, Valencia, 2017.

Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

Financiación

El documento ha sido elaborado sin financiación.

INCORPORACIÓN DE LOS WHATSAPP Y OTRAS APLICACIONES SEMEJANTES DE MENSAJERÍA ELECTRÓNICA AL PROCESO PENAL EN LA FASE DE INSTRUCCIÓN

Incorporation of whatsapp and other similar electronic messaging applications into criminal proceedings during the pre-trial phase

Por Alfredo Martínez Guerrero

Letrado de la Administración de Justicia
altiro1964@gmail.com

Artículo recibido: 22/05/22 | Artículo aceptado: 23/06/22

RESUMEN

Este artículo se ocupa de una práctica que se está extendiendo por las Oficinas Judiciales Penales a la misma velocidad con la que se extiende las aplicaciones de mensajería instantánea como medio de comunicación social. La incorporación anómala al procedimiento penal del contenido de la conversación o mensaje mediante su impresión y “cotejo” por parte del letrado de la Administración de Justicia. Un uso forense poco pensado y de perniciosos efectos probatorios. La alternativa prevista por legislación procesal existe. Es respetuosa con las competencias documentadoras/de fe pública de los Letrados Judiciales y escrupulosa con la naturaleza jurídica de la actuación procedimental que se realiza.

ABSTRACT

This article deals with the anomalous incorporation into the criminal procedure of the content of the conversation or message generated through instant messaging applications and its evidentiary effects from the perspective of the public faith competences of the Judicial Clerk.

PALABRAS CLAVE

WhatsApp, Mensajería electrónica, Cotejo, Documentos públicos y privados, Letrados de la Administración de Justicia, Diligencias de constancia.

KEYWORDS

WhatsApp, messaging applications, Document collation, Public and private documents, Judicial Clerk, Diligences of constancy

Sumario: 1. Introducción. 2. ¿Cómo se incorporan al procedimiento penal? La documentación de las aplicaciones electrónicas. 3. ¿Necesitan ser cotejadas?. 3.1. La conversación de Whatstapp, documento privado. 3.2. La conversación de WhatsApp, documento público. 3.3 Actividad procesal a desarrollar por los Letrados Judiciales en tales supuestos. 4. Verdadera naturaleza de la actuación a realizar en esta incorporación de mensajería instantánea por los Letrados de la Administración de Justicia. 5. Conclusiones. 6. Bibliografía.

1. Introducción

Las diligencias instructoras del proceso penal español vienen recogidas en una norma que ha conocido tres centurias y dos milenios, -yo apuesto a que conocerá alguna más, lo que no es, necesariamente, una mala noticia si uno se asoma al BOE actual-: la Lecrim. Comienza en sus artículos 326 a 485, se retoma en el artículo 545 y sigue hasta el 588 octies. Además de diversos preceptos en el Título II del Libro IV para el procedimiento abreviado, como el artículo 777 y 778. Su enumeración es demasiado farragosa para acometerla aquí; solo apuntaremos que la regulación de estas diligencias de investigación se inicia con la inspección ocular y termina con los registros remotos sobre equipos informáticos.

No es una relación exhaustiva y cerrada. Conforme a la STS 4183/1995: *“No es nuestro sistema procesal penal de los que mantienen pruebas legales o tasadas, que también existieron históricamente en España, sino que, con criterio más flexible, existe una libertad de aceptación de las pruebas por el juzgador a condición de que tengan en efecto carácter probatorio y, así, se aceptan no solo las enumeradas en la Ley de Enjuiciamiento Criminal, sino también otros medios probatorios más modernos, no conocidos aun cuando ese texto legal se promulgó, como son la dactiloscopia, la fotografía, los medios de reproducción de imágenes en movimiento (cinematografía, video), los fonográficos, los cibernéticos, etc.”*. Este sistema abierto no sirve de excusa, claro está, para *“inventarse”* usos forenses como el que es objeto de análisis en este trabajo, que desnaturaliza los medios probatorios ya existentes y malogra a los novedosos como el documento electrónico.

Por más que sea sabida¹, conviene recordar la distinción entre las fuentes de prueba, es decir los objetos o efectos que existen en la realidad -la cosa que ha de ser estudiada- y los medios de prueba, que son los instrumentos/formas a través de lo/as cuales aquélla se introduce en el procedimiento judicial. En el ámbito penal las fuentes de prueba se convertirán en diligencias instructoras y

¹ CARNELUTTI, F., La prueba civil, 2ª ed., Ejea, ed. Desalama, Buenos Aires, 2000, pp. 67 y ss.

medios de prueba, cuando se incorporen -adecuadamente- a la fase de investigación y se practiquen en el juicio oral, respectivamente.

En este artículo nos vamos a ocupar de una fuente de prueba que es la reina de la comunicación social y su derivada procesal como diligencia instructora incorporada, con validez y eficacia, al procedimiento penal. Nos estamos refiriendo al WhatsApp cuya extensión y uso generalizado justifica que lo utilicemos de modelo, con la aclaración inicial de que lo se diga de él, resulta aplicable al Line, Telegram, Instagram, Messenger, o cualquier otro que conozcan.

Intentaremos, para que tenga la máxima utilidad, ser muy concretos en la forma de abordar este trabajo, elaborando una especie de guía de actuación que facilite la labor cotidiana de los distintos profesionales que trabajamos en la jurisdicción penal, sean jueces, letrados de la Administración de Justicia, fiscales, abogados, policías o ciudadanos en general.

2. ¿Cómo se incorporan al procedimiento penal? La documentación de las aplicaciones electrónicas

2.1 Todos los que trabajamos en un Juzgado con competencias penales nos hemos acostumbrado a que llegue un ciudadano, con o sin su abogado, a la Oficina Judicial diciendo/pidiendo: “tengo aquí mi teléfono con un chat en el que me insultan, amenazan”... quiero que el letrado de la Administración de Justicia... lo coteje. El funcionario, gestor o tramitador, va raudo al despacho del juez a darle cuenta y éste sin más, dice que sí que el letrado judicial... coteje... Y el fedatario judicial, atareado en mil asuntos, sin más análisis ni cuestionamientos, extiende una diligencia en la que, poco más o menos se dice que visto el teléfono X, se lee en la pantalla una conversación en la que Fulanito manifiesta que va a hacer X a Mengano y que los pantallazos -fotocopias del chat- coinciden con lo que ha visto. La firma señalando que da fe y eso es todo. Devuelven el teléfono a su dueño que se lo lleva para seguir dándole uso y... hasta el acto del juicio oral, que tendrá como medio de prueba esa diligencia extendida por el fedatario judicial con los pantallazos en papel del chat.

La inercia del mundo analógico resulta, una vez más, triunfante y como si se tratara de comparar un documento original escrito en papel con una copia -también escrita en papel- del mismo, se confunde y mezcla el clásico cotejo previsto en el artículo 334 LEC, con la transcripción a papel de un documento electrónico, todo ello aderezado con una fe pública judicial adulterada e inoperante. Es un error muy frecuente en la jurisprudencia menor, sirva como ejemplo el AAP MA 209/2022, Sección 8ª, ponente Manuel Cabellero-Bonald Campuzano, en la que se estima un recurso de apelación contra una resolución del Juzgado de Instrucción y llega a establecer lo siguiente: “*Distinta decisión debemos adoptar sobre la segunda de las diligencias interesadas. La parte recurrente*

*interesó la práctica de diligencia de investigación "consistente en "certificación de la veracidad del material aportado en cuanto a imágenes y fechas" y "testimoniar la veracidad de la conversación abierta tipo WhatsApp entre la supuesta víctima y el investigado". Es cierto que la petición adolece de notables deficiencias técnicas. No es el Juzgado ni el Sr Letrado de la Administración de Justicia del mismo quien puede certificar la veracidad de tal contenido documental, siendo ese objeto más propio de una pericial, pero sí puede advenir el contenido y realidad de tales conversaciones y **mensajes**, así como de las fechas de los mismos (aunque no de su "ausencia de manipulación").*

*Dicha diligencia debe estimarse útil y relevante para concretar la existencia-o no- de indicios de un delito de detención ilegal, pues sería un indicio de que la denunciante supuestamente tenía a disposición y podía utilizar su teléfono móvil durante el tiempo que, según sus manifestaciones, estuvo retenida contra su voluntad por el investigado. Tal adveración y cotejo de mensajes, conversaciones...es una diligencia propia de la fase de instrucción y no del trámite de juicio oral, en su caso, sin que el hecho de que las conversaciones aparezcan en inglés sea obstáculo alguno para su **práctica**.*

Es por ello que el recurso de apelación debe ser admitido parcialmente en el sentido de acordar que por el Sr o Sra Letrado de la Administración de Justicia del Juzgado de Violencia Sobre la Mujer Nº 1 de Fuengirola se proceda al cotejo y adveración de los mensajes y llamadas señaladas por la parte recurrente en sus escritos, con indicación de fechas, horas y contenido(no respecto a la "ausencia de manipulación" pues no es esa su función y cometido), con citación de las partes para tal diligencia, debiendo auxiliarse del correspondiente intérprete si fuera necesario".

Esta resolución va más allá -incluso- de la confusión dicha y que trataremos de deshacer en este artículo. No sólo acuerda que se realice un cotejo y adveración de los mensajes y llamadas -cualquiera que sea lo que tal cosa significa desde un punto de vista procesal- sino que, además, le dice al letrado de la Administración de Justicia la manera de ejercer la fe pública judicial de la que es depositario exclusivo señalando lo que debe hacer constar: fechas, horas y contenido.

La sola transcripción de la cita hace que resuene con fuerza el artículo 452.1 de la LOPJ: "Los secretarios judiciales desempeñarán sus funciones con sujeción al principio de legalidad e imparcialidad en todo caso, al de autonomía e independencia en el ejercicio de la fe pública judicial". Es un precepto interpretado en numerosas ocasiones por nuestro Tribunal Supremo. Citaremos sólo la STS 2340/2007, Sala Tercera, por su claridad/rotundidad. En su fundamento jurídico quinto establece que: "resulta evidente que al Secretario corresponde con exclusividad y plenitud el ejercicio de la fe pública judicial, en el ejercicio de la cual dejará constancia fehaciente de la realización de actos procesales en el Tribunal o ante éste y de producción de hechos con trascendencia procesal".

La sola transcripción de la cita parece trasladarnos al año 2009 y a la redacción añeja del artículo 743.2 de la LECRIM que decía: *“Al terminar la sesión se leerá el acta, haciéndose en ella las rectificaciones que las partes reclamen, si el Tribunal en el acto las estima procedentes.”* Nefanda redacción sustituida por el actual artículo 743.5 según el cual: *El acta prevista en los apartados 3 y 4 de este artículo, se extenderá por procedimientos informáticos, sin que pueda ser manuscrita más que en las ocasiones en que la sala en que se esté celebrando la actuación carezca de medios informáticos. En estos casos, al terminar la sesión el Secretario judicial leerá el acta, haciendo en ella las rectificaciones que las partes reclamen, si las estima procedentes. Este acta se firmará por el Presidente y miembros del Tribunal, por el Fiscal y por los defensores de las partes.* Esta modificación legal que, para algunos, pasa desapercibida supuso dar coherencia ontológica a la fe pública en los Juzgado y Tribunales españoles que, al fin, hicieron efectiva la independencia de aquélla. No era, ni es sostenible que alguien ajeno al fedatario público pueda decidir lo que debe constar o no en un acta extendida por éste. Sería un vasallaje que pervertiría las garantías del proceso judicial para el ciudadano.

La sola transcripción de la cita parece ignorar lo que el Tribunal Supremo dejó bien claro: que los jueces no deben inmiscuirse -sic- en la fe pública judicial, STS 7208/2009 en la que se establece: *“Difícilmente es hoy sostenible, con el contenido de la Ley Orgánica del Poder Judicial, que el Tribunal pueda inmiscuirse en la fe pública judicial. El art. 454 les atribuye el principio de autonomía e independencia en el ejercicio de la fe pública judicial. Y en igual sentido, el art. 454 dispone que los secretarios judiciales son responsables de la función de documentación que les es propia.”*

La sola transcripción de la cita también parece borrar, de un plumazo, las grandes reformas que se llevaron a cabo a partir del año 2000 en nuestro Ordenamiento Jurídico procesal y orgánico. Como si los letrados judiciales y la fe pública que ostentan, siguieran tutelados e integrados en el haz de competencias jurisdiccionales que ejercen los Jueces, y no en las judiciales que ejercen aquéllos, como partes integrantes e indispensables de los Juzgados y Tribunales. Pero todos estos pareceres -y algunos más- constituyen otros asuntos ajenos a este trabajo. Asuntos ya tratados, con cierta profundidad, en otra ocasión.²

Incluso juristas de reconocido prestigio en materia de tecnología judicial como Joaquín Delgado, incurren en la práctica señalada de admitir los *“cotejos”* como medio probatorio y nos dice -si bien por medio de la cita de Jaume Alonso-Cuevillas- lo siguiente: *“Téngase en cuenta que en el mismo proceso pueden*

² Martínez Guerrero, A. (2021). El carácter judicial de los letrados de la administración de justicia. *Revista Acta Judicial*, (7), 72-124. Recuperado a partir de <https://revistaactajudicial.letradosdejusitia.es/index.php/raj/article/view/53>

*utilizarse varios medios probatorios de forma cumulativa: por La Ley no determina que la prueba electrónica solamente puede tener eficacia probatoria si se cumplen ciertos presupuestos legales; sino que cualquier prueba digital puede, en principio, desplegar efectos ejemplo, aportación del smartphone en el que se encuentre una conversación de WhatsApp, junto una transcripción escrita de la misma solicitando el cotejo por el Secretario Judicial; y testifical (o interrogatorio de parte o del acusado) sobre el contenido de esa conversación”.*³

El producto es -en realidad no podía ser otra cosa- algo de imposible catalogación procesal, cuya eficacia probatoria es mínima, salvo que la acepten los perjudicados y partes; lo que no resulta infrecuente, por extraño que parezca, sobre todo si tenemos en cuenta el asesoramiento jurídico de las partes. Aunque entonces nos encontraremos con que los hechos son probados no por tal *práctica forense*, sino mediante verdaderos medios de prueba: testificales o confesión del acusado. Un ejemplo -hay muchos- claro de la inconsistencia/inutilidad de estos mal llamados cotejos lo pone de manifiesto la SAP GR 1435/2021, en el que no dice: “ *El cotejo por la Letrada del Juzgado de Instrucción de las capturas o impresiones de pantalla aportadas en su día por la Acusación Particular con lo que se reflejaba en el terminal móvil... esa diligencia no prueba otra cosa sino que los documentos impresos aportados por la denunciante se correspondían con los mensajes escritos que efectivamente se encontraban en la pantalla de su terminal, pero no la procedencia de la línea telefónica remitente como se ocupó de consignar expresamente la Letrada de la Administración de Justicia. Y ello entronca una vez más con la falta de rigor probatorio de esos documentos telemáticos bien para demostrar la autoría del acusado en las expresiones ofensivas, bien como elemento de corroboración de la testifical de la denunciante que así lo sostiene, al no venir completada esa prueba documental con la pericial técnica”.*

Como veremos más adelante, es necesario determinar la naturaleza jurídica de lo que se pretende hacer dentro del procedimiento penal previsto en la actual LECRIM, con este nuevo fenómeno de comunicación social para encontrarle un acomodo procesal -que lo tiene- acorde a lo que se pretende.

2.2 Para evitar tales prácticas - hijas casi siempre del mucho trabajo en las Oficinas Judiciales y de la inercia del papiro que impera en ellas -, vamos a realizar una serie de reflexiones que culminarán en distintas recomendaciones. Su objetivo básico es que puedan utilizarse a modo de protocolo, para incorporar la fuente de prueba de una conversación en WhatsApp - o de cualquier otra aplicación de mensajería-, como un medio de prueba válido -con pleno valor probatorio- a una causa penal.

³ Delgado Martín, Joaquín. “La prueba digital. Concepto, clases, aportación al proceso y valoración”. Diario La Ley. Nº 6. 11 de abril de 2017

1º Aportación del dispositivo electrónico en que se contenga el WhatsApp. Las formas de aportación son, básicamente, dos:

a) *Que lo presente la propia parte -denunciante o investigado-*. En este caso habrá de hacerse constar las circunstancias de la entrega: fecha, persona que lo entrega, estado del mismo y su descripción con el modelo y el IMEI. Además, se deberá depositar en el Servicio Común de Piezas de Convicción donde se garantizará la cadena de custodia hasta que sea examinado por el Tribunal sentenciador. No debemos olvidar que esa incorporación solo puede hacerse, con validez, por uno de los sujetos que hayan intervenido en el proceso de comunicación de que se trate, o con su consentimiento si lo aportara un tercero que pretenda hacerlo en su nombre, para evitar contaminar la fuente de prueba con la ilicitud de vulnerar el artículo 18.3 de la CE. Así lo estableció el Tribunal Constitucional en su sentencia de referencia 114/1984, de 29 de noviembre en la que se dice: *“No hay «secreto» para aquel a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el art. 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje. Dicha retención (la grabación, en el presente caso) podrá ser en muchos casos, el presupuesto táctico para la comunicación a terceros, pero ni aun considerando el problema desde este punto de vista puede apreciarse la conducta del interlocutor como preparatoria del ilícito constitucional, que es el quebrantamiento del secreto de las comunicaciones. Ocurre, en efecto, que el concepto de «secreto» en el art. 18.3 tiene un carácter «formal», en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado. Esta condición formal del secreto de las comunicaciones (la presunción «iuris et de iure» de que lo comunicado es «secreto», en un sentido sustancial) ilumina sobre la identidad del sujeto genérico sobre el que pesa el deber impuesto por la norma constitucional. Y es que la imposición absoluta e indiferenciada del «secreto» no puede valer, siempre y en todo caso, para los comunicantes, de modo que pudieran considerarse actos previos a su contravención (previos al quebrantamiento de dicho secreto) los encaminados a la retención del mensaje. Sobre los comunicantes no pesa tal deber, sino en todo caso, y ya en virtud de norma distinta a la recogida en el art. 18.3 de la Constitución, un posible «deber de reserva» que —de existir— tendría un contenido estrictamente material, en razón de cual fuese el contenido mismo de lo comunicado (un deber que derivaría, del derecho a la intimidad reconocido en el art. 18.1 de la norma fundamental)”*.

b) *Que sea intervenido por la Policía*. Deberá presentarlo con el atestado oportuno, en el que se hagan constar todos los elementos dichos de las circunstancias que individualizan al aparato. Deberá, igualmente, depositarse en forma en el Servicio Común. La intervención podrá haberse realizado, sin mandato policial -en una detención como pertenencia- o con mandato judicial en el curso de un registro domiciliario. En ambos supuestos debe quedar constancia de todas las actividades llevadas a cabo por cada una de las personas

que se ponen en contacto con las evidencias, conforme a la STS 587/2014, de 18 de julio para garantizar la cadena de custodia.

2º Incorporación de su contenido a la causa. Varias son las formas de hacerlo en la actualidad.

a) La primera -y más recomendable- será la incorporación del propio dispositivo electrónico como *documento electrónico a la causa*.

Debemos tener en cuenta que estas aplicaciones de mensajería instantánea son muy peculiares desde el punto de vista procesal: su contenido material no está conservado en un servidor externo al que se pueda acudir, ajeno a los dispositivos electrónicos de los sujetos que intervienen en la comunicación. Es decir, no hay un disco duro, nube o dispositivo en el que se deposite y conserve la información transmitida en los mensajes. Esto supone que, una vez que los mensajes son lanzados por el emisor y abiertos por el receptor, cualquier examen o comprobación que quiera hacerse sobre la conversación mantenida entre ambos no puede llevarse a cabo sobre un original que la empresa que ha proporcionado el servicio tenga a buen recaudo. Dicho de otra forma: las conversaciones y archivos de la aplicación *únicamente se quedan registradas en los terminales móviles utilizados*, nunca en el servidor de la aplicación.

La consecuencia evidente es que ese *examen y estudio solo podrá realizarse sobre los propios aparatos electrónicos que se hayan utilizado en el proceso de comunicación* que son los que albergarán de forma única el contenido de la conversación. Examen que debe complementarse con los datos de tráfico que esa conversación genera, tales como la identidad de los intervinientes, nombres de usuario, claves, IP y números de teléfono; que en este caso si proporciona la empresa que presta el servicio⁴.

Este proceso complejo es muy relevante que se conozca y explique en el ámbito del procedimiento penal. Supone que si desaparecen los dispositivos electrónicos que han intervenido en la comunicación, nos quedemos sin el original *-con todos los datos que la integran-* de dicha comunicación. Por otro lado, hay que recordar que *los WhatsApp pueden ser manipulados si se dispone de los adecuados conocimientos informáticos. Puede imputarse a una persona la autoría de un previo mensaje interceptado y reenviado ulteriormente con su contenido convenientemente modificado*⁵.

⁴ En este sentido ver FUENTES SORIANO: El WhatsApp como fuente de prueba, Proceso Penal. Reflexiones. Tirant Lo Blanch, 2017, pp. 351 a 362.

⁵ Como nos señala José Luis RODRÍGUEZ LAINZ (Magistrado. Juzgado de Instrucción 4 de Córdoba), en su artículo «Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2.ª, 300/2015, de 19 de mayo)», Diario LA LEY, núm. 8569, Sección Doctrina, 25 Jun. 2015).

b) Mediante el volcado del contenido del móvil por perito informático de alguno de los grupos de policía científica; siempre que esté autorizado por resolución judicial. En este caso la fuente de prueba se convertiría en un medio de prueba pericial, cuyo valor probatorio puede y debe conjugarse con otros como testificales, declaraciones de las partes o reconocimiento judicial.

c) Por transcripción del mismo. La forma de esa transcripción es variada. Imprimiendo los “pantallazos” del aparato electrónico que deberán digitalizarse nuevamente para incorporarse a los Sistemas de Gestión Procesal. Aportando la parte el contenido de la conversación en un escrito digitalizado. O bien, remitiendo la conversación por correo electrónico a la cuenta de correo del Juzgado. En estos dos últimos supuestos, también se incorporarán al Sistema de Gestión Procesal directamente o en pdf escaneado. Este es el medio más usado, sin duda, por lo cómodo -y barato- que resulta. Como veremos a continuación el que más problemas ocasiona, porque no se debe olvidar el viejo adagio de lo barato sale caro...

3. ¿Necesitan ser cotejadas?

Una vez incorporadas las conversaciones al procedimiento penal -en alguna de las tres formas dichas- la pregunta a responder es si resulta necesario el cotejo, bajo la fe pública del letrado judicial, de lo incorporado con el dispositivo que lo contenga.

En relación a las dos primeras, la respuesta negativa es tan evidente que no necesita de mayor comentario. En la primera queda incorporada a la causa el propio documento electrónico en su soporte original, de forma que no hay copia que cotejar. Es, como dijimos la más recomendable y tiene su soporte legal en la aplicación analógica del 384 de la LEC, que se ocupa de los medios de prueba en relación a instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso. Además, al quedar incorporado el propio documento electrónico, permitirá cumplir las cautelas establecidas por la STS 300/2015, a propósito de la comunicación mantenida mediante la aplicación Tuenti, para poder llevar a cabo el peritaje oportuno sobre el mismo. Nos dice dicha resolución lo siguiente: *“la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quién pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que*

identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.”

En la segunda, la fuente de prueba se ha convertido en medio de prueba: un informe pericial. La innecesidad de los cotejos respecto a tales informes es tan evidente que permiten omitir cualquier otra argumentación al respecto.

Solo la tercera puede plantear las situaciones equívocas descritas en apartado II.1. Pero la respuesta es tan negativa como en las otras dos formas. Veamos la explicación/justificación de esta negación que debe ser contundente.

3.1. La conversación de Whatstapp, documento privado

Debemos empezar señalando que la LECRIM no tiene preceptos que nos puedan orientar en esta materia. Su antigüedad no es explicación suficiente para esta laguna que debemos colmar con la LECIVIL.

Este cuerpo legal distingue dos tipos de documentos como medios de prueba, los públicos y los privados. Con lo que nos encontramos ante la primera sorpresa: los usos forenses de la jurisdicción penal tienden a olvidar la naturaleza jurídica de las conversaciones de las aplicaciones de mensajería señaladas. Son documentos -electrónicos- privados, por lo que la fuerza probatoria de los mismos es la que se recoge en el artículo 324 y ss, no la del artículo 320 -documentos públicos- sobre la que volveremos después.

Conforme al artículo 326.1 LEC, aportada la conversación por escrito por la parte interesada, como documento privado que es, hará prueba plena en el proceso cuando su autenticidad no sea impugnada por la parte a quién perjudique.

En caso de impugnación, nos dice el párrafo tercero de ese artículo que *“Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014”*. Ese apartado 2 establece que cuando se impugne la autenticidad de un documento privado -como es el caso- *“se podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil”*.

La letra de los preceptos transcritos es tan clara que exime de interpretaciones/elucubraciones en las que pueda tener cabida la intervención de la fe pública judicial para realizar un cotejo. *Solo cabe la prueba pericial o cualquier otro medio de prueba que pudiera resultar útil* y entre tales medios de prueba no está la intervención del garante de la autenticidad e integridad de los mismos que debe documentarlos, no protagonizarlos.

3.2. La conversación de Whatstapp, documento público

Nos dice la STS 353/2021, de 11 de febrero, que *“los principios que, aun hoy, conforman nuestro proceso penal, en especial los de oficialidad y búsqueda de la verdad material, por mucho que en ocasiones hayan merecido cierto cuestionamiento doctrinal, siguen facultando al Juez, desde su actual vigencia configurando a éste en una posición exigentemente imparcial, pero absolutamente neutral, para la formulación de ese interrogatorio, de acuerdo con lo dispuesto en el párrafo segundo del art. 708 LECRIM. (STS 1320/2011, 9 de diciembre).”* Sobre la base de tales principios de oficialidad y búsqueda de la verdad material, habrá algún sector doctrinal/judicial que defienda que, aunque se trate de un documento privado, el juez instructor pueda acordar que se apliquen los preceptos del cotejo del artículo 320 LEC. Aceptemos esa postura a los solos efectos dialécticos, para ver dónde nos conduciría la aplicación de los mismos a la materia que nos ocupa.

Según la RAE cotejar es *“confrontar algo con otra u otras cosas, o compararlas teniéndolas a la vista”*. Por su parte, el artículo 320 LEC nos dice que el cotejo o comprobación de los documentos públicos -en papel o en soporte electrónico- con sus originales será llevado a cabo por el Letrado de la Administración de Justicia.

Así que podemos concluir que la actividad de cotejar *en un proceso jurisdiccional* requiere de:

1º El sujeto activo que realiza la acción en qué consiste.

2º La potestad del sujeto activo -depositada en él por el Estado- que garantiza la veracidad del resultado de esa actividad que no podrá ser puesta en duda -iuris tantum-, la fe pública judicial.

3º Un primer elemento material, integrado por el objeto que va a servir de muestra para ser comparado o confrontado, el original indubitado.

4º. Un segundo elemento material, integrado por el objeto que, en principio, es reproducción del original, dubitado.

Solo con la conjunción de esos cuatro elementos el resultado del cotejo cumplirá los requisitos exigidos en la LEC y, por ende, en la LECRIM a la que aquélla suple. El sujeto activo, el letrado judicial, examina el elemento indubitado, a continuación, hace lo propio con el dubitado y comprobando y confrontando ambos objetos, acreditará si el uno -dubitado- es reproducción fiel y exacta del otro -indubitado- o no. La diligencia o acta que extiende en ese proceso será garantizada con su fe pública judicial y servirá para que la instrucción concluya -en su caso- en un auto de juicio oral y, sobre todo, para ser introducida en el acto del juicio oral como medio de prueba en la categoría de documento público.

Es un proceso en apariencia sencillo. Pero su engranaje es delicado. Si quitas una de las piezas el resultado se descompone/disloca y dará lugar a un

“engendro” que lo privará de la validez a que está llamado. Y eso es lo que ocurre cuando se pretende que se coteje por un letrado de la Administración de Justicia, un documento electrónico privado integrado en un móvil, con un documento en papel que recoge la transcripción de la conversación contenida en él. *Falta el tercero de los elementos señalados del proceso: el original indubitado.* El documento privado electrónico en el que se recoge la información que debe ser cotejada, no se forma por los caracteres gráficos que se pueden observar en la pantalla del móvil. Eso es sólo una parte del mismo, la punta del iceberg. Tiene otros elementos que lo integran, de gran importancia, a los que no se puede acceder mirando, simplemente, la pantalla del artefacto. En consecuencia, no podrán ser comprobados por el letrado de la Administración de Justicia y el cotejo deviene imposible. Algunos de tales elementos son los metadatos, es decir los datos que describen el contenido del archivo o la información de tales archivos. Son de gran relevancia para conocer y determinar el original indubitado por dos razones que nos son muy familiares. La *autenticidad*: el documento electrónico privado será auténtico, cuándo sea lo que dice ser. La comprobación de dicha autenticidad se valida mediante los metadatos que permiten ubicar al documento en un proceso y contexto determinado. La *integridad*: un documento es integro, cuando es original. Es decir, cuando el mismo no ha sido manipulado o alterado deliberadamente. La integridad se puede comprobar mediante metadatos de auditoría, es decir, los que registran cada una de las acciones que se realizan sobre el documento original.

Pues bien, la ausencia de tales metadatos malogra/imposibilita, como hemos dicho, cualquier cotejo que se pretenda realizar.

3.3 Actividad procesal a desarrollar por los Letrados Judiciales en tales supuestos

Cuando la inercia forense se impone y se acuerda uno de los cotejos señalados en una resolución judicial, el letrado de la Administración de Justicia debe cumplir lo que acuerda aquélla, por mandato del artículo 452.2 de la LOPJ. Además, como autoridad pública que es, integrado en los Juzgados y Tribunales como parte indisoluble de los mismos, debe velar, por mandato del artículo 452.1 de la LOPJ, porque el resto del Ordenamiento Jurídico se cumple; lo que incluye la independencia del letrado judicial en el ejercicio de la fe pública judicial. Y ésta- la fe pública judicial-, no sólo garantiza la realización del acto, *sino el cumplimiento de las formas* que la Ley impone para su realización, extremo de importancia en el campo del proceso donde el cumplimiento de las *formas esenciales* es uno de los principios fundamentales que vertebran la institución procesal.

Para conjugar ambos mandatos los Letrados de la Administración de Justicia, en el trance señalado, deberán:

1º Citar a las partes a la diligencia instructora que se va a llevar a cabo, pues se debe respetar la contradicción.

2º Abierto el acto, harán constar las partes que comparezcan. A continuación, el nombre de quién presenta el teléfono o dispositivo de que se trate y los documentos impresos en papel, correspondientes a las conversaciones objeto de la diligencia. Para el supuesto de que no las trajera impresas se pueden hacer dos cosas, suspender el acto para que las aporte o remitir el chat por correo electrónico al del Juzgado e imprimirlo.

3º Hará constar en el acta o diligencia que se extienda que, tratándose de un documento electrónico privado la conversación del chat contenida en el teléfono descrito, *su incorporación al procedimiento mediante su conversión en documento escrito, no está prevista en la Lecrim y tampoco en la Lecivil.*

4º Hará constar que dicha impresión escrita y aportada por la parte, solo contiene el fichero con los datos en estructura XML y en formato work/word o PDF. Pero que no se aportan:

a) Los *metadatos de dicho fichero*, imprescindibles para poder realizar la trazabilidad del mismo, lo que permitirá eludir riesgos tales como el de la supresión de mensajes de WhatsApp de la secuencia de mensajes de la conversación aportada, el de la incorporación de mensajes reenviados, entre otros.

b) Ni *ningún tipo de certificado CSV* como parte integrante del documento electrónico privado.

5º Hará constar que la ausencia de tales elementos imposibilita la actividad del cotejo acordado, es decir, de comparar el original indubitado: el documento electrónico privado contenido en el teléfono móvil -pues no se tienen presentes todos los elementos que lo integran ya dichos-; con el documento dubitado: la transcripción en papel impreso aportada. Operación que, por otra parte, requeriría de unos conocimientos informáticos de los que carece un letrado judicial dada su formación jurídica.

6º Hará constar primero, que se devuelve a la parte que lo presenta el documento privado electrónico presentado -es decir el teléfono móvil que lo aloja-. A continuación, que se incorpora a las actuaciones, como parte del acta o diligencia, la impresión escrita aportada por la parte del archivo del documento electrónico ya señalado, para que -en su momento- sea valorado conforme a lo establecido en las Leyes Procesales por el personal jurisdicente al que corresponda y, sin perjuicio del derecho de las partes a proponer la prueba pericial que estimen oportuna sobre dicho documento electrónico para identificar el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad y autenticidad de su contenido.

4. Verdadera naturaleza de la actuación a realizar en esta incorporación de mensajería instantánea por los Letrados de la Administración de Justicia

Como venimos señalando, gran parte de los operadores jurídicos de los Órganos Judiciales penales -incluidas algunas Audiencias Provinciales-, vienen asimilando la antigua labor de cotejo de las escuchas telefónicas impuesta por el Tribunal Supremo en relación a las intervenciones de las comunicaciones telefónicas, a la forma de incorporar la mensajería instantánea a un proceso penal.

En modo alguno son comparables. Los cotejos de las escuchas telefónicas fueron establecidos por el Tribunal Supremo allá por el año 2008⁶ como protocolo que remediase la falta de regulación legal. Era un proceso bien descrito, establecido en una sentencia del Tribunal Supremo -a falta de texto legal-, con los pasos a realizar y, sobre todo, los elementos a incorporar. Los originales de unas cintas o DVDs con las conversaciones mantenidas y su transcripción al papel, ambas realizadas por la Policía. La función del letrado judicial era oír unas y garantizar que lo transcrito por la Policía era lo que se dijo en aquéllas. Los cuatro pasos ya dichos -fe pública, documento auténtico (las cintas), documento a comparar (la transcripción) la comparación de una y otra- se podían realizar sin obstáculo, por farragoso que fuese el proceso y un tanto absurdo, pues no evitaba que tuvieran que ser oídas las cintas en el juicio, si alguna de las partes lo interesaba.

Por cierto, protocolo ya innecesario en la medida que los artículos 588 ter f) y 588 ter i) de la Lecrim han venido a colmar el vacío, haciendo protagonista a las partes en la forma de determinar la veracidad de las transcripciones que se incorporan a la causa.⁷

¿Qué hacer entonces con la información de la mensajería instantánea en el proceso penal, si los cotejos no son posibles? ¿Cuál es la labor de los Letrados de la Administración de Justicia en relación a los mismos para el supuesto más que frecuente de que se obvие lo señalado en el apartado III.1 y se opte por la senda del apartado III.2?

La respuesta la encontramos, como casi siempre, en las leyes. En este caso concreto en la LOPJ y en el RD 1608/2005, en los artículos 453.1, 3 y 5 a) respectivamente. En el primero se establece que *“Corresponde a los Letrados de la Administración de Justicia, con exclusividad y plenitud, el ejercicio de la fe pública judicial. En el ejercicio de esta función, dejarán constancia fehaciente de la realización de actos procesales en el Tribunal o ante éste y de la producción de hechos con trascendencia procesal mediante las oportunas actas y diligencias”*.

⁶ España. Tribunal Supremo. Sentencia núm. 745/2008 de 25 de noviembre.

⁷ Ver España. Audiencia Provincial de Málaga, Sección 2ª. Auto núm. 183/2018, de dos de marzo.

Hay un hecho que tiene transcendencia procesal, la comunicación contenida en el whatstapp y será mediante una diligencia de constancia como incorporaremos lo acontecido al procedimiento judicial de que se trate. El acomodo procedimental está previsto. Hace innecesario todos los “*inventos*” ya descritos, además de cumplir con la naturaleza de lo que se documenta y las funciones del que lo hace.

El contenido de tal diligencia podrá ser el que expondré a continuación, más allá -claro está- de lo que considere necesario incluir o no cada letrado judicial en el ejercicio independiente de sus potestades de fe pública.

- Identificación de los intervinientes, con expresión literal de que la intervención del Letrado de la Administración de Justicia en esta diligencia no acredita la titularidad de la líneas de teléfono remitente y receptora, ni la identidad del autor de dichos mensajes, limitándose la intervención del fedatario judicial a dejar constancia de la existencia en el móvil de la parte, de los mensajes que se dirán, tal y como aparecen a la fecha de la diligencia; sin que pueda determinarse por el letrado judicial, si esos mensajes han podido ser alterado o no, lo que corresponderá, en todo caso, a expertos informáticos

- Identificación de los números de teléfono -o aparatos- utilizados para el envío y recepción de los mensajes, según lo que aporten las partes y sus manifestaciones, con expresión de los IMEI que deberán ser comprobados por el letrado judicial. (Puede hacerse, en la actualidad, mediante los comandos *#06#).

- Exhibición por la parte de la conversación o conversaciones que se quieren documentar. Examinada/s por el letrado judicial, dejará constancia de que la/s misma/s aparece/n vinculada/s al/os número/s telefónico/s de que se trate y a ningún/os otro/s más.

- Pedir a la parte que se envíe el contenido de los mensajes como archivo de texto, por correo electrónico, a la dirección del correo electrónico del Juzgado del letrado judicial interviniente.

- Una vez recepcionado, entrar en el correo del Juzgado abrirlo, copiar íntegramente su contenido y pegarlo a la diligencia que se esté extendiendo, quedando incorporado su contenido a la diligencia de constancia.

- Dar por concluido el acto, con la firma electrónica de la diligencia de constancia por el letrado judicial, quedando integrada la diligencia de constancia en el Sistema de Gestión Procesal correspondiente.

5. Conclusiones

1º. La actividad instructora y probatoria en un proceso penal está y debe estar revestida de unas garantías de legalidad que la inercia forense y la falta de reflexión sobre las diferencias entre el mundo analógico y digital está complicando de manera innecesaria.

2º Los preceptos legales de la LECIVIL permiten hacer frente, con claridad, a los retos procesales que el mundo electrónico nos presente en el procedimiento penal para incorporar al mismo las nuevas realidades de los procesos de comunicación entre los ciudadanos.

3º Los Whatstapp y resto de aplicaciones de mensajería instantánea se han convertido en las nuevas herramientas de comunicación en nuestra sociedad. Su realidad digital y privada le dota de acomodo procesal en los documentos electrónicos privados.

4º. La forma de incorporarlos al proceso penal es la prevista en los artículos 324 y ss LECIVIL que se ocupa de normalizar la forma de actuar en caso de que se ponga en duda su autenticidad.

5º El cotejo de tales documentos privados y electrónicos es una actividad ajena a la fe pública judicial y, por ende, a las funciones de los letrados de la Administración de Justicia.

6º En el supuesto, poco de ortodoxo y de nula eficacia probatoria *per se*, de que se acuerde el mencionado “cotejo”, la actividad del letrado de la Administración de Justicia, debe constreñirse a sus funciones legales: acreditar la presentación y devolución del documento electrónico privado a la parte que lo aporta, la transcripción en papel que se presente y la imposibilidad de confrontar uno con otro, dado el distinto contenido de ambos realidades, además de la falta de conocimientos técnicos para hacerlo, para el caso -poco probable- de que se aportaran al completo los dos.

7º Para los supuestos, seguro más que frecuentes, que se acuerde la intervención del letrado judicial en la incorporación al procedimiento judicial de las comunicaciones mantenidas por mensajería instantánea, la única forma válida de hacerlo de acuerdo con la naturaleza jurídica de la actuación a realizar y de las funciones y potestades de aquéllos, será mediante la extensión de una diligencia de constancia que acredite y documente la comprobación y descripción del aparato móvil, el fichero de texto de los mensajes y su remisión e incorporación a la diligencia extendida.

6. Bibliografía

CARNELUTTI, F., La prueba civil, 2ª ed., Ejea, ed. Desalama, Buenos Aires, 2000.

MARTINEZ GUERRERO, ALFREDO. (2021). El carácter judicial de los letrados de la administración de justicia. Revista Acta Judicial. Nº 7

DELGADO MARTÍN, JOAQUÍN. “La prueba digital. Concepto, clases, aportación al proceso y valoración”. Diario La Ley. Nº 6. 11 de abril de 2017.

FUENTES SORIANO: El Whatsaap como fuente de prueba, Proceso Penal. Reflexiones. Tirant Lo Blanch, 2017.

RODRÍGUEZ LAINZ, JOSÉ LUIS. “Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2.^a, 300/2015, de 19 de mayo)”, Diario LA LEY, núm. 8569, Sección Doctrina, 25 Jun. 2015.

Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

Financiación

El documento ha sido elaborado sin financiación.

LOS PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL Y SUS IMPLICACIONES EN EL PROCESO PENAL

The principles relating to processing of personal data and their implications for criminal proceedings

Por Juan Alejandro Montoro Sánchez¹

Investigador Postdoctoral Margarita Salas. Universidad Pablo de Olavide de Sevilla. Instituto de Justicia y Litigación “Alonso Martínez” de la Universidad Carlos III de Madrid.
jamonsan@upo.es

Artículo recibido: 15/05/22 | Artículo aceptado: 19/07/22

RESUMEN

El presente trabajo aborda el estudio de los principios rectores del tratamiento de datos de carácter personal asociados al derecho fundamental a la protección de datos, desde la perspectiva del órgano judicial del orden penal, en tanto autoridad responsable del tratamiento de datos con fines de investigación y enjuiciamiento del delito. Se analizarán igualmente las principales implicaciones procesales que se derivan de su efectiva aplicación.

ABSTRACT

This paper analyses the fundamental right of data protection regarding its treatment by the criminal court, as the authority responsible for the processing of data for the purposes of investigation and prosecution of crimes. The main procedural implications deriving from its effective application will also be analyzed.

PALABRAS CLAVE

Derecho protección de datos, Principios rectores del tratamiento, Tratamiento de datos, Principio limitación de la finalidad, Proceso Penal.

KEYWORDS

Data Protection Right, Principles relating to processing of personal data, Processing of personal data, Purpose limitation principle, Criminal proceeding.

¹ Trabajo vinculado al Proyecto de Investigación de Excelencia del Ministerio de Economía y Competitividad “Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea (LUDEI)”.

Sumario: 1. Los principios rectores del tratamiento de datos de carácter personal. 2. Principios de licitud y lealtad. 2.1 Principio de licitud. 2.2 Principio de lealtad. 3. Principio de limitación de la finalidad del tratamiento. 4. Principio de minimización. 5. Principio de exactitud. 6. Principio limitación del plazo de conservación. 7. Principios de integridad y confidencialidad. 8. Principio de responsabilidad activa o proactividad. 9. Bibliografía.

1. Los principios rectores del tratamiento de datos de carácter personal

Bajo el paraguas del Capítulo II de la Directiva 2016/680/UE, que tiene como rúbrica “Principios” se proclaman y desarrollan toda una serie de reglas y fundamentos heterogéneos² sobre los que se articula básicamente todo el régimen jurídico protector del derecho fundamental a la protección de datos de carácter personal en el ámbito penal³. Estos principios vertebradores constituyen el núcleo básico de las obligaciones de toda autoridad responsable de un fichero, que deben ser observados minuciosa y diligentemente a lo largo de todas las fases del tratamiento⁴, pues de su respeto y observancia depende, en gran medida, que se pueda garantizar adecuadamente a los interesados los poderes de

² APARICIO SALOM, J. La calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid, Civitas, 2010, p. 324, alude a la heterogeneidad de los principios, si bien, todos ellos contribuyen a un fin común, garantizar los poderes de control y disposición que atribuye al interesado el derecho fundamental a la protección de datos sobre sus propios datos.

³ Los primeros instrumentos jurídicos que fueron promulgados en la materia ya preveían una serie de principios básicos destinados a vertebrar los sistemas de protección de datos que configuraban. Las pioneras Resoluciones 22/73 y 29/74 del Consejo de Europa, referidas respectivamente a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos de los sectores privado y público proclamaron como principios informadores a la proporcionalidad, lealtad, licitud, finalidad, conservación y exactitud. De igual modo, el Convenio 108 dedicó sus arts. 4 a 7, comprendidos bajo su Título II sobre “Principios básicos para la protección de datos”, a fijar sus fundamentos estructurantes. Por su parte, la Directiva 95/46/CE los reconoció en su art. 6 bajo la expresiva denominación de principios relativos a la calidad de los datos. Por ello, puede comprobarse como ha sido una constante la existencia de estos principios en los instrumentos convencionales y legales de la materia y su posición privilegiada, en tanto elementos rectores e inspiradores de los sistemas de protección de datos.

⁴ Principios cuya observancia se debe procurar desde el mismo momento de la recogida de los datos hasta su supresión una vez concluya la finalidad para la que fueron recabados. Por lo tanto, el escrupuloso respeto de estos principios resulta esencial durante todas las fases o etapas del tratamiento y durante el desarrollo de cualquier actividad que se realice en la organización del responsable relacionada o vinculada al uso de los datos personales. TRONCOSO REIGADA, A. El principio de calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 340-343.

control y disposición⁵ sobre sus datos personales que atribuyen el derecho fundamental a la protección de datos reconocido tanto en el art. 18.4 CE⁶ como en el art. 8 de la CDFUE y del CEDH.

Tradicionalmente denominados como principios relativos a la calidad⁷ de los datos de carácter personal, consisten en una serie de directrices, prohibiciones y limitaciones estrechamente relacionadas y complementarias entre sí, que definen y condicionan la forma en la que los datos han de ser recabados y tratados con posterioridad por la autoridad responsable durante todo el ciclo de procesamiento⁸. Especialmente descriptiva de la función que están llamados a desempeñar es la definición recogida en la primigenia LORTAD⁹, en la que se expresaba que éstos "...definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y racionalidad de la utilización de los datos".

Son, por tanto, elementos de especial trascendencia para todos los operadores jurídicos implicados en el tratamiento¹⁰, incluidas las autoridades de

⁵ PUYOL MONTERO, J. Los principios del derecho a la protección de datos. En PIÑAR MAÑAS J. L. (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, 2016, p. 136.

⁶ La STC 292/2000 de 30 de noviembre, concretó el contenido basilar del derecho fundamental a la protección de datos afirmando que "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

⁷ En el RGPD y en la Directiva 2016/680/UE se califican meramente como "principios", mientras la Directiva 95/46/CE siendo más expresiva de su cometido los denominó como "principios relativos a la calidad de los datos" tal y como se reflejaba en el título dado a la Sección 1ª del Capítulo II en los que se enmarcaban. Expresión que también fue trasladada a la derogada LOPD de 1999, pero que no se ha mantenido en su sucesora, la Ley Orgánica 3/2018, ni en la más reciente Ley Orgánica 7/2021.

⁸ PALMA ORTIGOSA afirma que para garantizar el derecho a la protección de datos no basta con reconocer a los interesados el ejercicio de los derechos ARSOPOL, sino que es necesario imponer a los responsables una serie de obligaciones adicionales que hagan efectiva en toda su extensión la protección dispensada por el derecho fundamental, lo cual se consigue a través del respeto debido a dichos principios vertebradores. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Editorial Reus, 2018, pp. 39-40.

⁹ Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

¹⁰ PUYOL MONTERO subraya la importancia de los principios vinculados a la calidad del siguiente modo: "porque los mismos han de servir de referencia a los operadores jurídicos que intervienen en la materia, a los efectos de que puedan cumplir de manera satisfactoria las

control que supervisan y controlan la adecuada aplicación de la normativa, pues se erigen en parámetros de referencia nuclear para la toma de decisiones en el seno de la organización y para garantizar una respuesta respetuosa con los derechos fundamentales a los interesados¹¹. Incluso, es posible afirmar que actúan como auténticos principios informadores de la normativa, habida cuenta de que permiten extraer criterios con los que cubrir las lagunas normativas que puede surgir ante la ausencia de soluciones específicas que cubran supuestos de hechos controvertidos. Por su parte, para los interesados, estos principios actúan como variables de referencia permitiendo valorar la adecuación del tratamiento llevado a cabo por la autoridad, a las exigencias que dimanen del derecho a la protección de datos y su regulación.

Es el primero de los apartados del art. 4 de la Directiva 2016/680/UE, que tiene por título “Principios relativos al tratamiento de datos personales”¹², el precepto encargado de proclamar a los principios operantes en el sistema de protección de datos del ámbito penal. En particular, se reconocen como tales a los principios de licitud y lealtad; al principio de limitación de la finalidad del tratamiento; al principio de minimización de datos; al principio de exactitud; al principio de limitación del plazo de conservación; a los principios de integridad y confidencialidad y finalmente, al innovador principio de responsabilidad proactiva. Cabe mencionar que este precepto reproduce casi miméticamente los mismos principios enunciados en el Reglamento General de Protección de Datos, con la única excepción del principio de transparencia. Sin embargo, la falta de reconocimiento expreso en el articulado no impide que también resulte aplicable, habida cuenta de su reconocimiento explícito en el Considerando (26) de la Directiva¹³, aunque ciertamente, la intensidad de su eficacia es de mucho menor calado que en el régimen general, dadas las particularidades que presentan las actividades públicas vinculadas al sistema de represión del delito que se enmarcan en este ámbito.

Dicho listado de principios rectores del tratamiento ha sido incorporado al ordenamiento nacional a través del art. 6.1 de la Ley Orgánica 7/2021, de 26 de

exigencias jurídicas y de responsabilidad social empresarial vinculadas a las nuevas exigencias y requerimientos derivados de la protección de datos de carácter personal”. PUYOL MONTERO, J. Los principios del derecho a la protección de datos.... referencia 5 p. 136.

¹¹ APARICIO SALOM, J. La calidad de los datos... referencia 1 p. 335.

¹² Anteriormente en la LOPD y su reglamento de desarrollo sí se recogía expresamente la denominación de principios relativos a la calidad de los datos, en sus arts. 4 y 8 respectivamente.

¹³ Puede comprobarse que el Considerando (26) de la Directiva exige que todo tratamiento de datos personales sometido al mismo, además de ser lícito y leal, debe de reputarse transparente en relación con las personas físicas afectadas. Fórmula idéntica a la utilizada en el Reglamento General de Protección de Datos, aunque en la Directiva dicho principio no se eleve a la categoría de vertebrador del tratamiento.

mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, norma interna con la que el legislador ha procedido a la transposición de la Directiva 2016/680/UE, con un retraso superior a los cuatro años.

Tras la lectura del elenco de principios, es posible advertir que el grueso de éstos se mantiene intacto respecto al repertorio previsto en el anterior régimen encabezado por la Ley Orgánica 15/1999¹⁴, existiendo por tanto una vocación continuista respecto de los que podríamos tildar como principios arquetípicos del tratamiento de los datos de carácter personal. Sin embargo, es cierto que bien se ha previsto la incorporación de algún principio plenamente novedoso, como ha sucedido con el de responsabilidad proactiva, o bien se ha dado el caso de que elementos previamente vigentes en el orden anterior se han visto elevados expresamente al nivel de principios fundamentales de la materia, como sucede con los principios de integridad y confidencialidad.

A continuación, procede analizar individualmente a cada uno de estos principios al objeto de conocer su contenido, exigencias y alcance en lo que respecta al tratamiento de datos por parte de los órganos judiciales, en su condición de autoridades responsables del tratamiento, prestando especial atención a las implicaciones de índole procesal.

2. Principios de licitud y lealtad

Los primeros principios informadores del tratamiento de datos de carácter personal, se enuncian conjuntamente en el art. 4.1.a) de la Directiva 2016/680 y 6.1.a) de la Ley Orgánica 7/2021, al disponer este último que “Los datos personales serán tratados de manera lícita y leal”¹⁵. Nos hallamos ante dos principios consolidados y tradicionalmente incorporados en los textos

¹⁴ La doctrina ha destacado el carácter continuista del legislador europeo respecto a los principios que se dispusieron en la Directiva 95/46/CE y consecuentemente, los reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vid. PUYOL MONTERO, J. Los principios del derecho a la protección de datos.... referencia 5, p. 137. Por su parte, PALMA ORTIGOSA, destaca, además, que, en el nuevo paquete normativo de 2016, el legislador europeo ha aclarado y sistematizado la regulación atinente a los principios rectores, añadiendo alguno de suma importancia como el de responsabilidad activa. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales... referencia 8 p. 40.

¹⁵ Aunque la derogada LOPD no hacía mención a los mismos, el art. 8 del Reglamento LOPD fue la norma nacional encargada de proclamarlos. En concreto la disposición reglamentaria aún vigente, aunque inoperativa, establece que “Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos”. Ello en plena sintonía con lo preceptuado en la Directiva 95/46/CE, que en su art. 6.1 obligaba a los Estados miembros a disponer que los datos personales fueran tratados de manera leal y lícita.

convencionales más vetustos e importantes sobre la materia. No en vano, el Convenio 108, ya hacía referencia a los mismos al preceptuar que los datos personales “Se obtendrán y tratarán leal y legítimamente”, mientras el art. 8 del CDFUE, determina que los datos “...se tratarán de modo leal (...) y sobre la base del consentimiento (...) o de otro fundamento legítimo previsto por la ley”. Procede analizarlos de forma individualizada.

2.1 Principio de licitud

En el ámbito de aplicación del RGPD, el principio de licitud exige, en primer lugar, que cualquier tratamiento de datos que se efectúe por un responsable del tratamiento se ampare en una base legal habilitante de las enumeradas en su art. 6 y, en segunda instancia, que además dicho tratamiento se circunscriba en todo momento a las previsiones y obligaciones derivadas de la normativa reguladora del derecho a la protección de datos que resulte de aplicación.

Sin embargo, en el ámbito de la Directiva 2016/680/UE este principio presenta una serie de exigencias y connotaciones específicas que impiden equipararlos plenamente. Y ello se debe en gran medida, al hecho de que no nos situamos ante una norma que establezca un régimen jurídico garantista de vocación general que deba comprender cualquier actividad dirigida al tratamiento de datos, tal y como sucede con el RGPD, sino ante un régimen excepcional referido exclusivamente al tratamiento asociado a las actividades estatales vinculadas al sistema de represión penal, como acertadamente afirma GALÁN MUÑOZ¹⁶.

En concreto, es el art. 8 de la Directiva 2016/680/UE el que conceptúa y configura a este principio rector. Y lo hace, obligando a los Estados miembros a

¹⁶ GALÁN MUÑOZ habla de una doble vía europea de protección de los datos personales, distinguiendo entre “la vía garantista general, en orden a preservar ante la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición; y, la vía excepcional o especial, la relacionada con la represión, la investigación y el enjuiciamiento del delito, que requiere un tratamiento especial en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo en orden a la imposición de consecuencias jurídicas sancionadoras de naturaleza penal”. Vid. GALÁN MUÑOZ, A. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. En COLOMER HERNÁNDEZ, I. (dir.) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Cizur Menor: Aranzadi, 2015, pp. 43-44. En idéntico sentido, GONZÁLEZ CANO, M. I., Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. En *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, Brasil, p. 1363 y SOLAR CALVO, P. La doble vía europea en protección de datos. En *Diario La Ley*, núm. 7832, 2012, España, p. 3.

que dispongan en su ordenamiento interno, que únicamente sea lícito “el tratamiento en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1¹⁷, y esté basado en el Derecho de la Unión o del Estado miembro”. Mandato que conecta y debe interpretarse a su vez con las directrices dispuestas en su Considerando (11), que disponen que “Para que sea lícito, el tratamiento de datos personales en virtud de la presente Directiva debe ser necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente en virtud del Derecho de la Unión o de un Estado miembro con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública”¹⁸.

Así las cosas, la licitud del tratamiento de datos personales en el ámbito penal va a depender de la verificación conjunta de tres factores imprescindibles: 1) la contribución del tratamiento a alguno de los fines de la Directiva, como elemento teleológico; 2) la naturaleza del responsable, como factor subjetivo y; 3) la habilitación legal de la autoridad para el tratamiento, como factor legitimador. Dicho, en otros términos, el tratamiento de datos será lícito, en tanto se circunscriba a alguno de los fines referidos al ámbito de aplicación de la Directiva y se acometa por una autoridad competente habilitada legalmente para el tratamiento de datos a tales efectos¹⁹.

De este modo, la finalidad del tratamiento debe coincidir necesariamente con alguna de las señaladas en el primero de los preceptos de la Directiva, y que se relacionan con el ámbito penal y la seguridad pública, recordemos nuevamente: la prevención, investigación, detección o enjuiciamiento de

¹⁷ Tales fines son, de acuerdo con dicho precepto, la “prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública”.

¹⁸ Puede rechazarse de plano que el consentimiento, en los términos exigidos en el RGPD, pueda constituir un fundamento para el tratamiento por las autoridades competentes, pues como reza el Considerando (35) de la Directiva: “En este caso, el consentimiento del interesado [según se define en el Reglamento (UE) 2016/679] no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes. El ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de infracciones penales que la legislación atribuye institucionalmente a las autoridades competentes permite a estas exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan. Cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad”.

¹⁹ Véase que el mandato establecido en el art. 8 de la Directiva 2016/680/UE se ha materializado en el art. 11 de la Ley Orgánica 7/2021, disponiéndose que “El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones”.

infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Por tanto, se exige del tratamiento que sea necesario o coadyuve a la consecución de alguno de estos fines, o dicho de otro modo, que se lleve a cabo en el marco de alguna de dichas actividades públicas, puesto que únicamente en tal medida, puede colmarse la primera de las exigencias del principio de licitud.

Por otro lado, no puede obviarse, que todas y cada una de las actividades que integran el ámbito de la Directiva, constituyen por sí mismas el ejercicio de una función de interés público general, tal y como exige el precitado Considerando (11) Directiva 2016/680/UE. Y ello porque contribuyen a la consecución de intereses colectivos o supraindividuales²⁰ como la aplicación del *ius puniendi* por el Estado y el mantenimiento de la libertad y seguridad públicas²¹.

El segundo de los requisitos de licitud lo constituye la identificación del responsable con la de una autoridad competente, únicos sujetos legitimados para tratar datos de carácter personal con alguno de los fines penales que abarca la Directiva. De acuerdo con las definiciones dispuestas en el apartado 7º de su art. 3, tienen dicha consideración: las autoridades públicas competentes para alguno de los fines del art. 1, así como cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas con alguno de los fines de la norma²². Vista la primera

²⁰ La jurisprudencia del TJUE ha declarado que la lucha contra el terrorismo y frente a otros delitos especialmente graves para el mantenimiento de la paz y la seguridad son objetivo de interés general de la Unión. En este sentido, las sentencias Tribunal de Justicia de la Unión Europea, caso Kadi y Al Barakaat International Foundation/Consejo y Comisión (C-402/05 P y C-415/05 P), 3 de septiembre de 2008, apartado 363, y caso Al-Aqsa/Consejo (C-539/10 P y C-550/10 P), 15 de noviembre de 2012, apartado 130.

²¹ MORENO CATENA, V. y CORTÉS DOMÍNGUEZ, V. *Derecho Procesal Penal*. Valencia: Tirant Lo Blanch, 2021, p. 13, consideran al “proceso penal como el instrumento último de la política pública de seguridad y además como medio de reparación de las víctimas”. En idéntico sentido, RÍO LABARTHE, G. El proceso penal. Funciones. En ASENSIO MELLADO, J. M. (dir.) *Derecho procesal penal*. Valencia: Tirant Lo Blanch, 2020, p. 27. El TC sitúa a la persecución y castigo del delito como bienes constitucionalmente protegibles y de interés público pues a través de ellos “...se defienden otros como la paz social y la seguridad ciudadana. Bienes que igualmente reconocidos en los arts. 10.1 y 104.1 CE. Al respecto las SSTC 292/2000 de 30 de noviembre FJ 6º; 166/1999, de 27 de septiembre, FJ 2º; y 127/2000, de 16 de mayo, FJ 3º. El TJUE también ha declarado que la lucha contra la delincuencia grave es esencial para garantizar la seguridad pública y libertad garantizada en el art. 6 de la CDFUE. Véase la sentencia, caso Tsakouridis (C-145/09), de 23 de noviembre de 2010, apartados 46 y 47.

²² El art. 4 de la Ley Orgánica 7/2021 reputa como autoridades competentes a las Fuerzas y Cuerpos de Seguridad; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria; al Servicio Ejecutivo de la

definición y habida cuenta de su competencia para la investigación de los hechos criminales en la fase de instrucción²³ y posterior enjuiciamiento y ejecución de penas, es indiscutible que los órganos judiciales del orden penal pueden reputarse como autoridades competentes a efectos de la Directiva. En cualquier caso, tal catalogación se confirma expresamente, despejando cualquier duda que pudiera suscitarse, en el segundo de los apartados del art. 4 de la Ley Orgánica 7/2021²⁴.

En último lugar, cabe examinar al último de los presupuestos que son exigidos por la Directiva 2016/680/UE para determinar la licitud y que se concreta en la reserva de ley habilitante para el tratamiento de datos. Es decir, la exigencia de que la autoridad esté expresamente habilitada en el ordenamiento interno para tratar datos de carácter personal con alguno de los fines amparados por la Directiva. Requisito que viene motivado por la necesaria adecuación de una medida restrictiva de derechos fundamentales a los cánones y parámetros de proporcionalidad y necesidad establecidos en la CDFUE y la jurisprudencia del TEDH²⁵. Y es que no debe obviarse, que toda recogida y/o posterior tratamiento de datos por una autoridad competente supone una injerencia en el derecho a la vida privada de las personas y a la protección de sus datos de carácter personal tal y como ha reiterado el TJUE en su jurisprudencia²⁶.

Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y a la Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

²³ Véase al respecto los apartados 1º y 2º del art. 303.1 LECrim, que encomiendan la formación del sumario, a los jueces de instrucción. Tales preceptos deben ponerse en correspondencia con las reglas de atribución de competencia establecidas en la LOPJ, especialmente sus arts. 57, 61, 73.3, 87 y 87 *ter*. Únicamente en el ámbito del derecho penal del menor, dicha labor corresponde al Ministerio Fiscal según lo previsto en la Ley Orgánica 5/2000.

²⁴ Este reza que “También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal”.

²⁵ FRÍAS MARTÍNEZ, E. Obtención de datos personales en procesos penales y administrativos. En *Diario La Ley*, núm. 9404, 2019, España, explica que se trata de una consecuencia de la exigencia plasmada en el art. 8.2 CEDH y que, en su virtud, “solamente podrá haber recogida y tratamiento de datos en aquellos supuestos en los que exista una ley habilitante, que se hagan para una investigación o con finalidad concreta y no prospectiva y sean proporcionados a la misma”.

²⁶ Las sentencias del Tribunal de Justicia de la Unión Europea, caso Schwarz (C-291/12), de 17 de octubre de 2013, apartado 25, y caso Digital Rights Ireland y otros (C-293/12 y C-594/12), de 8 de abril de 2014, apartado 36, recogen la doctrina jurisprudencial por la que se considera que se produce una injerencia los derechos a la protección de datos de carácter personal por el mero hecho de que un responsable trate datos personales, y ello con independencia de la operación en que consista éste, al expresar que “Dichas operaciones [comunicación, acceso, etc.] son asimismo constitutivas de una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, puesto que constituyen tratamientos de datos de carácter personal”. Dicha doctrina se confirma de modo específico, en lo que respecta a las autoridades competentes del orden penal en la sentencia del Tribunal de Justicia de la Unión

En el ámbito nacional, el fundamento legal primario que habilita a los órganos judiciales para el tratamiento de datos de carácter personal se encuentra implícito en el art. 117.3 CE²⁷, precepto que atribuye en exclusiva a los jueces y magistrados el ejercicio de la potestad jurisdiccional, siendo el procesamiento de datos una actividad inherente e inescindible de dicha función. No obstante, la habilitación específica para el tratamiento de datos en el desarrollo de estas funciones, y particularmente en lo que respecta al orden jurisdiccional penal, se halla en los apartados 2º y 3º del art. 236 ter LOPJ. Preceptos que genéricamente autorizan a los órganos judiciales del orden penal a tratar datos personales para el ejercicio de las funciones y potestades encuadrables en dicho orden jurisdiccional. No obstante, de modo adicional es posible localizar en la legislación procesal, o incluso en otras leyes especiales del ordenamiento jurídico, habilitaciones específicas para la utilización de ciertas categorías de datos, principalmente, con motivo de la regulación de determinadas actuaciones judiciales o medidas de investigación, que llevan aparejadas la aprehensión o recogida de datos. Piénsese en todas aquellas medidas de investigación limitativas de derechos fundamentales, especialmente las de índole tecnológica introducidas por en la LECrim por la Ley Orgánica 14/2015, que fueron incorporadas en sus arts. 588 bis a 588 octies, como son el registro de dispositivos de almacenamiento masivo, la utilización de dispositivos de geolocalización para el seguimiento o la cesión de datos de tráfico por los operadores de comunicaciones electrónicas, medida cuya regulación se complementa con las disposiciones establecidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En cualquier caso, debemos tener presente, que las habilitaciones genéricas establecidas en favor de los órganos judiciales que legitiman la obtención y uso de datos con fines penales, no amparan el procesamiento de cualquier modalidad de dato de carácter personal. Al contrario, hay ciertas

Europea, caso Ministerio Fiscal (C-207/16), 2 de octubre de 2018, en cuyo párrafo 51 se expresa que “En cuanto a la existencia de una injerencia en los derechos fundamentales, procede recordar que (...) el acceso de las autoridades públicas a estos datos constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales [véase, en este sentido, el Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada]”.

²⁷ DELGADO MARTÍN, J. Reflexiones sobre la protección de datos personales en la Administración de Justicia. En *Diario La Ley*, núm. 9363, 2019, España, p. 4.

categorías de datos, que por su naturaleza y la especial capacidad que presentan para revelar aspectos nucleares sobre la vida privada de las personas, requieren que la autoridad competente, cuente con una base legal específica legitimadora del tratamiento. Nos referimos a los denominados tradicionalmente como datos sensibles o pertenecientes a categorías especiales, tal y como se denominan en la más reciente legislación europea. Bajo esta denominación se encuadran, por ejemplo, los datos que revelen el origen étnico o racial del interesado; sus opiniones políticas, convicciones religiosas o filosóficas o la afiliación sindical; y los datos genéticos y biométricos, y los relativos a la salud o a la vida sexual. La utilización de estas modalidades de datos que gozan de una protección privilegiada requiere ineludiblemente que la autoridad responsable cuente con una autorización legal específica en el derecho interno para el uso específico de tales datos, tal y como se menciona en el art. 10 de la Directiva 2016/680/UE y en el art. 13.1 de la Ley Orgánica 13/2021²⁸. Por ello, la licitud del tratamiento de datos de tal naturaleza por un órgano judicial, dependerá de que cuente con una base con rango de ley que lo autorice expresamente a su tratamiento, de lo contrario únicamente, podrá reputarse lícito cuando resulte necesario para proteger los intereses vitales de una persona o cuando los datos se hubieran hecho manifiestamente públicos por el interesado, como prevén los preceptos previamente citados.

2.2 Principio de lealtad

Además de ser lícito, todo tratamiento de datos debe ser leal, esto es, ser respetuoso con el principio de lealtad. Este presupuesto implica, en términos generales, que el tratamiento debe efectuarse por el órgano judicial en consonancia con las exigencias derivadas del principio general de la buena fe, al que se encuentra íntimamente ligado.

Tales condicionantes repercutirán al tratamiento de datos personales desde una doble perspectiva. En primera instancia, desde una posición subjetiva que se traducirá en la necesaria confianza en la apariencia y en la ausencia de dolo que deben resultar de la autoridad mientras se prolongue el tratamiento. Ello implica que el interesado cuyos datos vayan a ser tratados debe esperar del órgano judicial que toda su actuación se encamine a garantizar los principios, derechos y garantías que la ley le reconoce²⁹. Ello se compadece con la función de

²⁸ Ejemplos de dichas habilitaciones específicas las encontramos en el art. 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica para el acceso al historial clínico o en el art. 95.1 de la Ley General Tributaria, respecto a los datos con trascendencia fiscal que conservan las Administraciones.

²⁹ Muy expresiva de esta dimensión es el art. 6.1 de la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad, en relación con el

garante de los derechos fundamentales que cumplen los jueces y magistrados, especialmente durante la fase de instrucción.

En segundo lugar, el principio de la lealtad se manifiesta desde una perspectiva objetiva en la observancia de unas reglas de conducta social que imponen a la autoridad responsable un determinado comportamiento ético en su relación jurídica con el interesado, en la que deberán destacar especialmente la honradez y rectitud³⁰. Se trata, en definitiva, de evitar que la autoridad responsable pueda ejecutar operaciones de tratamiento de datos personales a espaldas del interesado, ya fuere de forma engañosa, prospectiva, clandestina, subrepticia o encubierta. Al contrario, el principio de lealtad persigue que el interesado deba tener constancia fehaciente, clara e inequívoca de que sus datos van a ser tratados, para qué concretos fines y bajo qué condiciones³¹, debiendo la autoridad contribuir activamente a la consecución de este objetivo, primordialmente a través del cumplimiento del deber de prestar información³²

tratamiento de datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, que en referencia a al principio de lealtad estableció que “Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos”.

³⁰ Este aspecto objetivo de la buena fe se traduce en una exigencia de rectitud, lealtad y honradez en el trato, que la ética social aprueba y considera como razonablemente exigibles. Por tanto, la lealtad “debe presidir con carácter general la actuación individual del responsable del fichero, siendo un parámetro objetivo que debe ser tenido en cuenta a la hora de valorar su conducta respecto al cumplimiento de sus obligaciones”. Vid. ATAZ LÓPEZ, J. La buena fe contractual. En Bercovitz RODRÍGUEZ-CANO, R., MORALEJO IMBERNÓN, N. y QUICIOS MOLINA, M. S. (coord.) *Tratado de los Contratos*. Valencia, Tirant Lo Blanch 2009, p. 167. En el mismo sentido PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales referencia 8, p. 49.

³¹ Esta dimensión informativa del principio de lealtad ha sido reconocida tanto por la AEPD como por la jurisprudencia. Por ejemplo, en las resoluciones recaídas en los procedimientos E/01490/2016, PS-00275-2016 y AAPP-00044-2015 la autoridad de control declaró que el principio de lealtad “se encuentra en el prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta”. Por su parte, la sentencia de la Audiencia Nacional de 13 septiembre 2002, destacó que “(...) el tratamiento de datos no debe ser solamente legal, sino también leal, e implícito en dicho deber de lealtad se encuentra el de prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta”.

³² Es patente que el principio de lealtad se encuentra inexorablemente vinculado al derecho/deber de información, puesto que este es el medio principal por el que el interesado adquiere constancia, no solo de la inminencia o preexistencia de un tratamiento de sus datos, sino de sus características, fines, de las circunstancias del responsable y de los medios de impugnación. Por ello, el Considerando (42) de la Directiva 2016/680/UE preceptúa que, a fin de garantizar un tratamiento leal “Debe informarse al interesado, como mínimo, de lo siguiente: la

completa y veraz en los términos planteados en el art. 13 de la Directiva 2016/680/UE y 21 Ley Orgánica 7/2021. Todo ello sin perjuicio de los supuestos legalmente establecidos en que el órgano judicial pueda retrasar o limitar el cumplimiento de dicho deber en aras de no perjudicar la investigación en curso.

Por lo expuesto, la lealtad se erige en un estándar jurídico de obligada observancia a toda la actividad vinculada al tratamiento de datos llevada a cabo por la autoridad judicial, implicando de manera genérica, que su propia actuación tenderá a garantizar las exigencias derivadas del derecho a la protección de datos en favor de los interesados³³, absteniéndose de efectuar cualquiera de las actividades comprendidas en el tratamiento de datos personales mediante prácticas engañosas, fraudulentas o ilícitas³⁴ o que puedan generar un efecto negativo o injustificado³⁵.

3. Principio de limitación de la finalidad del tratamiento

El siguiente de los principios informadores vinculados al derecho a la protección de datos es el denominado como principio de limitación de la finalidad del tratamiento. Se trata de un principio esencial que podría calificarse como la clave de bóveda del sistema protector del derecho a la protección de datos. Se reconoce en el art. 4.1.b) de la Directiva 2016/680/UE y en el ámbito interno ha sido transpuesto a través del art. 6.1.b) Ley Orgánica 7/2021 bajo la fórmula: “Los datos personales serán recogidos con fines determinados,

identidad del responsable del tratamiento, la existencia de la operación de tratamiento, los fines del tratamiento, el derecho a presentar una reclamación y el derecho a solicitar al responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, o la limitación de su tratamiento (...) Además, en determinados casos y con el fin de permitir que ejerza sus derechos, debe informarse al interesado de la base jurídica en la que se fundamenta el tratamiento y del período durante el que se conservarán los datos, siempre que dicha información adicional resulte necesaria y habida cuenta de las circunstancias concretas en que se produce el tratamiento de los datos...”.

³³ En sentido similar se pronuncia el art. 15.2 de los Estándares de Protección de Datos para los Estados Iberoamericanos, al establecer que “el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos”. Asimismo, la LOPD y el RLOPD, prohibían expresamente “la recogida de datos por medios fraudulentos, desleales o ilícitos” ex art. 4.7 y 8.1 respectivamente.

³⁴ En sentido contrario, una actuación desleal, podría considerarse aquella seguida en el tratamiento de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares, como señala el criterio interpretativo incluido en el art. 15.1 de los Estándares de Protección de Datos para los Estados Iberoamericanos.

³⁵ PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales... referencia 8, p. 49, colige que de este precepto debe derivarse una actitud honesta y abierta del responsable respecto a los datos que tratando de no causar efectos negativos en los interesados.

explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines”.

Debe partirse de que la recogida de cualquier dato personal - ya sea directamente del propio interesado o de otra fuente alternativa- y su posterior tratamiento deben obedecer, necesariamente, a la consecución de uno o varios fines perfectamente definidos. Es decir, el procesamiento de datos por la autoridad judicial es viable cuando se constituya como condición indispensable – ya sea principal o accesoria- para la obtención de un propósito circunscrito necesariamente al ámbito de aplicación de la Ley Orgánica 7/2021. Por tal motivo, se excluye la posibilidad de llevar a cabo la utilización de datos que no contribuyan o coadyuven a la consecución de unos propósitos concretos, como pudiera ser la mera acumulación gratuita o prospectiva de datos, actuaciones vedadas igualmente por el principio de especialidad proclamado en el art. 588 bis a) LECrim.

El concepto teleológico de fines o finalidad que se contempla en la Directiva 2016/680/UE – e igualmente en la Ley Orgánica 7/2021- adquiere en este ámbito mayores connotaciones que el incorporado en el RGPD. Concretamente, dicho concepto opera con dos sentidos distintos que resulta imprescindible distinguir a efectos de dilucidar el alcance y efectos del principio rector. Por un lado, podemos distinguir a los fines en sentido amplio, con los que se alude de forma genérica a los fines de interés general y actividades propias de las autoridades competentes que determinan el ámbito de aplicación de la Directiva. Esto es, a los fines que son propios de las autoridades competentes en virtud de las competencias genéricas que le son atribuidas *ope legis* y que sirven de fundamento legal a la licitud del tratamiento, a saber: fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Y de otro lado, los fines entendidos de forma específica o concreta. Es decir, al particular cometido que desarrolla la autoridad responsable al que se dirige el tratamiento de datos. Por ello, estos fines coincidirán con un concreto delito o riesgo para la seguridad pública que se pretende prevenir, atajar, investigar o enjuiciar. Pues bien, consideramos que es ésta última concepción del término “fines” a la que se refiere necesariamente el principio de limitación de la finalidad del tratamiento, pues es la única interpretación que resulta coherente de un análisis sistemático de la Directiva y especialmente de sus objetivos³⁶.

³⁶ Esta diferenciación se deduce especialmente de los Considerando (26) y (29) en relación con el art. 4.2 Directiva 2016/680/UE. Pues se observa como utiliza fines en sentido genérico y fines específicos con distinto sentido. Uno para referirse a los fines previstos en ley y otra para los fines específicos a los que obedezca el tratamiento por lo que deben determinarse con carácter

Estando analizando en este trabajo, de modo específico el tratamiento de datos por los órganos judiciales pertenecientes al orden penal, es posible concretar que: cuando éstos procesen datos personales, lo harán exclusivamente y en la medida en que sea necesario para la consecución de unos fines específicos, que se enmarquen, a su vez, dentro de unos fines generales. Por ejemplo, un Juzgado de Instrucción recopila y procesa datos para investigar (fines generales) un delito de robo cometido por A.A.A. frente a B.B.B (fines concretos). O un Juzgado de lo Penal recibe del Juzgado de Instrucción el anterior expediente del delito de robo (fines concretos), para ser enjuiciado (fines genéricos).

Si bien la atribución de la competencia a las autoridades para la realización de los fines genéricos en los que se enmarca el tratamiento de datos se prefijan a través de la ley, los fines concretos, se definen por la propia autoridad competente, generalmente, con carácter previo a la hora de obtenerse los datos. En el caso de los órganos judiciales mediante el dictado de la oportuna resolución que bien incoa la fase de instrucción o bien mediante la resolución de apertura del juicio oral. Fijados estos fines específicos, el tratamiento de los datos debe someterse con exclusividad a los mismos, hasta el punto de erigirse en un límite, *a priori*, infranqueable durante todo el ciclo de vida de los datos³⁷. Por consiguiente, es imprescindible que el órgano judicial delimite de antemano y con suficiente precisión, los fines a los que se destinarán los datos personales que se requieran obtener durante la instrucción, hasta el punto de que dicha determinación se erige en una suerte de autovinculación que impide, salvo bajo determinadas circunstancias extraordinarias, alterar o extender el ámbito finalista del tratamiento. Entre dichas causas, podemos señalar, por ejemplo, el descubrimiento de delitos conexos a los inicialmente investigados o de hallazgos casuales, pero al margen de estos supuestos, la mutación del destino de los datos queda proscrita en virtud de dicho principio.

De lo anterior, se deriva la necesidad de que los fines a los que responda el tratamiento sean explícitos, esto es que se expresen de una manera clara, transparente, determinante, unívoca y que sean puestos en conocimiento del interesado a través de los cauces informativos previstos –tanto en la legislación procesal como en la sectorial de protección de datos–, sin que proceda la persecución de otros fines encubiertos, solapados o ambiguos³⁸. Igualmente, y

previo a su recopilación. Debiendo ser adecuados y no excesivos, lo que exige una valoración respecto a los fines específicos, no es posible *ex ante*, al menos en el plano penal, la delimitación de los datos que pueden servir para la tramitación de un proceso penal, sino que dependerá en exclusiva de las circunstancias y particularidades que resulten del asunto.

³⁷ TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 344.

³⁸ Lo determinante es que al interesado no le queden dudas de la concreta y exacta finalidad para la que se destinarán sus datos personales y que dará lugar al tratamiento, pues esta

como regla complementaria y delimitadora de las anteriores, se exige que los fines perseguidos por la autoridad judicial responsable respondan al principio de legitimidad. Esto implica en primer lugar que los fines para los cuales se recaban los datos personales deben ser lícitos, esto es, que la finalidad a la que se destinan los datos debe estar amparada por la ley³⁹; y en segunda instancia, que la autoridad debe estar legitimada para la realización de la misma⁴⁰. Por tanto, todo tratamiento de datos cuya finalidad sea contraria a las normas o para la que no esté amparada la autoridad será ilegítima y vulnerará el presente principio, incluso, cuando los datos pudieran resultar adecuados a la finalidad.

Sin perjuicio lo anterior, lo cierto es que, el principio de limitación de la finalidad habilita de forma directa y automática y sin requisito adicional a una autoridad responsable a tratar datos para nuevos fines, cuando éstos no resulten incompatibles con los previos. Véase como el precepto que proclama este principio, prevé *in fine* que “[los datos] no serán tratados de forma incompatible con esos fines”, máxima que, interpretada a *sensu contrario*, infiere su destino a usos compatibles.

Bajo nuestro parecer, la compatibilidad resultará cuando la nueva finalidad se utilice como complemento necesario a la finalidad originaria específica. Dicho en otros términos, se reputa compatible el destino de los datos a las sucesivas fases que integran el proceso penal, entendido éste en sentido lato. De este modo, siempre que los datos se dediquen a nuevos fines de los generales plasmados en el art. 1 de la Directiva 2016/680/UE, más vinculados, derivados y accesorios o complementarios a los fines específicos existirá compatibilidad de usos. Por

claridad permite el ejercicio de las facultades de control y disposición con plenitud. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales... referencia 8, p. 44. Por tal motivo TRONCOSO REIGADA considera que es contraria a este principio la determinación de finalidades vagas, inconcretas o excesivamente generales, aunque ésta fueran legítimas. TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 345. APARICIO SALOM, clarifica esta concepción amplia de la finalidad, distinguiendo a la finalidad de las actuaciones concretas que se desarrollen en ejecución de la actividad. APARICIO SALOM, J. La calidad de los datos... referencia 1, p. 329.

³⁹ El término ley deberá de ser interpretado en sentido amplio, como cualquier disposición del ordenamiento jurídico que faculte, permita o ampare una concreta actividad para la que se desarrolle el tratamiento de datos. Vid. PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales... referencia 8, p. 44. TRONCOSO REIGADA añade que para que una finalidad sea legítima, debe de ajustarse en primer lugar a la Constitución y posteriormente a la ley. VID. TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 345

⁴⁰ Legitimidad por tanto referida al sujeto respecto a los fines. TRONCOSO considera que este requisito se cumpliría para personas jurídicas privadas si las finalidades de tratamiento de datos se encuadran el objeto social o la actividad que desarrolla habitualmente, mientras que, en el supuesto de los entes públicos, es imprescindible que la finalidad responda a una competencia previamente otorgada por el ordenamiento, identificándose el principio de finalidad con los principios de competencia y de reserva.

ejemplo, cuando los datos sean recopilados por una autoridad policial para la investigación preprocesal, podrán ser cedidos al órgano judicial de instrucción para el desarrollo de la instrucción y, a su vez, éstos podrán ser cedidos al juzgado de lo Penal o Audiencia Provincial para el enjuiciamiento, para finalmente ser comunicados al juzgado de Vigilancia Penitenciaria para la ejecución de la pena. Puede verse como, a pesar de sucederse varias comunicaciones de datos entre diferentes responsables y destinarse a varios fines genéricos – investigación policial, investigación judicial, enjuiciamiento y ejecución- todos ellos guardan relación con los fines específicos que dieron lugar al tratamiento inicial en el ámbito de la Directiva. Sin embargo, cuando unos datos fueron obtenidos inicialmente para la investigación o enjuiciamiento de unos hechos específicos y, posteriormente se ceden por el órgano judicial a fin de investigar o enjuiciar otros delitos ni siquiera conexos, se estaría produciendo un tratamiento incompatible, no amparado por el principio de limitación de la finalidad.

Ahora bien, la Ley Orgánica 7/2021 también establece excepciones de carácter relativo a este límite, a fin de permitir a una autoridad competente o incluso a una tercera, previa cesión, el tratamiento de los datos personales a otros fines específicos. Es decir, datos personales que son procesados por una autoridad competente para alguno de los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública respecto a unos hechos delictivos específicos, podrán ser destinados por esta a cualquiera de estos fines respecto a otros delitos o incluso ser comunicados a una tercera autoridad para que actúe en tal sentido. Posibilidad que también se contempla actualmente en los arts. 579 bis y 588 bis i) LECrim para los datos obtenidos por órganos judiciales. Aquí pues, sí que nos situamos ante una auténtica excepción al principio de finalidad, puesto que los fines que motivan el tratamiento se expanden y mutan necesariamente en su concepción específica, pudiendo afectar en el mismo sentido a su dimensión genérica.

Ahora bien, a pesar del contenido de este último precepto, las autoridades competentes no se encuentran legitimadas para ampliar o transmutar los fines del tratamiento en cualquier caso en que consideren que puede resultar útil para el ejercicio de las competencias que legalmente le sean atribuidas. La Directiva se encarga expresamente de limitar estas actuaciones, imponiendo requisitos que únicamente posibiliten la expansión del tratamiento cuando ello obedezca a situaciones de necesidad justificadas y sometidas a criterios de proporcionalidad. Por tanto, los señalados preceptos de la LECrim deben interpretarse conforme a las reglas establecidas en la Directiva y Ley Orgánica 7/2021, al menos, cuando

los medios de investigación o de prueba que se pretenden ceder, consistan en datos de carácter personal.

Es el art. 4.2 de la Directiva – y 6.3 de la Ley Orgánica 7/2021- el que establece la regla excepcional al principio de limitación de la finalidad que permite a las autoridades competentes que puedan destinar los datos, por sí mismas o a una tercera, previa cesión, para su utilización en unos fines penales distintos y desconectados de los que motivaron su uso. Es decir, lo que la normativa legitima, es ni más ni menos, el empleo de datos que se recogieron a efectos de ser utilizados con relación a un delito, con respecto a otro delito distinto. En cualquier caso, para que esta cesión de datos se repute legítima, habida cuenta de la pérdida de ineficacia que se deriva para el principio de limitación, se requiere que concurran acumuladamente los siguientes requisitos.

En primer lugar, que la autoridad que dedique los datos a una nueva finalidad esté legitimada, mediante ley, para desarrollar la actividad a la cual se destinan los datos. Es decir, la legislación del Estado miembro debe atribuir el ejercicio de competencias penales a la autoridad para el desarrollo de los fines genéricos a los que se destinan y de la que se derive la necesidad de tratamiento de datos⁴¹. Por ejemplo, cuando con motivo de un hallazgo casual, un Juzgado de Instrucción comunica los datos a otro órgano judicial de idéntica naturaleza, a efectos de que se despliegue la investigación, es imprescindible, que el cesionario de los datos esté legitimado por ley para la investigación del delito y, además, ostente competencia. Tal exigencia deriva de la garantía de reserva de ley de aquellas actividades que supongan una merma o limitación de aspectos esenciales de un derecho fundamental, como sucede en este caso con el derecho a la protección de datos.

En segundo lugar, el nuevo tratamiento pretendido debe ser necesario y proporcionado con relación a los nuevos fines. Es decir, no basta entonces con que la legislación atribuya a una autoridad la competencia genérica para ejercer ciertas funciones vinculadas a alguno de los fines del art. 1.1 de la Directiva y que exija, a su vez, el tratamiento de datos personales. Sino que atribuida *ex lege* la competencia, el ejercicio puntual de ésta que abarque nuevos usos o cesiones para finalidades distintas que se pretendan llevar a cabo, deberá superar individualmente el estricto filtro de un juicio de proporcionalidad. Es decir, en el ámbito que nos ocupa, cada cesión de datos para un nuevo uso, deberá ser sometida *ex ante* por la autoridad cedente a un examen de adecuación a los criterios de necesidad, proporcionalidad y aquellos otros condicionantes adicionales que la legislación procesal pueda plantear.

4. Principio de minimización

⁴¹ Considerando (29) Directiva 2016/680/UE.

El principio de minimización⁴² de los datos, se establece de forma idéntica en los arts. 4.1c) Directiva 2016/680/UE y 6.1.c) de la Ley Orgánica. En su virtud, los datos personales que se traten por una autoridad penal deben de ser “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados⁴³”. Como puede comprobarse, mediante este principio se persigue minimizar, en la medida de lo posible, el número de datos personales que se tratan con relación a una concreta finalidad. Por ello, la autoridad debe de ceñirse, de modo estricto, a la recopilación y utilización de aquellos datos imprescindibles que posibiliten lograr la finalidad perseguida. De esta manera, se consigue reducir el riesgo de afección sobre aquella parcela de datos personales superfluos que se evitan ser tratados⁴⁴. Se trata, por tanto, de una limitación que afecta a la actividad que desarrolla la autoridad responsable, tanto a nivel cuantitativo como cualitativo⁴⁵.

La primera regla que deben cumplir los datos personales que se utilicen para un tratamiento de datos por mor de este principio básico del derecho a la autodeterminación informativa son las de adecuación⁴⁶ y pertinencia⁴⁷. Elementos que implican en primer lugar que los datos deben ser apropiados para el tratamiento y además tener cierta relevancia⁴⁸ para el alcance del fin perseguido respectivamente.

⁴² TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 344 y PUYOL MONTERO, J. Los principios del derecho a la protección de datos... referencia 5, p. 138, denominan a este principio como de adecuación.

⁴³ Dicha regla puede considerarse análoga a la de proporcionalidad prevista en la derogada LOPD. Esta obligaba al responsable a que los datos fueran adecuados, pertinentes y no excesivos en relación con la finalidad perseguida y el ámbito en el que se recabaron. En cambio, la LORTAD aludía al principio de congruencia y racionalidad en su Exposición de Motivos, el cual garantizaba que los datos solo pudieran ser usados cuando lo justificara la finalidad para la que fueron recabados. Su observancia resultaba capital para evitar la difusión incontrolada de la información y garantizar el poder de control de los interesados sobre sus datos.

⁴⁴ Señala TRONCOSO REIGADA que mediante este principio se consigue frenar el conocimiento excesivo sobre el interesado que es posible conseguir mediante el tratamiento de sus datos, ya sea directamente o bien a través de técnicas avanzadas. Vid. TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 345.

⁴⁵ En virtud del Considerando (26) Directiva 2016/680/UE, la limitación a lo necesario debe ser evaluada tanto desde un punto de vista cuantitativo -volumen de datos-, como cualitativo -categoría de datos-.

⁴⁶ El concepto de adecuación se refiere a la eficacia del dato para conseguir la finalidad fijada del tratamiento, es decir, un dato será adecuado, cuando sea estrictamente necesario. Vid. PUYOL MONTERO, J. Los principios del derecho a la protección de datos... referencia 5, p. 138.

⁴⁷ Los datos serán pertinentes, cuando su recolección se encuentre plenamente justificada, en función de la naturaleza y la finalidad que se persigue por el tratamiento,

⁴⁸ TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, pp. 343-344 pone de relieve el debate doctrinal acerca del significado de estos subprincipios respecto al principio de calidad. Así mientras LUCAS MURILLO mantiene que ambos son términos

En segundo lugar, este principio conculca que los datos personales que se traten deben de limitarse a aquellos estrictamente necesarios en relación a los fines para los que son tratados. Vemos como por razón de la aplicación de estas máximas, los datos personales a tratar resultan restringidos fundamentalmente por la estricta necesidad que marquen los fines perseguidos⁴⁹ por el responsable del tratamiento, sin que sea posible exigir datos innecesarios o prescindibles, que no aporten ninguna utilidad para alcanzar los fines del tratamiento o que puedan ser sustituidos por otros menos invasivos. Por tanto, de no ser necesarios todo o parte de los datos personales, debe evitarse su tratamiento, tal y como reseña el Considerando 26 de la Directiva 2016/680/UE⁵⁰.

Así las cosas, en este momento histórico en el que el conocimiento, la acumulación de información y la ágil accesibilidad a los datos personales de la gran mayoría de los ciudadanos por el Estado constituye una realidad, limitar la recolección de los datos a aquellos que vienen justificados por la necesidad y pertinencia de la investigación o enjuiciamiento del delito, justifica que única y exclusivamente se recopilen aquellos datos que sean imprescindibles para la finalidad pretendida⁵¹.

sinónimos con pequeños matices que aluden a la idoneidad de los datos para la finalidad del tratamiento, mientras SÁNCHEZ BRAVO y HERRÁN ORTIZ, diferencian ambos elementos, considerando que su enunciación conjunta no responde a un interés de reforzar una idea, sino que a la necesidad de delimitar y definir realidades diferentes en relación con los datos personales, indicando que la adecuación hace referencia a la conexión del dato con la finalidad, mientras que la pertinencia con la exigencia de no solicitar más datos que los necesarios para cumplir el objetivo, criterio éste último con el que nos identificamos, en analogía a los requisitos de la prueba civil previstos en la Ley de Enjuiciamiento Civil. MURILLO DE LA CUEVA, P. *Informática y protección de datos personales*. Madrid: CEC, 1993, p. 65; HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales*. Madrid: Dykinson, 1999, p. 243 y SÁNCHEZ BRAVO, A. *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, 1998, p. 85.

⁴⁹ Por tanto, es la finalidad del tratamiento la que posibilita saber si los datos a recabar se ajustan a su logro desde el punto de vista de la causalidad, motivo por el que se convierte en el elemento clave para determinar la pertinencia o no de los datos. Vid. TRONCOSO REIGADA, A. *El principio de calidad de los datos...* referencia 4, p. 346.

⁵⁰ Esta indica que “Los datos personales solo deberían ser objeto de tratamiento si la finalidad del tratamiento no puede lograrse razonablemente por otros medios”.

⁵¹ Se establece, asimismo, junto a la adecuación y funcionalidad de los datos, una prohibición de exceso de los datos personales. Ello implica que debe reducirse el número de datos a tratar hasta el mínimo posible que permita seguir alcanzando la finalidad pretendida. Igualmente, de entre todos los datos personales que sirvan al cumplimiento de una misma finalidad, debe de optarse por el menos invasivo para la privacidad del interesado. Habida cuenta del desarrollo de técnicas especialmente intrusivas para los ciudadanos, es por lo que se exige en estos casos someter las opciones disponibles a un juicio de proporcionalidad de conformidad con las asentadas reglas establecidas por nuestro Tribunal Constitucional en su STC 207/1996, de 16 de diciembre.

En el ámbito del proceso penal, y principalmente en su fase de instrucción, dada su función recopiladora de medidas de investigación y fuentes de prueba para la preparación del juicio, el cumplimiento de este principio va a exigir, que en la medida de lo posible, el órgano judicial que pretenda obtener datos personales necesarios, delimite y acote cuantitativa y cualitativamente, en la medida de lo posible, siquiera relativamente o en base a ciertos criterios, la información cuya obtención se requiere. Esta concreción deberá de definirse necesariamente en la resolución judicial que acuerde la medida de investigación consistente en la aprehensión o recogida de datos.

Más complejo resulta el cumplimiento de dicho principio en los supuestos en los que se lleva a cabo una medida limitativa de derechos sobre soportes y dispositivos que almacenen o conserven importantes cantidades de información y datos de carácter personal, que impidan filtrar y discriminar, durante el propio registro inicial, los que presentan relevancia para el proceso. En estos supuestos, sería imprescindible articular en la Ley de Enjuiciamiento Criminal un procedimiento posterior al registro, con intervención de las partes implicadas, dirigida a determinar la información que debe ser objeto de expurgo por no resultar pertinente ni útil para la investigación. De este modo se conseguiría un mayor respeto al principio de adecuación y se evitaría, la acumulación gratuita de datos en manos de las autoridades con la tentación de utilización para otros fines distintos⁵².

5. Principio de exactitud

Los arts. 4.1.d) Directiva 2016/680/UE y 6.1.d) Ley Orgánica 7/2021 proclaman el principio de exactitud⁵³, como regla cuya observancia coadyuva a

⁵² “La conservación de datos personales con una determinada finalidad despierta el deseo de hacer uso de dichos datos con otros fines”. Con esta reveladora sentencia dio inicio el escrito de conclusiones de la Abogada General del TJUE de fecha 18 de julio de 2007 relativas a la cuestión prejudicial planteada por el Juzgado Mercantil núm.5 de Madrid en el caso Promusicae contra Telefónica de España S.A.U. (C-275/06), y en la que se pone de relieve los riesgos que se crean de la mera acumulación de datos de interesados.

⁵³ Principio que ya se dispuso en el Convenio 108 del Consejo de Europa, al proclamar en su art. 5.d) que los datos “serán exactos y si fuera necesario puestos al día”. La LORTAD, en su art. 4.3 recogía el principio tal que así “Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado”, aunque sin precisar el momento al que debía de referirse dicha situación. Por su parte, la Directiva 95/46/CE en términos similares a los del RGPD y la Directiva 2016/680/UE, establecía en su art. 6.1.c) la obligación de los Estados de disponer la obligación de que los datos personales fueren “exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas”. Y también la LOPD en los apartados 3º y 4º de su art. 4 proclamaba a este principio bajo los siguientes términos: “Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del

garantizar la calidad del dato⁵⁴. Ambos preceptos disponen que los datos personales tratados deberán ser “exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados”.

Esta regla, de la que se derivan varias implicaciones para la autoridad judicial, acarrea en primer término, la necesidad de que los datos que recoja y conserve en sus ficheros, con fines penales, sean en todo momento correctos⁵⁵ y/o que respondan fidedignamente a la realidad del interesado. En segundo término y como consecuencia de la anterior, que aquellos datos que por su propia naturaleza o características sean susceptibles de modificación o variación, deban de ser correctamente actualizados⁵⁶, si durante el curso del tratamiento son objeto de cambio, para reflejar en todo momento la veracidad, especialmente, si de los mismos se puede derivar alguna consecuencia jurídica.

De este modo, en caso de que los datos albergados en los ficheros no sean exactos, bien por no reflejar la realidad o bien por haber variado el valor del dato, la autoridad queda obligada a adoptar, sin dilaciones indebidas, todas las medidas razonables que sean necesarias para suprimir o actualizar los datos. Recaen, por tanto, en la autoridad judicial, las referidas tareas de control, supervisión, supresión y actualización de los datos personales de los afectados,

afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16”. Siendo posteriormente desarrollado en el RLOPD, a través del apartado 5º de su art. 8 estableciendo que “Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste. Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello (...)”.

⁵⁴ SANZ CALVO, L. Calidad de los datos. En LESMES SERRANO, C. (coord.) *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*. Valladolid: Lex Nova, 2008, p. 142.

⁵⁵ El RGPD alude al término exacto, lo que hace referencia a lo puntual, fiel y cabal, en relación con la realidad que el dato pretenda reflejar. Así, el dato es exacto cuando refleja lo que el titular del mismo quiere reflejar y es reconocido por en idénticos términos por el responsable. Vid. ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)*. Bilbao: Universidad del País Vasco, 2011, p. 236.

⁵⁶ El término actualizado, hace referencia a la correspondencia con el tiempo presente, por lo que deben aludir a la realidad del tiempo en que se tratan. ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)*... referencia 55, p. 236.

so pena de incumplimiento del principio de exactitud. Así las cosas, el responsable deberá en su caso, corregir el dato inexacto si existe una contradicción entre el registro conservado y realidad; actualizar el dato a su valor actual si el mismo ha sufrido una variación o, en su caso suprimir radicalmente el dato si no responde a la realidad y además no nos encontramos en ninguno de los anteriores supuestos.

Ahora bien, en este punto, hay que hacer varias precisiones. En primer lugar, se requiere diferenciar entre los datos obtenidos directamente del afectado de los datos que se obtienen de terceros, fuentes accesibles al público y otras autoridades. En el primero de los casos, dado que los datos a tratar son entregados libre y directamente por el interesado a la autoridad, los mismos pueden presumirse correctos y exactos, de forma análoga a la prevista en la Ley Orgánica 3/2018 para el régimen general. En estos supuestos, la autoridad judicial, no está obligada a llevar una verificación de los mismos, al menos cuando se soporten mediante algún medio idóneo para sustentarlos. Tan solo cuando se ponga de manifiesto por el propio interesado o a través de otro medio, la inexactitud del fichero deberá proceder su actualización. Todo ello, sin perjuicio de las facultades de control de la fiabilidad del dato que para este ámbito se atribuyen a la autoridad en el art. 7 de la Directiva 2016/680/UE y 10 de la Ley Orgánica 7/2021. De hecho, el primero de los apartados de este último precepto, obliga a las autoridades, a distinguir, en la medida de lo posible, entre los datos personales basados en hechos y los basados en apreciaciones personales. Sin embargo, para los supuestos en que los datos se obtienen de otras fuentes distintas del interesado, la autoridad deberá mostrar una especial diligencia a la hora de realizar el precitado análisis de calidad, procurando confirmar la realidad del dato y su fiabilidad objetiva.

Asimismo, como consecuencia de este principio, el art. 10 de la Ley Orgánica 7/2021, también ordena que las autoridades competentes deben adoptar cuantas medidas organizativas y técnicas razonables sean necesarias para garantizar que aquellos datos que no reúnan las cualidades vinculadas a la exactitud, esto es, que sean inexactos, incompletos o desactualizados, no sean comunicados ni puestos a disposición de terceros. De hecho, se les exige que si una vez consumada la transmisión de unos datos, se comprobara que los mismos no eran correctos, por adolecer de alguno de los defectos señalados con anterioridad, deberán de ponerlo en conocimiento inmediato del cesionario, con el objeto de que, según proceda, se rectifiquen, se supriman o se limite su tratamiento.

La anterior restricción de transmisión de datos no empece que aquellos no sustentados en hechos objetivos, sino en valoraciones subjetivas, puedan cederse a terceras autoridades. Para ello, además de cumplir con los requisitos ordinarios que se exigen para la cesión de datos entre autoridades, se deberá de incorporar

una valoración sobre la calidad, exactitud y estado de actualización de estos. Y ello con el fin de que la autoridad cesionaria pueda advertir el nivel de calidad y fiabilidad de los datos que recibe. A tal fin, la autoridad cedente tendrá la obligación, cuando ello sea factible, de controlar ex ante tales cualidades. No obstante, bajo nuestro punto de vista, dicha valoración debería ser objeto de transmisión, incluso en aquellas cesiones que tengan por objeto la cesión de datos objetivos que sean susceptibles de alteración por cualquier razón y no presenten un carácter puramente estático.

En conclusión, nos encontramos ante un principio esencial del derecho a la protección de datos, que aunque no ha sido abordado muy extensamente por la doctrina, es de especial relevancia, como ha destacado en algún pronunciamiento la jurisprudencia de la Audiencia Nacional⁵⁷, por contribuir con su cumplimiento la protección enérgica de los derechos del interesado, toda vez que su falta de verificación puede afectar negativamente al interesado, acarreándole perjuicios o inconvenientes de suma importancia, especialmente en determinados ámbitos⁵⁸.

6. Principio limitación del plazo de conservación

El principio de limitación del plazo de conservación⁵⁹ aparece regulado en el art. 4.1.e) de la Directiva 2016/680/UE y 6.1.e) de la Ley Orgánica 7/2021. En el primero de los preceptos, aparece formulado bajo la siguiente máxima: “Los datos personales serán: mantenidos de forma que se permita la identificación de

⁵⁷ España. Sentencia Audiencia Nacional de 28 de junio 2002, FJ 3º.

⁵⁸ TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 358.

⁵⁹ Principio que también se previó por el Consejo de Europa en el Convenio 108 bajo su art. 5.e) al precisar que los datos personales “se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario”. La LORTAD, por su parte, lo introdujo en el ordenamiento español expresando que los datos “no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados”. Posteriormente, la Directiva 95/46/CE lo configuró determinando que los *datos* “deberían ser conservados de forma que no permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente”, por lo que amplió la posibilidad de conservación más allá de la conclusión del tratamiento inicial a otros tratamientos que eventualmente pudieran desarrollarse con posterioridad. Asimismo, contempló la posibilidad de que dicho plazo se extendiera siempre que se tomaran las medidas adecuadas de seguridad y el tratamiento a realizar tuviera finalidad histórica, estadística o científica. La LOPD, siguiendo la senda de la norma a la que sucedió, proclamó el principio en su art. 4.5 mediante una regla similar, estableciendo que “Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados”.

los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales”⁶⁰.

En virtud de dicho principio, la autoridad judicial responsable del tratamiento debe de limitar de manera general el plazo de conservación de los datos personales mantenidos en los ficheros por el plazo imprescindible para el cumplimiento de la finalidad para la que fueron recogidos. Para conseguir tal objetivo, se exige que la autoridad competente establezca de antemano los plazos previstos o previsibles para su supresión, de acuerdo a los criterios adecuados para ello. Esta delimitación temporal, a pesar de que consta como elemento del derecho de información y debe ser comunicada al interesado cuando los datos son recogidos, no exige en todo caso una concreción *ab initio* exacta y perfecta del plazo por el que los datos van a ser tratados. Por ejemplo, el art. 8 de la Ley Orgánica 7/2021, sin prever plazos concretos o máximos de conservación, dispone la obligación de las autoridades de conservar los datos únicamente durante el tiempo necesario para cumplir los fines penales que estén desarrollando. Y es que, en el ámbito del proceso penal, no resulta controvertido que no es posible fijar los plazos de supresión de forma general con relación a cifras temporales cuantitativas, habida cuenta de la contingencia e incertidumbre en la duración y alcance del desarrollo de éstos. Y es que, aunque el art. 324 LECrim establezca un plazo máximo de instrucción, ésta puede ser objeto de prórroga, no existen plazos para la celebración del juicio oral y los posibles medios de impugnación existentes al alcance de las partes impiden determinar plazos temporales concretos.

Por ello, únicamente en el caso de que se pueda prever con certeza el mismo con anterioridad a acometer el tratamiento será necesaria su determinación precisa. Lo habitual, siendo regla igualmente válida a los efectos de cumplimiento de este principio, es que el responsable en cambio sí pueda determinar este periodo relativamente atendiendo a alguna circunstancia o exigencia legal. Así, en el ámbito de la Directiva 2016/680/UE, dichos plazos coinciden con el tiempo establecido en la legislación que obligue a conservar determinada información durante un concreto periodo⁶¹ o el plazo de

⁶⁰ En la Ley Orgánica 7/2021, se recoge bajo una redacción distinta, aunque con idéntico alcance: “Los datos personales serán conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados”.

⁶¹ Piénsese por ejemplo en las exigencias de conservación de los datos de tráfico y localización de las comunicaciones electrónicas a las que se someten los operadores de telecomunicaciones en virtud de lo dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, las previstas en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica referidas a la historia clínica o las derivadas de la normativa fiscal y de prevención del blanqueo de capitales.

prescripción o caducidad⁶² de las eventuales acciones que contemple el ordenamiento para la relación de la que subyace al tratamiento.

No obstante, lo anterior, sin perjuicio de que pueda extenderse la conservación de los datos personales en previsión del cumplimiento de aspectos secundarios o accesorios de los fines principales, por aplicación de este principio, los datos que sucesivamente vayan dejando de ser adecuados y pertinentes para la conclusión de aquellos que permanecen, no deberán seguir siendo conservados, lo que implica la obligación de la autoridad de proceder a su borrado definitivo. En caso contrario, es decir en todos aquellos supuestos en los que sea viable, siquiera relativamente mediante la aplicación de algún criterio predefinido, establecer dichos plazos de antemano por cualquier razón que impida determinar precisamente el periodo en que se prolongará el tratamiento, se hace necesaria que el responsable del tratamiento efectúe revisiones periódicas de los datos almacenados, con el objetivo de que aquellos datos que se compruebe que han devenido innecesarios para la finalidad dejen de ser conservados de forma que permitan la identificación de su titular.

En el ámbito aplicativo de la Directiva 2016/680/UE, dicha obligación se ha incorporado en el art. 8.2 de la Ley Orgánica 7/2021 disponiendo la necesidad de revisar, cada tres años, a lo sumo, y si fuere posible mediante tratamientos automatizados, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento que ejecutan. Para lo cual deben atender a factores como la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal.

La aplicación de este principio se complementa con una exigencia lógica y consecuente, que no puede ser otra que la obligación de la autoridad responsable del tratamiento de suprimir los datos personales una vez que han cumplido su función. Ciertamente, al contrario de lo que hiciera la derogada LOPD en su art. 4.5 al disponer que “Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados”, ni la Directiva 2016/680/UE ni la Ley

Troncoso precisa que el señalamiento de plazos es habitual en el ámbito del derecho administrativo, echando en falta la existencia de una norma que establezca plazos de conservación general de la información que fije los criterios de archivo y los procedimientos de expurgo. TRONCOSO REIGADA, A. El principio de calidad de los datos... referencia 4, p. 385.

⁶² PUYOL MONTERO expresa que la conservación de los datos siempre ha sido un tema polémico en función de la discrepancia existente entre los plazos que cubren las responsabilidades derivadas del propio tratamiento de los mismos, de aquellos que se vinculan a la prescripción de las acciones derivadas del negocio jurídico subyacente, sobre la base del cual se han recolectado dichos datos. PUYOL MONTERO, J. Los principios del derecho a la protección de datos... referencia 5, p. 139.

Orgánica 7/2021 prevén una regla análoga. En todo caso, la misma es posible deducirla de la lectura de los diferentes supuestos enumerados en 16.2 de la Directiva 2016/680/UE –23.2 de la Ley Orgánica 7/2021-, coincidentes con los casos en los que encaja la aplicación del derecho de supresión, en los que se encuentra implícita.

No obstante, lo anterior, debemos señalar que en la LECrim es posible encontrar ciertos plazos de naturaleza relativa que condicionan la limitación de la conservación de los datos. En particular, es el art. 588 bis k) LECrim el destinado a reglamentar la destrucción de registros, si bien, su aplicación se circunscribe *prima facie*, a los datos e información obtenidos a través de diligencias de investigación tecnológica. Sin perjuicio de que su aplicación pueda extenderse a la totalidad de los datos obrantes en un expediente, sería imprescindible, en aras de garantizar la seguridad jurídica y una aplicación efectiva de dicho principio, la introducción de una regulación específica de alcance general a cualquier dato, con independencia de la fuente de origen.

Este precepto, establece que una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, que habitualmente coincidirán con los de la Policía Judicial. Y ello sin perjuicio de que se conserve una copia bajo la custodia del Letrado de la Administración de Justicia. Dichas copias, serán igualmente destruidas, cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

En cualquier caso, para los casos en que dicha supresión no se lleve a cabo en los plazos estipulados o se prorrogue su cancelación, el art. 8.3 de la Ley Orgánica 7/2021 establece un plazo máximo absoluto y terminante de veinte años, que, en principio, no debe sobrepasarse. No obstante, éste pierde su carácter de plazo propio, al preverse ciertas causas que permiten la extensión del mismo, como, por ejemplo, que se incorporen en una causa abierta o se vinculen a un delito no prescrito o cuya ejecutoria no ha concluido. En cualquier caso, lo cierto es que acudir a dichos plazos máximos, debe ser en todo caso la excepción, al menos en el ámbito penal, debiendo entrar en juego rotundamente la regla general de operatividad del principio de limitación de la conservación, por el cual deben ser suprimidos los datos en los plazos marcados por la LECrim.

7. Principios de integridad y confidencialidad

La consagración de la integridad y confidencialidad – o seguridad⁶³- de los datos como auténticos principios informadores⁶⁴ del derecho a la protección de datos ha venido de la mano del nuevo paquete legislativo de protección de datos aprobado por la Unión Europea en 2016. Tanto la Directiva 2016/680/UE, como la Ley Orgánica 7/2021 como ley de transposición, preceptúan que los datos personales deben ser “tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas”⁶⁵.

De sendos principios dimana la obligación de la autoridad competente de dotar a los ficheros y a los sistemas – manuales o automatizados- utilizados en la organización para el desarrollo y ejecución de las actividades vinculadas al tratamiento, de una protección suficientemente adecuada para garantizar la seguridad de los datos personales que se conservan en sus ficheros⁶⁶. No es

⁶³ Como era denominado dicho principio en la Directiva 95/46/CE y la LOPD.

⁶⁴ La seguridad –tal y como se denominaba a la integridad y confidencialidad- se configuraba en la antigua Directiva 95/46/CE no directamente como principio, sino como un elemento condicionante de las actividades y sistemas vinculados al tratamiento de los datos del responsable. En cambio, la LOPD sí reconocía a ambos elementos como auténticos principios, al encuadrarlos bajo su Título II dedicado a la regulación de éstos. Muestra de ello es el pronunciamiento de la Audiencia Nacional, en su sentencia de fecha 09/05/2008, cuyo Fundamento de Derecho 2º comienza diciendo: “El art. 10 de la LOPD regula de forma individualizada el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos, lo que refleja la gran importancia que el legislador atribuye al mismo”.

⁶⁵ Puede apreciarse la incidencia del Convenio 108 en la redacción de este principio, toda vez que en su art. 7, se reconocía a la seguridad de los datos como principio básico, estableciéndose al efecto que “Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados”.

⁶⁶ El concepto de seguridad aplicado a un sistema de información, tal y como puede entenderse un fichero a efectos de la normativa de protección de datos, se describe en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, como “la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles”. Concepto que a su vez se conforma de cuatro dimensiones diferenciadas: la disponibilidad, propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren; la integridad, propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada; la confidencialidad, propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados y la autenticidad, propiedad o característica

posible obviar que de la existencia de brechas y fisuras de seguridad en la organización y en los sistemas de tratamiento de datos deriva en un riesgo para los derechos y libertades de las personas físicas cuya gravedad y probabilidad dependerá de la naturaleza, el alcance, el contexto y los fines del tratamiento de datos.

Por tal razón, a todo el sistema de protección de datos se le deben de aplicar las medidas de naturaleza técnica y organizativa apropiadas⁶⁷ que permitan garantizar en todo momento⁶⁸ la integridad⁶⁹ y la confidencialidad de los datos⁷⁰, debiendo evitarse específicamente supuestos tales como el

consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

⁶⁷ Obligación que se recoge en el art. 29 Directiva 2016/680/UE para autoridades competentes, cuando precisa que "... teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10". En mismo sentido se pronunciaba el art. 17 de la Directiva 95/46/CE, cuando requería la "aplicación de las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales". La LOPD también preceptuaba en su art. 9.1 que "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

⁶⁸ La legislación europea persigue que la seguridad se garantice incluso con carácter previo al comienzo del tratamiento, por tal motivo, establece como una de sus prioridades en cuanto a las medidas de seguridad, el cumplimiento *ab initio* de los principios de protección de datos desde el diseño y por defecto que se plasman en el art. 20 Directiva 2016/680/UE, que colaboran en la minimización de uso de datos y de los riesgos.

⁶⁹ Por integridad de un dato se debe entender el atributo o cualidad que permite considerar a la información como exacta, completa, homogénea, sólida y coherente, con la intención de los creadores del fichero. Esto es, los datos serán íntegros cuando mantenga las características de completitud y corrección. Esta cualidad, que va ligada al propio dato y no al lugar donde se almacena, se obtiene cuando se impide eficazmente que el contenido de un fichero se vea accidental o intencionalmente modificado, en base a su propio contenido o con ayuda de la inserción de nuevo o destruido total o parcialmente. Vid. MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, octubre 2012.

⁷⁰ Por confidencialidad, se debe entender la situación que permite acceder a un determinado dato de un fichero exclusivamente a la o las personas autorizadas para ello en función del cargo o puesto que desempeñan. La confidencialidad se rompe al acceder un tercero sin legitimación ni autorización por razón del cargo que desempeña, sea de manera voluntaria

tratamiento de datos no autorizado o ilícito, la pérdida accidental y el daño o destrucción de éstos.

Hasta la entrada en vigor del paquete legislativo de protección de datos, las concretas medidas técnicas y organizativas que debían de implantarse por el responsable del tratamiento en su organización se determinaban por vía reglamentaria en el RLOPD⁷¹, estableciéndose al efecto tres niveles diferenciados de protección, a aplicar, según el grado de sensibilidad que presentaran los datos personales objeto de tratamiento. No obstante, esta situación se ha visto alterada en el régimen vigente a raíz de la introducción del principio de responsabilidad activa o proactividad que será analizado en el epígrafe siguiente. Actualmente, de acuerdo con lo estipulado en los arts. 29 Directiva 2016/680/UE – art. 37 de la Ley Orgánica 7/2021 -, se obliga a los responsables y encargados del tratamiento, previa evaluación de los riesgos inherentes al tratamiento, especialmente para los derechos y libertades fundamentales, a adoptar aquellas medidas técnicas y organizativas necesarias para garantizar la integridad y confidencialidad de los datos, si bien facultándolos para que ellos mismos puedan seleccionar las que consideren oportunas, con la única condición de que sea apropiadas, adecuadas y suficientes para tales fines y se muestren respetuosas con los demás principios y obligaciones de la normativa y, muy especialmente, con los derechos y libertades de los interesados. Y es por este giro en la delegación de la capacidad de decidir del responsable sobre las concretas medidas de seguridad a adoptar,

por haber vulnerado las medidas de seguridad establecidas al efecto o involuntaria por no haberse establecido aquellas. Vid. MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, octubre 2012.

⁷¹ El régimen de las medidas de seguridad aplicables a los sistemas de tratamiento de datos se establecía anteriormente en el Título VIII del RLOPD, desarrollándose en sus arts. 79 a 114. Este marco clasificaba en tres niveles – bajo, medio y alto – las medidas de seguridad exigidas a los ficheros, enumerando las diferentes reglas que serían de aplicación a cada nivel diferenciando a su vez entre los ficheros manuales y los automatizados, y cuya aplicación era acumulativa, según se iba ascendiendo de categoría. De modo que a los ficheros que exigían una protección más elevada, se le aplicaban conjuntamente las medidas de los niveles alto, medio y bajo, mientras a los que merecían una protección más leve, tan solo se les deberían aplicar las de nivel bajo, ex art. 81 RLOPD. Aunque actualmente el marco dispuesto en el RLOPD no es directamente aplicable, constituye un elemento esencial para la guía y orientación de responsables en cuanto a la adopción de medidas en la organización. Vid. RIBAGORDA GARNACHO, A. Las medidas de seguridad en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal: Título II. Principios de la Protección de Datos. Artículo 9. en TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 735-761 y MARTÍNEZ MARTÍNEZ, R. Las medidas de seguridad. En MARTÍNEZ MARTÍNEZ, R. (coord.), *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Valencia: Tirant lo Blanch, 2009, pp. 89-119.

por lo que recae en éste la carga de demostrar su adecuación a la salvaguarda de seguridad del tratamiento de los datos personales.

No obstante, en el ámbito de aplicación de la Directiva 2016/680/UE, habida cuenta del desarrollo de una función eminentemente pública, como es la jurisdiccional, la libertad de maniobra de los órganos judiciales, en tanto responsables, no es tal, sino que viene establecida reglamentariamente por el Esquema Nacional de Seguridad y particularmente por el Esquema judicial de interoperabilidad y seguridad. En estas normas técnicas, se compaginan toda una serie de objetivos o medidas de obligada consecución o implantación que se relacionan en los preceptos mencionados. Dicha distinción con el ámbito general obedece, sin duda alguna, al reforzamiento de las garantías que requieren la naturaleza de los datos y la propia actividad a la que se vincula el tratamiento, en la que la cadena de custodia, la trazabilidad de las operaciones y la seguridad se erigen elementos esenciales, incluso para garantizar la validez de las fuentes de prueba que se pretendan practicar. Para este ámbito, en particular, la Ley Orgánica 7/2021, exige en su art. 37 que las autoridades competentes garanticen la implantación, cuanto menos, de las siguientes medidas orientadas a la seguridad:

a) Control de acceso a los equipamientos, a fin de denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

b) Control de los soportes de datos, a fin de impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

c) Control del almacenamiento, a fin de impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

d) Control de los usuarios, a fin impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

e) Control del acceso a los datos, con el objeto de garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.

f) Control de la transmisión, en aras de garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.

g) Control de la introducción, para garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los

sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) Control del transporte, con miras a impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) Control de restablecimiento, al objeto de garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) Control de fiabilidad e integridad, con la finalidad de garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

Como puede comprobarse, la aplicación de las medidas de seguridad y control que se establecen en pos de asegurar la integridad y confidencialidad de los datos obrantes en los ficheros jurisdiccionales no se circunscriben únicamente a los elementos materiales que conforman los sistemas de tratamiento, sino que se extienden igualmente a las personas que tienen acceso o que intervienen activamente de cualquier modo en actividades que conlleven aparejado inexorablemente un tratamiento de datos personales. Por tal motivo, la normativa exige igualmente al responsable que extienda la adopción de medidas de seguridad que tiendan a garantizar que de entre los sujetos que se hallen bajo su autoridad, únicamente puedan tratar datos personales aquellos que se señalen y exclusivamente de acuerdo a las instrucciones y directrices que imparta⁷².

En todo caso, con relación a este principio es imprescindible recordar que la provisión de medios materiales y personales, y por tanto de los medios tecnológicos adecuados para el tratamiento de los datos personales, no depende de los propios órganos judiciales, ni de sus titulares, a pesar de tener la condición de autoridades competentes. Al contrario, éstos son suministrados por las denominadas Administraciones prestacionales⁷³. Por tanto, son éstas, como encargadas del tratamiento, las que deben asegurar el cumplimiento de las obligaciones en materia de tratamiento y protección de datos personales, especialmente, en lo que se refiere al tratamiento que se lleva a cabo por medios y sistemas electrónicos, totalmente automatizado. Ello sin perjuicio de, tal y como prevé el art. 236 *sexies* LOPJ en su apartado 3º, que el Ministerio de Justicia,

⁷² Con esta exigencia se trata, en definitiva, de conseguir la acomodación de la forma en que los funcionarios integrados en los Juzgados realizan sus funciones acorde exigencias que resultan de las medidas técnicas y organizativas implantadas, para asegurar el mantenimiento de la confidencialidad y seguridad de los datos personales.

⁷³ Arts. 236 *sexies* 1º y 2º LOPJ.

previo informe del Consejo General del Poder Judicial, elabore códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la oficina judicial, adecuando los principios de la normativa general a los propios de la regulación procesal y organización que resultan aplicables a los órganos judiciales.

8. Principio de responsabilidad activa o proactividad

Como colofón a los principios rectores vinculados al tratamiento de datos, el legislador europeo ha introducido *ex novo* al principio responsabilidad activa o proactividad⁷⁴, que se recoge en los arts. 4.4⁷⁵ Directiva 2016/680/UE y art. 6.5 Ley Orgánica 7/2021. Dicho principio puede, además, considerarse como una de las grandes novedades en la materia, por provocar un giro copernicano en cuanto al sistema de responsabilidad al que se sujetan las autoridades intervinientes en el tratamiento⁷⁶. Éste se proclama bajo la siguiente consigna: “El responsable del

⁷⁴ Los términos de responsabilidad activa o proactividad -tal y como ha sido señalado mayoritariamente por la doctrina- han sido los vocablos utilizados para la trasposición al castellano del término anglosajón *accountability*, que es el concepto al que alude el legislador europeo para definir a tal principio. Véase ALBERTO GONZÁLEZ, P., *Responsabilidad proactiva en los tratamientos masivos de datos*. En *Dilemata*, núm. 24, 2017, España, p. 120 y MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability* [en línea]. *El Derecho*, 2019. Éste último autor considera que los vocablos por los que se ha trasladado el término *accountability* al castellano no acaban de reflejar la riqueza material de este concepto anglosajón.

⁷⁵ Aunque el principio de responsabilidad proactiva se incorpora por primera vez en el ordenamiento jurídico como modelo preceptivo y orientador del marco de protección de datos a través del paquete legislativo impulsado por la Unión Europea en 2016, lo cierto es que la Organización para la Cooperación y el Desarrollo Económico ya optó por la adopción de este principio en sus Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de 23 de septiembre de 1980. Asimismo, el GTA29 en su Dictamen 3/2010 sobre el principio de responsabilidad sugería la introducción de este modelo de responsabilidad mediante el otorgamiento de margen de actuación a los responsables del tratamiento para la modulación progresiva de la aplicación de medidas concretas en función del riesgo del tratamiento y la naturaleza de los datos a tratar.

⁷⁶ En los regímenes previos al RGPD se contemplaba un sistema de responsabilidad esencialmente basado en la responsabilidad reactiva – en contraposición al sistema proactivo o de responsabilidad activa- del responsable del fichero, pues los arts. 23 y 24 de la Directiva 95/46/CE conminaba a los Estados miembros a sancionar a los responsables que incumplieran las obligaciones que se dispusieran en las legislaciones nacionales que la transpusieran. Principio reactivo que en el ordenamiento interno se plasmó en el art. 43.1 LOPD al indicar que “*Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley*”. Es decir, el responsable del tratamiento estaba obligado a adoptar las concretas medidas de seguridad que se enumeraban con carácter general en la normativa de protección de datos para todos los responsables, con independencia de las particulares circunstancias existentes en la organización y la efectividad real de las medidas, respondiendo ante un eventual incumplimiento de estas obligaciones so pena de incurrir en la comisión de una

tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo”.

El principio de responsabilidad proactiva determina que la responsabilidad del cumplimiento de las distintas obligaciones y garantías establecidas en el marco jurídico vigente del derecho a la protección de datos, con especial atención de los principios vertebradores del sistema, recae en último término en la autoridad competente⁷⁷. Por tanto, los órganos judiciales, en tanto autoridad, deben no solamente cumplir diligentemente con los principios y obligaciones dispuestos en la normativa, sino que, además, deben de ser capaces de demostrarlo a la autoridad de control e incluso al propio interesado. O, dicho en otros términos, la autoridad competente, en tanto organiza y gestiona el sistema de protección de datos se encuentra sujeto a la condición inexcusable de cumplir férrea y escrupulosamente todos los principios y obligaciones esenciales de la materia con el fin de respetar los derechos y libertades del interesado, debiendo estar en disposición de poder acreditar fehacientemente tal cumplimiento⁷⁸.

En términos prácticos, este modelo requiere la realización de un análisis previo, exhaustivo y *ad casum* de los riesgos que entraña el tratamiento, atendiendo a los datos tratados, las finalidades a las que se destinan los mismos y las modalidades de operaciones de tratamiento seguidas. De acuerdo con los

infracción administrativa. Mientras la implantación de un sistema alternativo de responsabilidad activa supone un auténtico cambio de paradigma en la concepción del modelo de responsabilidad, pues los actores implicados adquieren un papel activo en la implantación y seguimiento de los procesos de cumplimiento de la normativa de protección de datos, debiendo afrontar tareas encaminadas una previa valoración de los riesgos que pudieran generarse con el tratamiento y a partir de los resultados obtenidos, proceder a la adopción de las medidas adecuadas para garantizar los principios y garantías de la materia, dotándose asimismo de mecanismos internos y externos para evaluar su fiabilidad y demostrar su efectividad cuando se solicite por las autoridades de control.

⁷⁷ BAJO ALBARRACÍN, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el Compliance. En LÓPEZ CALVO, J. (coord.) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Las Rozas de Madrid: Wolters Kluwer, 2019, p. 975.

⁷⁸ El Considerando (50) Directiva 2016/680/UE describe a la perfección las implicaciones esenciales de este principio para el responsable, tal que así “Se debe establecer la responsabilidad del responsable del tratamiento en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe estar obligado a poner en marcha medidas oportunas y eficaces y a poder demostrar la conformidad de las actividades de tratamiento con la presente Directiva. Estas medidas deben tener en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo que representan para los derechos y las libertades de las personas físicas. Las medidas adoptadas por el responsable del tratamiento deben incluir la formulación y puesta en marcha de salvaguardias específicas en relación con el tratamiento de los datos personales de personas físicas vulnerables, en particular los niños”.

resultados obtenidos, la autoridad deberá de determinar explícitamente los medios y formas de aplicar las medidas de seguridad y principios rectores del tratamiento, cerciorándose de que son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Obligaciones que adquieren especial significación a la hora de adoptar medidas de investigación para la obtención de fuentes de prueba consistentes en datos de carácter personal.

Asimismo, dichas obligaciones deben entenderse de modo dinámico, pues exigen del responsable una labor continua de revisión, actualización y mejora, especialmente ante los cambios que puedan acontecer en alguno de los elementos que participen en las actividades de tratamiento⁷⁹. En síntesis, este principio exige principalmente del responsable del tratamiento por estar a la cabeza, aunque también de todos los demás participantes⁸⁰, una actitud consciente, diligente, preventiva y proactiva⁸¹ frente a las operaciones de tratamiento de datos, con el claro objetivo de asegurar el respeto a los derechos y libertades del interesado.

9. Bibliografía

ABERASTURI GORRIÑO, U. *Los principios de la protección de datos aplicados en la sanidad (tesis doctoral)*. Bilbao: Universidad del País Vasco, 2011.

ALBERTO GONZÁLEZ, P., *Responsabilidad proactiva en los tratamientos masivos de datos*. En *Dilemata*, núm. 24, 2017, España, pp. 115-129. [consulta: 14 junio 2022] ISSN: 1989-7022. Disponible en:

<https://dialnet.unirioja.es/descarga/articulo/6066825.pdf>

APARICIO SALOM, J. La calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid, Civitas, 2010, pp. 324-339.

ATAZ LÓPEZ, J. La buena fe contractual. En Bercovitz RODRÍGUEZ-CANO, R., MORALEJO IMBERNÓN, N. y QUICIOS MOLINA, M. S. (coord.) *Tratado de los Contratos*. Valencia, Tirant Lo Blanch 2009, pp. 167-170. ISBN 9788498765045.

⁷⁹ MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability...* referencia 74.

⁸⁰ PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales... referencia 8, p. 48, considera que con este principio se pretende instaurar una filosofía y cultura de respeto al derecho a la protección de datos en el seno de la organización.

⁸¹ PALMA ORTIGOSA, A., Principios relativos al tratamiento de datos personales... referencia 8, p. 48 y LORENZO CABRERA, S., PALMA ORTIGOSA, A., y TRUJILLO CABRERA, C., «Responsabilidad proactiva» en MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dir.), *Protección de datos, responsabilidad activa técnicas de garantía*, Reus, Madrid, 2018, pág. 154.

BAJO ALBARRACÍN, J. C. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el Compliance. En LÓPEZ CALVO, J. (coord.) *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Las Rozas de Madrid: Wolters Kluwer, 2019, pp. 973-981. ISBN 9788490903452.

DELGADO MARTÍN, J. Reflexiones sobre la protección de datos personales en la Administración de Justicia. En *Diario La Ley*, núm. 9363, 2019, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: <https://diariolaley.laleynext.es/>

FRÍAS MARTÍNEZ, E. Obtención de datos personales en procesos penales y administrativos. En *Diario La Ley*, núm. 9404, 2019, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: <https://diariolaley.laleynext.es/>

GALÁN MUÑOZ, A. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. En COLOMER HERNÁNDEZ, I. (dir.) *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Cizur Menor: Aranzadi, 2015, pp. 37-70. ISBN 9788490599174.

GONZÁLEZ CANO, M. I., Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. En *Revista Brasileira de Direito Processual Penal*, vol. 5, núm. 3, 2019, Brasil, pp. 1331-1384. [consulta: 16 junio 2022] ISSN: 2525-510X. Disponible en: <https://revista.ibraspp.com.br/RBDPP/article/view/279/188>

HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales*. Madrid: Dykinson, 1999. ISBN 9788481554090.

LORENZO CABRERA, S., PALMA ORTIGOSA, A., y TRUJILLO CABRERA, C. Responsabilidad proactiva. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dir.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Editorial Reus, 2018, pp. 143-172. ISBN 9788429020939.

MARTÍNEZ MARTÍNEZ, R. Las medidas de seguridad. En MARTÍNEZ MARTÍNEZ, R. (coord.), *Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*. Valencia: Tirant lo Blanch, 2009, pp. 89-119. ISBN 9788498763560.

MARTÍNEZ MARTÍNEZ, R. *Diligencia y responsabilidad en protección de datos: la llamada accountability* [en línea]. *El Derecho*, 2019. [consulta: 16 junio 2022]. Disponible en: <https://elderecho.com/diligencia-y-responsabilidad-en-proteccion-de-datos-la-llamada-accountability>

MORENO CATENA, V. y CORTÉS DOMÍNGUEZ, V. *Derecho Procesal Penal*. Valencia: Tirant Lo Blanch, 2021. ISBN 9788411130479.

MURILLO DE LA CUEVA, P. *Informática y protección de datos personales*. Madrid: CEC, 1993.

PALMA ORTIGOSA, A. Principios relativos al tratamiento de datos personales. En MURGA FERNÁNDEZ, J. P., FERNÁNDEZ SCAGLIUSI M. A. y ESPEJO LERDO DE TEJADA, M. (dirs.), *Protección de datos, responsabilidad activa técnicas de garantía*. Madrid: Editorial Reus, 2018, pp. 39-49. ISBN 9788429020939.

PUYOL MONTERO, J. Los principios del derecho a la protección de datos. En PIÑAR MAÑAS J. L. (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Madrid: Editorial Reus, 2016, pp. 135-150. ISBN 9788429019360.

RIBAGORDA GARNACHO, A. Las medidas de seguridad en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal: Título II. Principios de la Protección de Datos. Artículo 9. en TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 735-761. ISBN 9788447034239.

RÍO LABARTHE, G. El proceso penal. Funciones. En ASENSIO MELLADO, J. M. (dir.) *Derecho procesal penal*. Valencia: Tirant Lo Blanch, 2020, pp. 25-36. ISBN 9788413559544.

SÁNCHEZ BRAVO, A. *La protección del derecho a la libertad informática en la Unión Europea*. Sevilla: Universidad de Sevilla, 1998. ISBN 8447204936.

SANZ CALVO, L. Calidad de los datos. En LESMES SERRANO, C. (coord.) *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*. Valladolid: Lex Nova, 2008, pp. 138-162.

SOLAR CALVO, P. La doble vía europea en protección de datos. En *Diario La Ley*, núm. 7832, 2012, España. [consulta: 18 junio 2022] ISSN: 1989-6913. Disponible en: <https://diariolaley.laleynext.es/>

TRONCOSO REIGADA, A. El principio de calidad de los datos. En TRONCOSO REIGADA, A. (dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas, 2010, pp. 340-396. ISBN 9788447034239.

Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

Financiación

Esta publicación ha sido financiada por la Unión Europea “NextGenerationEU”, por el Plan de Recuperación, Transformación y Resiliencia y por el Ministerio de Universidades, en el marco de las ayudas Margarita Salas, para la Recualificación del sistema universitario español 2021-2023 convocadas por la Universidad Pablo de Olavide, de Sevilla.



Las opiniones expuestas en los distintos trabajos y colaboraciones son de la exclusiva responsabilidad de los autores. Acta Judicial no comparte necesariamente las opiniones y juicios expuestos en los trabajos firmados.

Las obras se publican bajo una licencia Creative Commons Reconocimiento-NoComercial-Sin Obra Derivada 4.0 Internacional:

No se permite un uso comercial de la obra original ni generar obras derivadas (texto legal).



Director ejecutivo

Fernando Javier Cremades López de Teruel

Editor

Jesús Sancho Alonso

ISSN 2603-7173

www.letradosdejusticia.es/revistaactajudicial

Dirección de comunicación con la Revista

revista@letradosdejusticia.es

Para el envío de trabajos deberá registrarse en la página web

Normas de publicación

<http://www.letradosdejusticia.es/revistaactajudicial>

Puede verlas también en la página 76

Consejo Editorial

Ernesto Casado Rodríguez (Presidencia del Colegio Nacional de Letrados de la Administración de Justicia, España)

María José Cañizares Castellanos (Secretario Coordinador de Almería, España)

Fernando Javier Cremades López de Teruel (Letrado de la Administración de Justicia, España)

Jesús Sancho Alonso (Doctor en Derecho. Letrado de la Administración de Justicia, España)

José Palazuelos Morlanes (Letrado de la Administración de Justicia del Tribunal Supremo, España)

Isabel Morales Mirat (Letrado de la Administración de Justicia, España)

Comité Científico

Los miembros del Comité Científico han expresado su autorización para aparecer en este listado:

María José Alonso Más (Profesora Titular de Derecho Administrativo. Universitat de València, España)

María Luisa Atienza Navarro (Profesora Titular de Derecho Civil. Universitat de València, España)

María Asunción Barrio Calle (Letrado de la Administración de Justicia, España)

José Bonet Navarro (Catedrático de Derecho Procesal. Universitat de València, España)

Emiliano Borja Jiménez (Catedrático de Derecho Penal. Universitat de València, España)

María José Cañizares Castellanos (Secretario Coordinador de Almería, España)

Carolina del Carmen Castillo Martínez (Magistrada. Profesora Titular de Derecho Civil (excedente), Profesora Asociada de Derecho Civil. Universitat de València, España)

Vicente Cuñat Edo (Catedrático Emérito de Derecho Mercantil. Universitat de València, España)

Daniel de la Rubia Sánchez (Secretario Coordinador de Granada, España)

José Ramón de Verda y Beamonte (Catedrático de Derecho Civil. Universitat de València, España)

Joaquín Delgado Martín (Magistrado. Miembro de la Red Judicial de Expertos en Derecho Europeo (REDUE). Doctor en Derecho, España)

María del Pilar Diago Diago (Catedrática de la Universidad de Zaragoza, España)

Jesús Estruch Estruch (Catedrático de Derecho Civil. Universitat de València, España)

Antonio Fernández de Bujan y Fernández (Catedrático de la Universidad Autónoma de Madrid, Departamento de Derecho Privado, Social y Económico. Académico de Número de la Real Academia de Jurisprudencia y Legislación de España)

Carmen García Cerdá (Fiscal de la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada, España)

Pablo Izquierdo Blanco (Magistrado, España)

Francisco Marín Castán (Magistrado. Presidente de la Sala Primera Tribunal Supremo, España)

Alfredo Martínez Guerrero (Letrado de la Administración de Justicia, España)

María Dolores Mas Badía (Profesora Titular de Derecho Civil. Universitat de València, España)

Diego Medina García (Secretario de Gobierno del Tribunal Superior de Justicia de Andalucía, España)

María Pilar Montés Rodríguez (Profesora Titular de Derecho Civil. Universitat de València, España)

Manuel Ortells Ramos (Catedrático de Derecho Procesal. Universitat de València, España)

Guillermo Palao Moreno (Catedrático de Derecho Internacional Privado. Universitat de València, España)

Inmaculada Revuelta Pérez (Profesora Titular de Derecho Administrativo. Universitat de València, España)

Ricardo Rivero Ortega (Catedrático de Derecho Administrativo. Rector de la Universidad de Salamanca, España)

Ángel Sánchez Blanco (Catedrático Emérito de Derecho Administrativo. Universidad de Málaga, España)

Remedios Sánchez Ferriz (Catedrática de Derecho Constitucional. Universitat de València, España)

Raúl Sánchez Gómez (Profesor de Derecho Procesal de la Universidad Pablo de Olavide, Sevilla, España)

Antonio Vercher Noguera (Fiscal de Sala de Medio Ambiente y Urbanismo del Tribunal Supremo, España)

Rafael Verdura Server (Catedrático de Derecho Civil. Universitat de València, España)

PETICIÓN DE PUBLICACIONES

La Revista Acta Judicial pretende ofrecer un espacio de difusión del estudio e investigación en el campo del Derecho español. La Revista está abierta a todo tipo de trabajos doctrinales relacionados con el Derecho público y privado, tanto en su perspectiva sustantiva como procesal. Puede tener un ámbito y dimensión autonómica, nacional, europea e internacional, debiendo tener, en estos dos últimos casos, claros vínculos con el Derecho español. Si el estudio realizado aparece como Derecho comparado, ambos Derechos tratados deben alcanzar la misma, o análoga, proporcionalidad, relevancia y profundidad de estudio del tema, de modo que el Derecho español no quede relegado y sea su referencia meramente testimonial. Al mismo tiempo, se pretende ofrecer un canal de reflexión y difusión de estudios técnicos sobre nuevas tecnologías y ciberseguridad que tengan aplicación, incidencia o influencia en el Derecho español.

La Revista Acta Judicial tiene una periodicidad semestral, publicándose en los meses de enero y julio.

La revista está abierta a la recepción de artículos originales, hasta el 15 de mayo para el número de julio y el 15 de noviembre para el número de enero.

Se establece un sistema de evaluación de artículos de revisión por pares, en el que intervienen un mínimo de dos evaluadores externos a la entidad editora de la Revista Acta Judicial, [pulse para más información](#).

Acta Judicial se edita en Madrid, España, bajo el ISSN 2603-7173

Le agradecemos la difusión que pueda aportar a la revista informando de su disponibilidad y periodo de recepción de colaboraciones a quién considere que puede interesar.

Normas de publicación

Para publicar en la Revista Acta Judicial, los autores interesados deben enviar sus textos en formato de Word (doc, docx) en cualquiera de sus versiones, a través de la página web de la Revista, [pulse aquí para más información](#).

1. Contenido del artículo

Los artículos deben tener una extensión entre 15 y 40 páginas (sin contar los resúmenes, las palabras clave y el sumario), si bien con carácter excepcional se podrá admitir hasta 50 páginas, siempre que se justifique la razón al enviar el trabajo. Se seguirá estrictamente la [plantilla](#) que la Revista pone a disposición del autor, cuyo uso se recomienda para facilitar el trabajo. Consulte la información para autores disponible en la página web de la Revista.

El artículo enviado para su publicación deberá contener los siguientes elementos:

1. Título del artículo, en español y en inglés.
2. Nombre completo del autor o autores (máximo 4), con indicación de su filiación (profesión o actividad académica) y una dirección electrónica de contacto.
3. Un resumen de 250 palabras como máximo (en español y en inglés).
4. Palabras clave: entre cinco y diez (con un máximo de 2 líneas), separadas por comas (en español y en inglés).
5. Sumario, consistente en los epígrafes y sub-epígrafes del artículo.
6. El texto del artículo, en español, incluyendo en él los cuadros y figuras (si las hubiera), con una extensión mínima de 15 hojas y máxima de 40 hojas, o 50 hojas con carácter excepcional y siempre que se justifique la razón al enviar el trabajo.
7. Bibliografía. Al final del texto se consignará un listado completo con la bibliografía o referencias bibliográficas empleadas en la elaboración del artículo. Todas las citas que se realicen dentro del texto deberán reflejarse en la bibliografía. Las referencias bibliográficas se ordenarán por orden alfabético del primer apellido del autor o primer autor si son varios. Para distintos trabajos de un mismo autor o autores se tendrá en cuenta el orden cronológico según el año de publicación.
8. El autor podrá incorporar en el texto o pie de página del artículo palabras o conjunto de palabras con hiperenlaces que considere oportunos (por ejemplo, enlace a normas en el BOE, sentencia en el CENDOJ o Tribunal Constitucional), que quedarán en azul y no tendrán subrayado. Siempre que no sean citas, que deberán tener el formato específico de las citas.
9. El autor deberá indicar, al final del artículo, si existe algún tipo de conflicto de intereses relacionado con el artículo. Así mismo deberá señalar si el artículo ha sido realizado gracias a algún tipo de financiación.

2. Formato del artículo

La no adecuación a la [plantilla](#) de Word establecida para la Revista y que se pone a disposición de los autores (tipo de letra, sangrado, espacios, formatos de edición, estructura,...), es motivo de rechazo directo del artículo presentado,

pudiendo ser invitado desde el Comité Editorial a modificarlo según plantilla y enviarlo de nuevo.

A continuación, se establecen una serie de reglas que el autor deberá seguir a la hora de escribir su artículo, así como unas normas sobre el formato que, si no se utiliza la plantilla facilitada por la Revista, deberá tener en cuenta tomando como base el formato que por defecto establece Word:

- 1. Tamaño de hoja.** Los artículos deben estar escritos en un tamaño de hoja A4, con márgenes de 3 cm por cada lado (superior, inferior, izquierdo y derecho), con letra base Palatino Linotype, tamaño 12 puntos y espacio sencillo, sin espaciado anterior ni posterior. En una sola columna. Solo con “sangría especial” en “primera línea” de 1,25 cm ([pinche aquí para consultar la forma de realizarlo en Word](#)).
- 2. Título del artículo en español.** Debe estar en letra Mayúscula, Palatino Linotype 14, centrado en negrita (con el estilo “Título 1” de la plantilla).
- 3. Título del artículo en inglés.** Debe estar en letra Minúscula, Palatino Linotype 12, centrado en negrita (con estilo “Title in English” de la plantilla).
- 4. Autores.** Debe constar el nombre y apellidos de los autores, en letra Palatino Linotype 12, centrada (con estilo “Título 2” de la plantilla).
- 5. Afiliación autores.** Debe constar la profesión, actividad académica, etc., Palatino Linotype 10, centrada (con estilo “Filiación” de la plantilla).
- 6. Correo electrónico autores.** Debe constar el correo electrónico de contacto del autor, Palatino Linotype 10, centrada (con estilo “Filiación” de la plantilla).
- 7. Resumen y Abstract.** Deberán tener una extensión máxima de 250 palabras, en letra Palatino Linotype 12, justificado (con estilo “Normal” de la plantilla).
- 8. Palabras clave y Keywords.** Deberán tener entre cinco y diez palabras, tanto en español como en inglés, separadas por comas, en letra Palatino Linotype 12, justificado (con estilo “Normal” de la plantilla).
- 9. Cuerpo del artículo.** Con letra base Palatino Linotype 12 puntos, justificado y espacio sencillo, sin espaciado anterior ni posterior. Solo con “sangría especial” en “primera línea” de 1,25 cm.
- 10. Epígrafes y sub-epígrafes.** Los títulos de los diferentes apartados (epígrafes y sub-epígrafes) deberán ir en minúscula y negrita precedido de

la correspondiente numeración no automática, que seguirán las siguientes pautas:

- 1.
- 1.1.
- 1.1.1.
- 1.1.1.a.

Al terminar un epígrafe o sub-epígrafe hay que dejar un espacio entre el texto y el epígrafe siguiente.

El título de los epígrafes y sub-epígrafes deben tener activados el “control de líneas viudas y huérfanas” y “Conservación con el siguiente” (en “Paginación” de “Líneas y saltos de página” de la sección “Párrafo” de Word. ([Pinche aquí para consultar la forma de realizarlo en Word](#)).

11. Notas al pie. Las notas al pie del texto, estarán enumeradas correlativamente al final de cada página (en letra Palatino Linotype 10, justificado, con espacio sencillo, sin espaciado anterior ni posterior). [Pinche aquí para consultar sobre notas al pie](#).

12. Numeración de página. Los números de las páginas estarán alineados a la derecha, en fuente Palatino Linotype, tamaño 10.

13. Bibliografía. Al final del texto del artículo, se consignará un listado completo con la bibliografía o referencias bibliográficas empleadas en la elaboración del mismo.

TODAS las citas que se realicen dentro del texto deberán reflejarse en la bibliografía.

Las referencias bibliográficas se ordenarán por orden alfabético del primer apellido del autor o primer autor si son varios. Para distintos trabajos de un mismo autor o autores se tendrá en cuenta el orden cronológico según año de publicación.

14. Hiperenlaces. No tendrán subrayado y quedarán con su característico color azul (según el estilo de la plantilla “Hipervínculo”). En caso de ser una cita, debe tenerse en cuenta el formato específico de las citas.

3. El formato de las citas y bibliografías

El formato de las citas bibliográficas deberá seguir la [norma ISO 690:2010](#), cuyo equivalente en español es la norma UNE-ISO 690:2013, que fue traducida por la Asociación Española de Normalización y Certificación (AENOR).

La norma UNE-ISO 690:2013 (ISO 690:2010) acepta el sistema de notas continuas, que es el sistema que se exige en la Revista Acta Judicial.

- Cita: Se insertan los números en cada nota de forma consecutiva. Si hay diversas citas de un mismo recurso, se usará un número de nota para cada mención que da lugar a la cita.
- Referencia: Se presentan las notas en su orden numérico. Si una nota se refiere a un recurso ya mencionado (recurso citado en una nota anterior), bien se repite la referencia completa o bien se da el número de la nota anterior seguido de los números de páginas necesarios, etc. (*Ejemplo número nota anterior:* ³⁴ ESPAÑA PEREZ, M.D., referencia 8, p 556.)
- Fuentes de datos: Los datos usados en una referencia deberán tomarse del propio recurso citado (siempre que sea posible). Por orden de preferencia, las fuentes apropiadas serán en primer lugar de la portada (o página de inicio de un sitio web, rótulos de un audiovisual, etc.) y de otras partes de la obra en caso necesario (verso de la portada, la cabecera, etc; cubierta o etiqueta asociada permanentemente con el documento).
Se pueden añadir elementos que no aparezcan en el documento fuente, con el fin de completar la información. Estos elementos deberán ir encerrados entre corchetes [].

3.1. A continuación le mostramos ejemplos de referencias bibliográficas que cumplen con la norma UNE-ISO 690:2013.

Libros impresos y publicaciones monográficas similares con un autor

NOMBRE DEL CREADOR. *Título del libro (cursiva)*. Edición (si no es la primera edición). Lugar: Editor, Fecha de publicación. Rango de páginas (de la contribución). Identificador normalizado (ISBN, ...) (si está disponible)

Ejemplo: ESPAÑA PEREZ, M.D. *La división de poderes en la constitución española*. Pamplona: Anagrama, 2004. pp. 25-26. ISBN 55-557960-37-5

Libros impresos y publicaciones monográficas similares con dos o más autores

NOMBRE DEL (DE LOS) CREADOR (ES). *Título del libro (cursiva)*. Edición (si no es la primera edición). Lugar: Editor, Fecha de publicación. Rango de páginas (de la contribución). Identificador normalizado (ISBN,...) (si está disponible)

Para las obras con más de tres autores, se recomienda dar todos los nombres. Si se elige no mencionar a todos los autores, se dará el nombre del primer autor seguido de "y otros" o "et al."

Ejemplo: THOMPSON, J., BERBANK-GREEN, B. y CUSWORTH, N. *Introducción a la historia del derecho*. Madrid: Taurus, 1988. p. 30.

Libros electrónicos y publicaciones monográficas en línea

Ejemplo 1: PASTOR PRIETO, S. *Análisis Económico de la Justicia y Reforma Judicial* [en línea]. Tirant Lo Blanch, 2016. [consulta: 15 enero 2017] Disponible en: <http://www.tirantonline.com>

Ejemplo 2: KAFKA, Franz. *The Trial* [en línea]. Translated by David WYLLIE. Project Gutenberg, 2005. [consulta: 5 junio 2006]. Disponible en: <http://www.gutenberg.org/dirs/etext05/ktria11.txt>

Capítulo de libro (referencias a contribuciones dentro de publicaciones monográficas impresas)

NOMBRE DEL (DE LOS) CREADOR (ES). Título de la contribución. En: NOMBRE DEL (DE LOS) CREADOR (ES) *Título (cursiva)*. Edición (si no es la primera edición). Lugar: Editor, Fecha de publicación, Rango de páginas (de la contribución). Identificador normalizado (ISBN...) (si está disponible)

Ejemplo: GONZALEZ VEGA, F.J. La letra de cambio. En FERNÁNDEZ TORREJÓN, J.A. (coord.) *Manual de derecho mercantil*. Granada: Comares, 2014, pp. 162-179.

Capítulo de libro en línea (referencias a contribuciones dentro de publicaciones monográficas en línea)

Ejemplo: NATIONAL RESEARCH COUNCIL [U.S.], *Committee on the Training Needs of Health Professionals to Respond to Family Violence. Current Educational Activities in the Health Professions*. En: *Confronting Chronic Neglect: The Education and Training of Health Professionals on Family Violence* [en línea]. Washington DC: National Academy Press, 2002, pp. 35-44 [consulta: 23 junio 2006]. Disponible en: http://darwin.nap.edu/openbook.php?record_id=10127&page=35

Artículo de revista (publicaciones seriadas impresas)

NOMBRE DEL (DE LOS) CREADOR (ES). Título de la contribución En: Título de la publicación seriada fuente (cursiva). Edición. Lugar: Editor, Fecha de publicación, Numeración, Rango de páginas (de la contribución). Identificador normalizado (ISSN, ...) (si está disponible)

Ejemplo: LÓPEZ CASTRO, A. La fe pública judicial. En: *Revista de Derecho Político*. Madrid: UNED, 1998, no. 84, pp. 173-194.

Artículo de revista en línea (contribución dentro de una publicación seriada en línea)

Ejemplo: SALVADOR-OLIVÁN, J.A., MARCO CUENCA, G., ARQUERO AVILÉS, R. Impacto de las revistas españolas de Biblioteconomía y Documentación y repercusión de las autocitas en su índice h. En: *Revista Investigación Bibliotecológica: archivonomía, bibliotecología e información*, vol. 32, núm. 77, octubre/diciembre, 2018,

México. pp. 13-30. [consulta: 01 noviembre 2018] ISSN: 2448-8321. Disponible en: <http://rev-ib.unam.mx/ib/index.php/ib/article/view/57852/51944>

Referencia a publicación seriada en línea

Nombre publicación (cursiva) [en línea]. Lugar: Editor, Fecha de publicación, Numeración, Rango de páginas (de la contribución) [consulta: fecha]. Identificador normalizado (ISSN, ...) (si está disponible). Disponible: enlace a la publicación

Ejemplo 1 : *Acta Zoologica* [en línea]. Oxford, U.K.: Blackwell Publishing Ltd., January 2006, vol. 87, issue 1 [consulta: 6 julio 2006]. Academic Search Premier. EBSCOhost Research Databases. ISSN 0001-7272. Disponible en: <http://search.epnet.com>

Ejemplo 2: *AJET: Australasian Journal of Educational Technology* [en línea]. Australia: ASCILITE, Winter 2000, vol. 16, no.2 [consulta: 23 octubre 2003]. ISSN 0814-673X. Disponible: <http://www.ascilite.org.au/ajet/ajet16/ajet16.html>

Contribución a las Actas de un Congreso

NOMBRE DEL (DE LOS) CREADOR (ES). Título de la contribución. En: Título de la publicación fuente (cursiva). Edición. Lugar: Editor, Fecha de publicación, Numeración, Rango de páginas (de la contribución). Identificador normalizado (si está disponible)

Ejemplo: DE OCAÑA LACAL, D. Los archivos judiciales ante el reto de las nuevas tecnologías. En: *Congreso de archivos judiciales en Sevilla en mayo de 2007*. Sevilla, Consejería de Justicia y Administración Pública de la Junta de Andalucía, 2007. pp. 98-101.

Legislación

País. Título. Publicación, fecha de publicación, número, páginas.

Ejemplo: España. Ley orgánica 10/1995, de 23 de noviembre, del Código penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281, p. 33987.

También puede consultar las normas de publicación en la página web, pulsando aquí.

Los autores autorizan la reproducción y comunicación pública de los textos completos de sus artículos a efectos de su inclusión en la base de datos de Dialnet, así como en otras necesarias para garantizar el impacto de las obras.



Tercera época

ACTA JUDICIAL

Revista editada por Ilustre Colegio Nacional de Letrados de la Administración de Justicia

<http://www.letradosdejusticia.es/revistaactajudicial>

revista@letradosdejusticia.es

Dirección postal
Ilustre Colegio Nacional de Letrados de la Administración de Justicia
Edificio del Tribunal Supremo
Planta baja, Despacho B-17
C/ Villa de París s/n
28004 Madrid

La Revista Acta Judicial y su signo distintivo son marcas registradas