NECESIDAD DE DAÑO PARA QUE LA INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DÉ LUGAR A INDEMNIZACIÓN*

Comentario a la STS 398/2024, de 19.03 (ECLI:ES:TS:2024:1495)

José María Martín Faba
Profesor Ayudante Doctor UAM
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 16 de mayo de 2024

1. INTRODUCCIÓN

La STS 398/2024, de 19.3., proporciona una clara demostración de que, a pesar de producirse una vulneración de la normativa de protección de datos personales, el derecho a indemnización no nace si el demandante no prueba la existencia de unos daños reales.

2. HECHOS

Los días 15 y 17 de octubre de 2013 y 15 de enero de 2014, Dña. Beatriz, empleada de SURAVAL S.G.R., realizó una consulta de solvencia patrimonial de D. Eugenio (hermano) y Dña. Aida (sobrina) en el fichero de ASNEF, a través de la empresa y utilizando el usuario y clave que para ello tenía asignados.

El 28 de abril de 2014, D. Eugenio y Dña. Aida dirigieron un escrito a SURAVAL en el que solicitaban información sobre el motivo de tales consultas y, tras no obtener respuesta, el 13 de junio de 2014 y el 8 de julio de 2014 presentaron sendas denuncias ante la Agencia Española de Protección de Datos, que incoó un expediente, en el que Dña.

* Trabajo realizado en el marco del Proyecto de Investigación PID2021-128913NB-I00, del Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación (AEI) cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) titulado "Protección de consumidores y riesgo de exclusión social: seguimiento y avances", dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato, en el marco del Proyecto de Investigación SBPLY/23/180225/000242 "El reto de la sostenibilidad en la cadena de suministros y la defensa del consumidor final" cofinanciadas por el Fondo Europeo de Desarrollo Regional, en el marco del Programa Operativo de Castilla-La Mancha 2021-2027 dirigido por Ángel Carrasco Perera y Ana Carretero García.

Beatriz reconoció la utilización de la clave de la empresa SURAVAL para acceder al fichero ASNEF y consultar los datos de solvencia de su hermano y sobrina por un interés personal y al margen de la empresa para la que trabajaba.

A raíz de este reconocimiento, SURAVAL incoó un expediente disciplinario a la Sra. Beatriz y le impuso una sanción de suspensión de empleo y sueldo. El 9 de septiembre de 2015, la Agencia Española de Protección de datos dictó una resolución en el mencionado expediente administrativo que impuso a Dña. Beatriz, como autora de una infracción del artículo 6.1 de la LOPD, una multa de 1.500 €.

D. Eugenio y Dña. Aida presentaron sendas demandas contra Dña. Beatriz y SURAVAL los días 27 de julio de 2016 y 24 de octubre de 2016, que fueron acumuladas. Basaban su reclamación en una vulneración del derecho al honor, a la intimidad y a la protección de datos de carácter personal, solicitando una indemnización por daños y perjuicios valorados en 45.000 euros.

Previa oposición de los demandados, la sentencia de primera instancia desestimó la demanda. Respecto de las pretensiones formuladas contra la Sra. Beatriz, argumentó que la acción ejercitada era la de protección civil del derecho al honor del artículo 7.7 LO 1/1982, por la consulta efectuada por ella, y no una acción basada en el derecho a la protección de datos al amparo de la LOPD. Tras lo cual, descartó que existiera intromisión ilegítima en el derecho al honor, porque lo que se produjo fue una investigación patrimonial que no afectaba a dicho derecho fundamental y que fue sancionada en la vía administrativa correspondiente. Asimismo, desestimó la acción de responsabilidad civil extracontractual dirigida contra SURAVAL, porque a pesar de haber cumplido todos los protocolos y medidas de seguridad previstos con el fin de garantizar el acceso a los datos personales de ASNEF por usuarios registrados de la propia empresa, no pudo evitar el mal uso en dichos accesos realizados por su empleada que de ninguna manera eran consentidos ni conocidos.

El recurso de apelación de los demandantes fue desestimado por la Audiencia Provincial. En lo que ahora interesa, confirmó que no existía responsabilidad civil extracontractual de SURAVAL. En cuanto a la intromisión ilegítima en la intimidad por parte de la empleada, consideró que no se había vulnerado porque la mala situación económica del Sr. Eugenio constaba en diversos registros públicos. Y concluyó que la actuación ilícita de la empleada fue sancionada laboral y administrativamente, sin que se aprecie razón para que los demandantes se lucren de una suerte de daños punitivos (de no escasa cuantía) ajenos a la estructura del Derecho de Daños en nuestro ordenamiento.

Los demandantes interpusieron sendos recursos de casación, con motivos coincidentes tanto en las infracciones denunciadas como en sus argumentaciones, por los que el Tribunal Supremo los resuelve conjuntamente para evitar reiteraciones. Con todo, aquí solo trataremos el segundo motivo del recurso de casación.

3. FUNDAMENTO DE DERECHO: NO HAY INDEMNIZACIÓN SIN DAÑO

Los recurrentes argumentan, sintéticamente, que la consulta no autorizada de un fichero de datos personales no solo tiene consecuencias de orden administrativo, sino que también supone una intromisión ilegítima en el derecho fundamental a la intimidad de los demandantes, infringiendo la sentencia recurrida los artículos 18 CE y 6.1 y 20.e) de la LOPD.

En realidad, los recurrentes no basan expresamente su derecho a indemnización en el artículo 82 RGPD, que no era aplicable por razones transitorias, sino en una amalgama de infracciones de derechos fundamentales, entre las que se encuentran el honor, la intimidad, y la protección de datos personales. El Tribunal Supremo, después de establecer las líneas divisorias entre los mencionados derechos, acaba refiriéndose al artículo 82 RGPD, y lo utiliza para resolver la controversia.

Así, el Tribunal Supremo trae a colación la STJUE de 4 de mayo de 2023, C-300/21 (que, aunque se refiere al art. 82 RGPD, su doctrina es aplicable a la legislación anterior). Según la mencionada STJUE, no puede considerarse que toda infracción de las disposiciones sobre protección de datos personales dé lugar, por sí sola, a un derecho a una indemnización a favor del interesado. Por el contrario, para la pertinencia de la indemnización deberían concurrir tres requisitos cumulativos: (i) un tratamiento de datos personales en infracción de las disposiciones legales pertinentes; (ii) la existencia de daños y perjuicios para el interesado; y (iii) una relación de causalidad entre dicho tratamiento ilícito y esos daños y perjuicios.

La referida STJUE declara que “la realización de daños y perjuicios en el marco de tal tratamiento solo es potencial; [...] la infracción del RGPD no conlleva necesariamente daños y perjuicios, y [...] debe existir una relación de causalidad entre la infracción en cuestión y los daños y perjuicios sufridos por el interesado para fundamentar un derecho a indemnización”. Insiste la STJUE en que una cosa es la infracción de la normativa sobre protección de datos, que puede dar lugar a una sanción administrativa y otra la obtención de una indemnización que no puede ser automática; sin que quepa una equiparación lineal entre infracción e indemnización.

En igual sentido, la STJUE de 14 de diciembre de 2023, C-456/22, declara que es preciso que el afectado pruebe que la vulneración de la normativa de protección de datos le haya causado algún perjuicio, por mínimo que sea, y que "el interesado debe demostrar que las consecuencias de esa infracción que afirma haber sufrido constituyen un perjuicio distinto de la mera infracción de las disposiciones de dicho Reglamento".

Según el Tribunal Supremo, en este caso únicamente concurre el primero de los requisitos indicados que, por sí solo, es insuficiente a los efectos pretendidos por los demandantes. Aunque el acceso a los datos patrimoniales de los demandantes se hizo a través de un fichero de solvencia patrimonial, las demandadas no incluyeron a los actores en ningún fichero de tales características. No hubo revelación de datos personales pues esos datos ya eran públicos, puesto que, en registros de dicha naturaleza, como el de la Propiedad, figuraban diversos embargos. No consta que la mera consulta por la demandada de los datos personales de la demandante tuviera ninguna relevancia externa o su resultado fuera conocido por terceros, ni que se causara perjuicio alguno a los demandantes. En consecuencia, el motivo de casación es desestimado.

4. COMENTARIOS

1. El Tribunal Supremo afirma que hay una infracción del RGPD, aunque no especifica quién la ha cometido y porqué. Según se desprende de los hechos de la sentencia, la empleada de SURAVAL S.G.R ha consultado datos personales de los demandantes sin existir una base legitimadora para ello, contraviniendo el artículo 6.1 RGPD. En principio, todo tratamiento de datos personales realizado por empleados en el ámbito de las actividades de una organización se presumirá realizado bajo el control de dicha organización. No obstante, es posible que, como sucede en el caso comentado, un empleado decida consultar ilícitamente datos personales para sus propios intereses, extralimitándose en el ejercicio de las funciones que le ha atribuido la empresa responsable del tratamiento. En efecto, no parece que el incumplimiento del RGPD pueda imputarse a SURAVAL, pues la empleada actúo con dolo, independientemente y en contra de las instrucciones de la empresa. En consecuencia, SURAVAL no habría incumplido el principio de responsabilidad proactiva, por no adoptar las medidas apropiadas para garantizar un tratamiento de datos personales conforme al RGPD (arts. 24 y 32). En otras palabras, la empresa habría actuado con toda la diligencia de un padre de familia, por lo que no respondería del acto doloso de su dependiente (art. 1903. VII CC). Si se considerara que SURAVAL no ha infringido el RGPD, los demandantes no podrían reclamarle una indemnización basada en el artículo 82 RGPD.

2. ¿Cabría entonces que los demandantes exigieran una indemnización a la empleada de la empresa, con fundamento en el artículo 82 RGPD, por consultar datos personales sin

existir una base legitimadora para ello, infringiendo el artículo 6.1 RGPD? Nótese que, según el artículo 82 RGPD, quien paga la indemnización es el responsable del tratamiento (o el encargado). El responsable del tratamiento es "la persona física o jurídica (...) que, solo o junto con otros, determine los fines y medios del tratamiento (…)" (art. 4.7 RGPD), esto es, el porqué y el cómo del tratamiento. Las empresas asociadas a AESNEF, como SURAVAL, determinan los fines de los datos personales que consultan (tratan ex art. 2.2 RGPD). En efecto, dichas empresas consultan datos personales para sus políticas comerciales, decidiendo en virtud de la consulta efectuada si, por ejemplo, conceden un aval o un crédito o lo deniegan. Ahora bien, es dudoso que pueda considerarse que la empleada de SURAVAL determina los fines y medios del tratamiento, y que, en consecuencia, pueda ser calificada como responsable del tratamiento. Normalmente, los empleados que realizan el tratamiento de los datos personales en su organización lo hacen en cumplimiento de las instrucciones proporcionadas por la propia organización como responsable del tratamiento. Con todo, cuando un empleado consulta ilícitamente datos personales incumpliendo las instrucciones de su organización, puede considerarse que dicho empleado es responsable del tratamiento, porque la consulta de los datos personales se ha realizado conforme a los fines e intereses de la propia empleada, y no conforme a los fines e intereses de su empleador. Si el empleado trata datos personales para sus propios fines, distintos de los del empleador, debe considerarse que aquel es responsable del tratamiento. Por lo tanto, en este caso, la empleada puede ser considerada responsable del tratamiento, y al haber infringido el artículo 6.1 RGPD, los interesados pueden reclamarle una indemnización basada en el artículo 82 RGPD.

3. A pesar de que los demandantes puedan dirigir su acción indemnizatoria basada en el artículo 82 RGPD frente a la empleada, no nace el derecho a indemnización. Por un lado, porque, aunque la empleada haya infringido el RGPD, los demandantes no sufren un daño moral consistente en el temor, ansiedad o preocupación por un futuro uso indebido de sus datos personales por parte de terceros. En efecto, la empleada que consultó sin autorización los datos personales de los demandantes no los reveló a terceros, por lo que la consulta no tuvo trascendencia externa. El temor a un futuro uso indebido de los datos personales por parte de terceros sería entonces infundado, improbable e hipotético. Por otro lado, no hay relación de causalidad entre la consulta no autorizada de los datos personales por parte de la empleada y que dichos datos puedan ser conocidos por terceros y usados indebidamente en el futuro. Aunque la empleada no hubiera consultado tales datos personales, y hubiera ajustado su conducta a la prescrita por el RGPD (conducta lícita alternativa), los datos sobre la mala situación económica del demandante serían igualmente accesibles a terceros, al figurar en un registro público. En consecuencia, los demandados quedarían exentos de responsabilidad por no ser "en modo alguno responsables del hecho que haya causado los daños y perjuicios (art. 82.3 RGPD)