

# PERSPECTIVAS TRANSVERSALES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Dirección

Raquel Pérez Díaz

Diana Paola González Mendoza

Paula Vega García



**Actividad financiada por la Unión Europea-NextGenerationEU, Ministerio de Universidades y Plan de Recuperación, Transformación y Resiliencia, mediante convocatoria de la Universidad de Oviedo (MU-21-UP2021-030 70087867 y MU-21-UP2021-03076582600Y). Igualmente, esta actividad se enmarca en el Proyecto PID2021-126784NB-I00 «Reorganización Administrativa y de los Servicios Públicos a los ciudadanos en la post-pandemia» financiado por MCIN/AEI/10.13039/501100011033/ y por FEDER Una manera de hacer Europa.**

# PERSPECTIVAS TRANSVERSALES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

## Dirección

Raquel Pérez Díaz

Diana Paola González Mendoza

Paula Vega García

Proyecto PID2021-126784NB-I00 financiado por:



COLEX 2024

Copyright © 2024

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. del Código Penal). El Centro Español de Derechos Reprográficos ([www.cedro.org](http://www.cedro.org)) garantiza el respeto de los citados derechos.

Editorial Colex S.L. vela por la exactitud de los textos legales publicados. No obstante, advierte que la única normativa oficial se encuentra publicada en el BOE o Boletín Oficial correspondiente, siendo esta la única legalmente válida, y declinando cualquier responsabilidad por daños que puedan causarse debido a inexactitudes e incorrecciones en los mismos.

Editorial Colex S.L. habilitará a través de la web [www.colex.es](http://www.colex.es) un servicio online para acceder a las eventuales correcciones de erratas de cualquier libro perteneciente a nuestra editorial.

© Raquel Pérez Díaz  
© Diana Paola González Mendoza  
© Paula Vega García

© Editorial Colex, S.L.  
Calle Costa Rica, número 5, 3.º B (local comercial)  
A Coruña, 15004, A Coruña (Galicia)  
[info@colex.es](mailto:info@colex.es)  
[www.colex.es](http://www.colex.es)

I.S.B.N.: 978-84-1194-764-0  
Depósito legal: C 1887-2024

# SUMARIO

## PRESENTACIÓN

|                    |    |
|--------------------|----|
| Presentación ..... | 13 |
|--------------------|----|

## PROTECCIÓN DE DATOS Y FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO: ESTADO DE LA CUESTIÓN A LA LUZ DE LAS ÚLTIMAS RESOLUCIONES JUDICIALES

*Natalia Muñiz Casanova*

|                                                                        |    |
|------------------------------------------------------------------------|----|
| I. Introducción .....                                                  | 15 |
| II. Existencia de una deuda vencida, liquida, exigible y cierta .....  | 16 |
| III. El requerimiento previo de pago .....                             | 18 |
| IV. Controversia respecto a la normativa aplicable .....               | 20 |
| V. La indemnización de los daños producidos por el alta indebida ..... | 22 |
| VI. Conclusiones .....                                                 | 24 |

## LA PROTECCIÓN DE DATOS POR LAS ADMINISTRACIONES TRIBUTARIAS: HACIA UN EQUILIBRIO ENTRE EL SECRETO FISCAL Y EL PRINCIPIO DE MÁXIMA PUBLICIDAD

*Israel Santos Flores*

|                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------|----|
| I. Introducción .....                                                                               | 27 |
| II. El principio de transparencia y máxima divulgación de la información .....                      | 28 |
| III. La importancia de la transparencia en la divulgación de información fiscal ..                  | 30 |
| IV. El secreto fiscal: ¿qué es y para qué sirve? .....                                              | 31 |
| V. La falta de armonización del secreto fiscal con el principio de máxima<br>publicidad .....       | 32 |
| VI. Apuntes para un equilibrio entre el secreto fiscal y el principio de<br>máxima publicidad. .... | 33 |
| VII. A modo de conclusión .....                                                                     | 34 |
| VIII. Bibliografía .....                                                                            | 35 |

## LA PROTECCIÓN DE DATOS EN EL ÁMBITO SANITARIO

*Carmen Cabal Fernández*

|                                                                                                           |    |
|-----------------------------------------------------------------------------------------------------------|----|
| I. Introducción: retos del sector sanitario . . . . .                                                     | 37 |
| II. El control y la penalización sobre los accesos indebidos a las historias clínicas. . . . .            | 38 |
| III. Trascendencia penal: delito de descubrimiento y revelación de secretos . . . .                       | 40 |
| IV. El uso de datos sanitarios asistenciales con fines de investigación . . . . .                         | 41 |
| V. Los intercambios de información con terceros. . . . .                                                  | 43 |
| VI. La interoperabilidad de la historia clínica. . . . .                                                  | 47 |
| VII. Los planes de contingencia para asegurar la continuidad de los servicios en caso de ataque . . . . . | 49 |
| VIII. Otras problemáticas del sector . . . . .                                                            | 51 |
| IX. Conclusiones . . . . .                                                                                | 52 |
| X. Bibliografía . . . . .                                                                                 | 53 |

## PROTECCIÓN DE DATOS PERSONALES EN PLATAFORMAS DE RESOLUCIÓN DE CONFLICTOS

*Paola Jackeline Ontiveros Vázquez*

|                                                                    |    |
|--------------------------------------------------------------------|----|
| I. Introducción . . . . .                                          | 55 |
| II. Desarrollo . . . . .                                           | 58 |
| 1. Proveedores de disputas en línea en México y Europa . . . . .   | 59 |
| A) México . . . . .                                                | 59 |
| B) Europa . . . . .                                                | 60 |
| 2. Regulación en materia de privacidad de datos para ODR . . . . . | 61 |
| 3. Regulación de datos personales en México. . . . .               | 63 |
| 4. Retos en la regulación de datos personales en los ODR . . . . . | 68 |
| III. Conclusiones . . . . .                                        | 71 |
| IV. Bibliografía . . . . .                                         | 72 |
| V. Referencias normativas. . . . .                                 | 73 |

## CREDIT SCORING EN LA NUEVA DIRECTIVA DE CONTRATOS DE CRÉDITO AL CONSUMO: RGPD, AI ACT, PRIVACIDAD DE GRUPO Y DERECHO AL OLVIDO ONCOLÓGICO

*Gonzalo Campos Rivera y José Antonio Castillo Parrilla*

|                                                                                                                   |    |
|-------------------------------------------------------------------------------------------------------------------|----|
| I. La evaluación de solvencia en la Directiva 2022/2023, relativa a los contratos de crédito al consumo . . . . . | 77 |
| II. La evaluación de solvencia basada en el tratamiento automatizado de datos o <i>credit scoring</i> . . . . .   | 80 |
| 1. Bases de legitimación y finalidad del tratamiento en la evaluación de solvencia . . . . .                      | 81 |

## SUMARIO

|                                                                                                                              |     |
|------------------------------------------------------------------------------------------------------------------------------|-----|
| 2. ¿Qué datos pueden utilizarse y cuáles no en una evaluación de solvencia? . . .                                            | 83  |
| 3. Principio de exactitud en el tratamiento de datos y evaluación de solvencia . . . . .                                     | 85  |
| 4. Las herramientas de evaluación de solvencia como sistemas IA de alto riesgo . . . . .                                     | 86  |
| III. La privacidad de grupo como nueva perspectiva del derecho a la protección de datos . . . . .                            | 88  |
| IV. Privacidad de grupo, evaluación de solvencia y datos proxy. Especial referencia al derecho al olvido oncológico. . . . . | 93  |
| V. Conclusiones . . . . .                                                                                                    | 99  |
| VI. Bibliografía . . . . .                                                                                                   | 101 |

### **EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL COMO LÍMITE A LA ACTUACIÓN DEL DETECTIVE PRIVADO**

*Luis Pérez Fernández*

|                                                                                                                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| I. Introducción . . . . .                                                                                                                                                                                 | 105 |
| II. El detective privado y la actividad investigadora . . . . .                                                                                                                                           | 105 |
| III. El encargo profesional realizado al detective. Contenido y límites . . . . .                                                                                                                         | 107 |
| IV. El derecho fundamental a la protección de datos de carácter personal y su incidencia en la investigación privada. . . . .                                                                             | 109 |
| V. El test de proporcionalidad constitucional como búsqueda de un equilibrio entre el fin legítimo de una investigación privada y la limitación del derecho fundamental a la protección de datos. . . . . | 113 |
| VI. Conclusiones . . . . .                                                                                                                                                                                | 115 |
| VII. Bibliografía . . . . .                                                                                                                                                                               | 116 |
| VIII. Recursos en internet . . . . .                                                                                                                                                                      | 117 |
| IX. Jurisprudencia . . . . .                                                                                                                                                                              | 117 |
| Sentencias del Tribunal Constitucional . . . . .                                                                                                                                                          | 117 |
| Sentencias del Tribunal Europeo de Derechos Humanos . . . . .                                                                                                                                             | 117 |

### **LA PROTECCIÓN DE DATOS PERSONALES EN LOS JUICIOS PENALES EN MÉXICO**

*Mtro. Jorge Alberto Vázquez Segura*

|                                                                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| I. Introducción . . . . .                                                                                                                               | 119 |
| II. Planteamiento de la problemática. . . . .                                                                                                           | 120 |
| III. La protección de datos personales en las audiencias públicas del sistema penal acusatorio . . . . .                                                | 121 |
| IV. La protección de datos personales en las solicitudes de acceso a las videograbaciones de audiencias públicas del sistema penal acusatorio . . . . . | 125 |
| V. Conclusiones . . . . .                                                                                                                               | 130 |
| VI. Bibliografía . . . . .                                                                                                                              | 130 |

## **RETOS PARA LA PROTECCIÓN DE DATOS EN EL USO DE LAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL**

*Natalia Menéndez González*

|                                                                                               |     |
|-----------------------------------------------------------------------------------------------|-----|
| I. Introducción: ¿qué es y cómo funciona el reconocimiento facial? . . . . .                  | 131 |
| II. Características del reconocimiento facial y su impacto en la protección de datos. . . . . | 133 |
| 1. Potenciado por Inteligencia Artificial . . . . .                                           | 133 |
| 2. Algorítmicamente sesgado. . . . .                                                          | 133 |
| 3. Remoto . . . . .                                                                           | 134 |
| 4. No invasivo . . . . .                                                                      | 135 |
| 5. Omnipresente . . . . .                                                                     | 136 |
| III. Tipos de datos «extraíbles» por un sistema de reconocimiento facial. . . . .             | 137 |
| IV. Regulación de los sistemas de reconocimiento facial: retos y oportunidades. . .           | 138 |
| V. Conclusiones. . . . .                                                                      | 140 |
| VI. Bibliografía . . . . .                                                                    | 141 |
| VII. Referencias normativas. . . . .                                                          | 143 |

## **DEBERES DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES DE CONSUMIDORES**

*Pablo Muruaga Herrero*

|                                                                                                                                                              |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| I. Planteamiento de la cuestión. . . . .                                                                                                                     | 145 |
| II. Marco jurídico de los deberes de confidencialidad. . . . .                                                                                               | 147 |
| 1. La buena fe precontractual. . . . .                                                                                                                       | 147 |
| 2. La falta de regulación y la información sobre la que recae el deber de confidencialidad . . . . .                                                         | 148 |
| 3. El deber de confidencialidad en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales —LOPD— . . . . . | 151 |
| III. Reflexiones finales: los puntos de fricción entre los deberes de confidencialidad . . . . .                                                             | 153 |
| IV. Bibliografía . . . . .                                                                                                                                   | 155 |

## **MARCO JURÍDICO DE PROTECCIÓN DE DATOS EN LAS INSTITUCIONES DE LA UNIÓN EUROPEA**

*Emma Rodríguez Montes*

|                                                                |     |
|----------------------------------------------------------------|-----|
| I. Contexto. . . . .                                           | 157 |
| II. Principales diferencias entre el EUDPR y el RGPD . . . . . | 158 |
| 1. Ámbito de aplicación . . . . .                              | 158 |
| 2. Bases legales . . . . .                                     | 159 |
| 3. Régimen de transmisión de datos . . . . .                   | 159 |

## SUMARIO

|                                       |     |
|---------------------------------------|-----|
| 4. Autoridad de supervisión . . . . . | 161 |
| III. Contratación pública . . . . .   | 161 |
| IV. Conclusiones . . . . .            | 162 |

### **CONFIDENCIALIDAD EN LA COMUNICACIÓN POR INTERNET**

*Carlos Enrique Vigil de Quiñones Fernández*

|                                                              |     |
|--------------------------------------------------------------|-----|
| I. La comunicación electrónica . . . . .                     | 163 |
| 1. ¿Derecho u obligación? . . . . .                          | 163 |
| 2. Definiciones . . . . .                                    | 164 |
| 3. La red Internet . . . . .                                 | 166 |
| II. Confidencialidad entre comunicantes . . . . .            | 167 |
| 1. La confidencialidad como obligación legal . . . . .       | 168 |
| A) La reserva como regla general de actuación . . . . .      | 168 |
| B) Datos personales . . . . .                                | 169 |
| 2. Su aplicación a los contratos . . . . .                   | 170 |
| III. El secreto frente a terceros . . . . .                  | 172 |
| 1. El mensaje y sus datos asociados . . . . .                | 172 |
| 2. Datos asociados en Internet . . . . .                     | 174 |
| IV. Excepciones al secreto . . . . .                         | 174 |
| 1. Por mandato legal . . . . .                               | 175 |
| 2. El control judicial . . . . .                             | 176 |
| A) Anterior a la interceptación . . . . .                    | 176 |
| B) Posterior . . . . .                                       | 178 |
| V. El plazo de conservación de los datos asociados . . . . . | 179 |
| VI. Conclusiones . . . . .                                   | 182 |
| VII. Bibliografía . . . . .                                  | 182 |



# PRESENTACIÓN

En los últimos años hemos presenciado una evolución exponencial de las tecnologías y el surgimiento de las adjetivadas como «disruptivas», caracterizadas por utilizar mayormente datos para su entreno. En consecuencia, los datos cada vez cobran mayor relevancia en el mundo digitalizado en el que vivimos, hasta el punto en el que hay quienes señalan que se han convertido en la moneda de cambio del siglo XXI. Un claro ejemplo se encuentra en el caso de la empresa *Tools for Humanity*, la cual opera en diversos países del mundo recopilando datos biométricos a cambio de algunas criptomonedas. En paralelo, la normativa ha tenido que enfrentarse a un escenario cambiante para tratar de salvaguardar los derechos de las personas. A ello se suma que las problemáticas no solo afectan a agentes privados o públicos. En este sentido es imprescindible la existencia de una adecuada gobernanza de datos, ya que es una cuestión que afecta a todos los sectores productivos. No obstante, su incidencia es mayor en entidades o profesiones que, de algún modo, requieran tratar datos de sus clientes o usuarios como despachos de abogados, entidades financieras, institutos de investigación, centros sanitarios, entre otros.

Ante este contexto, es necesario abordar el tema desde una perspectiva multidisciplinar, aunando tanto las visiones de profesionales que en su día a día se enfrentan a los retos de la protección de datos como los análisis concienzudos de investigadores en la materia. El objetivo de este diálogo es la búsqueda de soluciones que no solo sean satisfactorias para quienes usan los datos, sino también para quienes los aportan. Encontrar el equilibrio adecuado entre el establecimiento de garantías suficientes para que los ciudadanos consideren protegidos sus derechos en relación con sus datos personales y la utilización de estos.

En la búsqueda de ese diálogo y soluciones, el pasado 21 de abril de 2023 se celebró el Seminario Internacional «Perspectivas transversales del Derecho a la Protección de Datos Personales», organizado por la Universidad de Oviedo con la inestimable colaboración de la Universidad de Guadalajara (México), la Cátedra Rafael del Riego de Buen Gobierno y REDALC, en el marco del Proyecto Nacional MCIU-22-PID2021-126784NB-I00.

Dirigida por las Doctoras Raquel Pérez Díaz, Diana Paola González Mendoza y Paula Vega García, el evento se convirtió en un foro donde poner sobre la mesa algunas de las cuestiones más apremiantes en materia de protección de datos como son el tratamiento en los ficheros de morosos o las plataformas de resolución de conflictos, el secreto fiscal, los datos médicos o la privacidad de grupos. Para ello se invitó a participar a ponentes de España y México, a los que se les unió una docena de comunicantes. En esta obra se recogen algunos de los resultados de las investigaciones presentadas en las intervenciones de aquel Seminario, con la esperanza de que puedan traer luz sobre problemas acuciantes en la materia.

**Raquel Pérez Díaz**  
**Diana Paola González Mendoza**  
**Paula Vega García**

*Directoras del Seminario*

# **PROTECCIÓN DE DATOS Y FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO: ESTADO DE LA CUESTIÓN A LA LUZ DE LAS ÚLTIMAS RESOLUCIONES JUDICIALES**

**Natalia Muñiz Casanova**

*Profesora Asociada Departamento de Derecho Privado y de la Empresa  
Doctora en Derecho*

## **I. Introducción**

La indebida inclusión de los datos de una persona en un registro de solvencia patrimonial y crédito, popularmente conocido como derecho de morosos, constituye un menoscabo de su derecho al honor que indudablemente debe ser reparado.

En España hemos estado inmersos en los últimos años en una oleada de reclamaciones masivas frente a entidades financieras motivadas por inclusiones de datos de sus clientes en este tipo de ficheros. Sin duda, las cifras de estos procedimientos resultan preocupantes y aconsejan un análisis certero de las circunstancias que nos han llevado a estar en esta situación. Se han vertido opiniones de todo tipo sobre esta cuestión. Hay quien considera que la vulneración de la normativa protección de datos por parte de las entidades financieras es consciente y está dirigida a utilizar este tipo de ficheros como herramienta para forzar la recuperación de sus deudas. No comparto esta visión. Creo, más bien, que en estas reclamaciones subyace un problema de indefinición del procedimiento a seguir en la tramitación del alta en estos ficheros y de prueba por parte de las entidades financieras.

No puede obviarse la existencia de errores de operativa bancaria<sup>1</sup> y algún problema de suplantación de personalidad<sup>2</sup> pero, en la mayor parte de los supuestos que he analizado con motivo de este trabajo, los datos que se comunicaron a estos ficheros correspondían a personas que mantenían deuda vencida, líquida y exigible, con la entidad comunicante. En un porcentaje muy alto, la cuestión que hizo que el juez se inclinara a considerar vulnerado el derecho al honor del solicitante radica en la incapacidad de las entidades financieras de acreditar (i) la existencia de una reclamación previa a la incorporación de los datos al fichero y (ii) la advertencia de inclusión de los datos en el referido fichero de morosos en caso de no atender la reclamación de pago. Tras ambas cuestiones existe un problema que tiene su origen, a mi modo de ver, en las dudas sobre del procedimiento a seguir para la tramitación del alta que, en buena medida, vienen dadas por las incertidumbres en torno a la normativa aplicable.

El objeto del presente trabajo no es otro que el de exponer el estado de la jurisprudencia sobre las cuestiones controvertidas que abrieron la brecha de estas reclamaciones masivas y que hoy, gracias a la labor judicial, se encuentran en una situación más contenida.

## **II. Existencia de una deuda vencida, líquida, exigible y cierta**

Para que proceda el alta de un cliente bancario en un fichero de solvencia patrimonial y crédito ha de partirse de la existencia de una deuda vencida, líquida y exigible<sup>3</sup>. Esto no suele ser motivo de controversia. La mayoría de entidades financieras pueden acreditar con solvencia estos tres requisitos. Los problemas en este ámbito suelen pivotar sobre la certeza de la deuda.

- 
- 1 Muy frecuentes, por ejemplo, cuando las sucursales cancelan una tarjeta o una cuenta corriente y, con posterioridad al cierre, el sistema liquida unas comisiones que no fueron tenidas en cuenta. Se genera de este modo una deuda que puede no ser notificada al cliente al estar ya de baja su cuenta pero que, al no resultar atendida, finalmente se comunica al fichero.
  - 2 Estos supuestos de suplantación, en mi experiencia, se producen más en casos de operadoras de telefonía que en el sector financiero.
  - 3 Así lo contempla, entre otras muchas, la STS 174/2018, de 23 de marzo, en la que se indica lo siguiente: «La calidad de datos de los Registros de morosos. Es determinante para enjuiciar la solvencia económica de los interesados la existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada, y que se haya requerido de pago al deudor, informándole que en caso de no producirse el pago en el término previsto para ello y cumplirse los demás requisitos, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento (...) El principio de calidad de datos no se limita a exigir la veracidad de la deuda. Es pertinente la inclusión en estos ficheros de aquellos deudores que no pueden o no quieren, de modo no justificado, pagar sus deudas, pero no aquellos que legítimamente discrepan del acreedor respecto de la existencia y cuantía de la deuda».

Para que el alta en el fichero se repunte correcta la deuda, además de vencida, líquida y exigible, debe ser cierta. La certeza de la deuda implica que es inequívoca, indudable y no controvertida. Si el titular de los datos considera legítimamente que no debe lo que se reclama, y así se lo ha hecho saber al acreedor, la falta de pago no es indicativa de la insolvencia y, por tanto, la inclusión de los datos del cliente en uno de estos ficheros no es pertinente.

Es importante tener presentes las aclaraciones que la jurisprudencia ha ido haciendo sobre esta cuestión. La primera de ellas es que la controversia sobre la deuda tiene que ser anterior a la inclusión del dato en el fichero y no posterior al mismo. Se pronuncia sobre esta cuestión la STS 832/2021, de 1 de diciembre, en la que se establece lo siguiente: «Si la controversia a la que alude se expresó en su oposición a la ejecución y esta se inició con posterioridad a la inclusión de sus datos en el fichero, sostener que dicha inclusión resultaría ilegítima por falta de certeza y exactitud de la deuda por cuanto que la misma estaba siendo objeto de controversia, no tiene ninguna lógica, dado que la inclusión se produjo antes de que la deuda se controvertiera. Cosa distinta es que, una vez controvertida esta, los datos que ya habían sido incluidos en el fichero, en vez de cancelarse o rectificarse se mantuvieran».

Otra importante puntualización realizada por los tribunales es que, la existencia de esas discrepancias sobre la deuda, deben de ser comunicadas al acreedor y ha de formularse una oposición fundada ya que, de otro modo, bastaría alegar cualquier excusa incierta para evitar el trámite de inscripción. En este sentido, la STS 245/2019, de 15 de abril, indica, de forma expresa, que: «no cabe cualquier oposición al pago de una deuda para calificarla de incierta o dudosa, pues de ser así la certeza y exigibilidad de la deuda quedaría al exclusivo arbitrio del deudor».

Pero, el aspecto que ha dado lugar a mayores divergencias jurisprudenciales es si, el hecho de comunicar una deuda por un importe distinto del real afecta al requisito de certeza y da lugar a que la inscripción vulnere el derecho al honor de la persona cuyos datos se comunican. Las distintas Audiencias mantuvieron posiciones encontradas al respecto que fueron resueltas por el TS en sus STS 671/2021, de 5 octubre y STS /2022 de 14 de septiembre<sup>4</sup>. Consideran estas resoluciones que no vulnera el derecho al honor del cliente el hecho de que la cantidad comunicada al fichero no sea la correcta. Lo que vulnera el derecho al honor del afectado es que se le de tratamiento de moroso sin serlo realmente.

4 En concreto, recoge esta sentencia que: «La discordancia entre la cantidad por la que se practicó el requerimiento de pago en 2017 y la que en el año 2020 figura en el fichero de solvencia patrimonial no determina por sí sola que haya existido una vulneración del derecho al honor de la demandante. Como afirmamos en la sentencia 671/2021, de 5 de octubre, "lo verdaderamente relevante para que pudiera considerarse infringido el derecho al honor de los demandantes [...] no es tanto la corrección de la concreta cantidad en que el banco cifró la deuda, sino que se hubiera comunicado a la CIRBE sus datos personales asociados a datos económicos de los que resultara su condición de morosos, sin serlo realmente"».

### III. El requerimiento previo de pago

El gran problema que debían afrontar los bancos cuando recibían una demanda por vulneración del derecho al honor como consecuencia del alta indebida de los datos de un cliente en un fichero de solvencia patrimonial y crédito era acreditar que le habían requerido previamente el pago y facilitado información sobre la posible inclusión de sus datos en el mencionado registro. Este requerimiento de pago, tal y como el TS se ha cuidado de recordar, no es simplemente un requisito formal cuyo incumplimiento únicamente pueda dar lugar a una sanción administrativa. Se trata de un verdadero requisito esencial que responde a la finalidad del fichero y que trata de evitar la inclusión de personas que, por un simple descuido, por un error bancario al que son ajenas, o por cualquier otra circunstancia de similar naturaleza, han dejado de hacer frente a una obligación, sin que ese dato sea pertinente para enjuiciar su solvencia.

Pese a la relevancia del requerimiento y, a buen seguro por una cuestión de costes, estas comunicaciones a los clientes no se enviaron por correo certificado con acuse de recibo y certificación de texto. La mayoría de las entidades lo que hicieron fue contratar una empresa externa de mensajería a la que encomendaron el envío de estas notificaciones. La remisión del requerimiento de pago por esta vía no planteaba ninguna duda a las entidades sobre su valor como medio de prueba ya que había sido expresamente admitida por la Agencia Española de Protección de Datos, siempre y cuando se cumplieran unos requisitos mínimos de trazabilidad.

Pero los juzgados no consideraron suficientemente probado el requerimiento remitido de este modo. Estimaron muchas demandas pese a que las entidades financieras sostenían firmemente que habían requerido de pago a los deudores. Acreditaban esta manifestación con los certificados que aportaban las empresas de mensajería en los que se ponía de manifiesto que la carta dirigida al deudor había sido entregada por la entidad para su remisión y se había enviado al domicilio facilitado, sin que existiera constancia de su devolución. Como he indicado, los juzgados no consideraban suficiente esta prueba ya que, aun admitiendo que el envío se hubiera efectuado, no existía constancia ni del contenido de la carta ni de su recepción.

De nuevo el TS ha ido paulatinamente poniendo orden sobre esta cuestión. Las primeras resoluciones que abordaron esta controversia, aunque, desde mi punto de vista, no la cerraron del todo, son las SSTS 81/2022, de 2 de febrero y de 13 de octubre de 2022. En la primera de ellas, el alto Tribunal aclara que los certificados aportados por las empresas encargadas de los envíos masivos tienen validez como medio de prueba ya que no son ellas las que envían las cartas, sino que las entregan a Correos y lo que hacen es unir los certificados que aporta el servicio de Correos, que es un organismo público o semipúblico que cuenta con total fiabilidad<sup>5</sup>.

---

5 En concreto en la referida STS, de 2 de febrero de 2022, establece lo siguiente: «La misiva de requerimiento de pago y de apercibimiento, redactada por la demandada Primrose

Aclara también la STS de 13 de octubre que, aunque el requerimiento tiene naturaleza recepticia no es necesario que el sujeto a quien va dirigida llegue a conocer la reclamación ya que no puede dejarse a la voluntad del deudor requerido la recepción y el conocimiento del contenido de las notificaciones<sup>6</sup>.

Por su parte, la STS 78/2023, de 27 de septiembre, viene a establecer la posibilidad de deducir la recepción de la notificación de una suerte de prueba de presunciones. En concreto, indica la mencionada resolución que «la dirección a la que se envió la carta que lo contenía es idónea. Fue la que la propia recurrente señaló en el contrato, y no consta que, tal y como se había pactado, esta comunicara a la recurrida su cambio. (...) De otra parte, la sentencia recurrida no conculca nuestra doctrina sobre el carácter recepticio del requerimiento previo de pago, que, como hemos dicho reiteradamente, no exige la fehaciencia de su recepción, puesto que esta se puede considerar fijada a través de las presunciones siempre que exista garantía o constancia razonable de ella (por todas, sentencias 863/2023, de 5 de junio, 960 y 959/2022, de 21 de diciembre), que en el presente supuesto existe, al ser idónea la dirección a la que se envió la carta conteniendo el requerimiento, acreditarse su admisión para envío por el servicio postal de correos y no

---

Partners Ltd, aparece en los autos y su lectura no deja lugar a duda alguna; Servinform, S. A., como prestadora, en favor de la demandada, de un servicio de envío de esta clase de notificaciones de modo masivo, etc. (en virtud de una previa relación contractual), certifica que en fecha 8-5-2018, vamos a decirlo así, "prepara" y gestiona el envío de la citada misiva de requerimiento dirigida al demandante, junto con otras muchas más (supera las cien), y las deposita todas ellas en el Servicio de Correos correspondiente.(...) Podrá argüirse lo que se quiera al respecto de si es o no una empresa ajena a la demandada, pero, el que prepare o gestione en favor la demandada el envío de la carta conteniendo los cuestionados requerimiento y apercibimiento al demandante, es algo que no puede negarse, siendo así que el enfoque esencial ha de ponerse más bien en la circunstancia o extremo fáctico de que quien garantiza que se verificó el envío de la carta al domicilio del demandante no lo es tanto ninguna de las citadas empresas, como el mismo Servicio estatal de Correos. (...) Quiere decirse que, en nuestro caso, fuera quien fuera quien se encargara de gestionar la carta de requerimiento y apercibimiento, a la postre, no puede dejarse de ponderar que su remisión al Sr. Roberto se instrumenta a través del citado servicio de Correos, o sea, a través de un organismo público o semipúblico, que es el que da verificación de que esa carta se ha dirigido y enviado al domicilio del demandante, precisamente a aquel que este demandante facilitó a la hora de suscribir el contrato de préstamo litigioso. (...) "Y, el albarán de entrega de Correos, que aparece unido a este procedimiento, da fe de la recepción en sus oficinas de aquellas misivas, entre ellas la enviada al apelante. Quien materializa la entrega de la carta-notificación es el Servicio de Correos, no aquellas empresas, con independencia de que una de ellas como empresa del servicio de gestión de cartas devueltas de notificación de requerimientos de pago, pueda ostentar a su vez la condición de ser una empresa de gestión del registro de morosos de ASNEF, etc."»

- 6 Contempla esta sentencia que el requerimiento de pago es un acto de comunicación de carácter recepticio que exige una constancia razonable de la recepción de la comunicación por parte del destinatario, pero no se exige fehaciencia de dicha recepción que puede ser probada por diversos medios, incluso a través de presunciones, si bien se exige una cierta constancia de la comunicación al destinatario.

constar su devolución, no existiendo de otra parte dato alguno con reflejo en los autos del que se pueda inferir que la carta no llegara a su destino o que su recepción se hubiera malogrado por razones achacables al prestador del servicio postal encargado responsable de entregarla al destinatario».

No obstante, el problema, para un buen número de juzgados, no es tanto que se pueda acreditar el envío y, en su caso, recepción de una comunicación al cliente, sino cuál es su contenido concreto cuando no hay otros medios, más allá del propio requerimiento, para acreditar que, quien considera su honor vulnerado por el alta del dato en el fichero de morosos, conocía la deuda. De ahí que sea importante para las entidades financieras llevar al pleito cualquier tipo de prueba que permita acreditar que la existencia deuda no es desconocida para el cliente<sup>7</sup>.

Un problema añadido era que algunas entidades no informaban expresamente en este requerimiento de la posible inclusión de los datos en el fichero de solvencia patrimonial y crédito porque lo consideraban innecesario ya que esta advertencia se había hecho constar ya en el contrato del que dimanaba el alta. Este fue también un motivo que llevó a la estimación de muchas demandas frente a las entidades y que dio lugar a una controvertida jurisprudencia menor. La STS, 945/2022, de 20 de diciembre aclaró definitivamente esta cuestión al señalar que, con la nueva regulación de la Ley 3/2018, no es necesario que en el requerimiento de pago se advierta de la posibilidad de incluir los datos en un fichero de morosos en caso de impago, siempre que esa advertencia haya sido efectuada en el momento de contratar.

## **IV. Controversia respecto a la normativa aplicable**

Otra importante controversia se planteó respecto de los asuntos en los que el alta en el fichero de solvencia patrimonial y crédito se había producido con posterioridad a la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos

---

7 En este sentido resulta muy esclarecedora la sentencia de la Sección Séptima de la Audiencia Provincial de Asturias, de 20 de abril de 2023, en la que se establece lo siguiente: «Pero es que, en el caso de autos, todos los antecedentes llevan a concluir que tales requerimientos fueron recibidos por el demandante, y así, al igual que las ya mencionados, la apelante acompañó a su contestación varias cartas reclamando el pago de las deudas que se iban generando como consecuencia de la citada operación, en todas ellas figura el mismo domicilio del actor, que es el que figura en el contrato, y si bien es cierto que no hay constancia fehaciente de su envío y recepción, parece razonable estimar que así aconteció, pues responde la operativa general de los bancos en este tipo de situaciones. Además, el propio hecho que, en algunos casos la deuda aparentemente se regularizase permite concluir la realidad de tal envío, no existiendo la más mínima explicación del motivo por el que las misivas no fueron recibidas, cuando hay constancia de que sí lo fue la que se le comunicaba la inclusión de los datos en el fichero...».

# PERSPECTIVAS TRANSVERSALES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

---

En un mundo cada vez más digitalizado y globalizado, los datos personales adquieren mayor protagonismo en los diversos ámbitos en los que se desarrollan los individuos, convirtiéndose en el recurso más valioso del siglo XXI.

Bajo la dirección académica de las Doctoras Raquel Pérez Díaz, Diana Paola González Mendoza y Paula Vega García, este libro ofrece un análisis transversal y exhaustivo sobre el derecho a la protección de datos personales tanto en el ámbito nacional como internacional. Es resultado del Seminario Internacional «Perspectivas transversales del Derecho a la protección de datos personales», organizado por la Universidad de Oviedo, llevado a cabo el 23 de abril de 2023.

Así pues, en su interior se pueden encontrar trabajos que analizan tratamientos de datos personales específicos, como la confidencialidad en el tratamiento, los realizados por Administraciones tributarias, los que se derivan de la comprobación de solvencia patrimonial, los realizados en el marco de resolución de conflictos a través de plataformas digitales, los llevados a cabo por detectives privados, los que se derivan de los juicios penales en México, los que se realizan con motivo del uso de tecnologías de reconocimiento facial y los realizados por las Instituciones Europeas. Algunos trabajos abordan tratamientos realizados en sectores específicos como el financiero, en consumo y el sanitario. De esta manera, su contenido ofrece una visión jurídica actual en la materia.

---

## DIRECCIÓN

Raquel Pérez Díaz, Diana Paola González Mendoza y Paula Vega García

## AUTORES

Carmen Cabal Fernández, Gonzalo Campos Rivera, José Antonio Castillo Parrilla, Natalia Menéndez González, Natalia Muñiz Casanova, Pablo Muruaga Herrero, Paola Jackeline Ontiveros Vázquez, Luis Pérez Fernández, Emma Rodríguez Montes, Israel Santos Flores, Jorge Alberto Vázquez Segura y Carlos Enrique Vigil de Quiñones Fernández

Proyecto PID2021-126784NB-I00 financiado por:



PVP: 25,00 €

ISBN: 978-84-1194-764-0



OA