El responsable del tratamiento de los datos de carácter personal responde por la actuación culpable de sus empleados en la violación de las medidas de seguridad existentes en materia de protección de datos

Se plantea en el presente recurso si las infracciones de la LOPD por fallos de las medidas de seguridad que puedan cometer los empleados de una persona jurídica deben examinarse en atención al resultado y, por tanto, imputarse a la persona jurídica de la que depende el empleado, con independencia de los medios y medidas de prevención que hubiera podido adoptar.

Para dar respuesta a esta cuestión la Sala examina el tipo de obligación que implica la adopción de las medidas de seguridad en materia de protección de datos, la responsabilidad de las personas jurídicas en relación con las mismas y por los incumplimientos de sus empleados. Al respecto señala que no basta con diseñar los medios técnicos y organizativos necesarios, también es necesaria su correcta implantación y utilización de forma apropiada, de modo que responderá de la falta de la diligencia en su utilización. Como en una reciente sentencia ha sostenido la Sala, el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros.

TRIBUNAL SUPREMO

Sala de lo Contencioso-Administrativo

Sección 3.ª

Sentencia 188/2022, de 15 de febrero de 2022

RECURSO DE CASACIÓN Núm: 7359/2020

Ponente Excmo. Sr. DIEGO CORDOBA CASTROVERDE

En Madrid, a 15 de febrero de 2022.

Esta Sala ha visto por los magistrados indicados al margen, el recurso de casación número 7359/2020 interpuesto por la mercantil COMMCENTER, S.A., representada por la procuradora de los tribunales doña Adela Gilsanz Madroño, bajo la dirección letrada de don Xavier Saula Adell, contra la sentencia de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 22 de julio de 2020, en el recurso contencioso administrativo número 136/2019.

Ha sido parte recurrida la Administración General del Estado, representada por el Sr. Abogado del Estado.

Ha sido ponente el Excmo. Sr. D. Diego Córdoba Castroverde.

ANTECEDENTES DE HECHO

PRIMERO. La Procuradora de los Tribunales doña Adela Gilsanz Madroño, actuando en nombre y representación de la entidad "Commcenter, S.A" interpone recurso de casación contra la sentencia de la Sección Primera de la Sala de lo Contencioso-administrativo de la Audiencia Nacional de 22 de julio

de 2020 (rec. 136/2019) por la que se desestimó el recurso interpuesto por dicha entidad contra la resolución de la directora de la Agencia Española de Protección de Datos de 27 de noviembre de 2018 y contra la resolución de 3 de octubre de 2018 que impuso a dicha entidad una sanción de 40.001 € por infracción del art. 9.1 de la LOPD, tipificada como grave en el art. 44.3.h) de dicha norma.

Los hechos por los que se sancionó a la empresa recurrente pueden sintetizarse en los siguientes: en las solicitudes de financiación de productos de telefonía de distintos clientes con la entidad Telefónica Consumer Finance, S.A.U. figuraba una dirección de correo electrónico que no correspondía a los clientes-solicitantes, con la consecuencia de que se permitió el acceso no autorizado por parte de terceros, al menos a 14 solicitudes de financiación, en las que obraban datos personales de los clientes (nombre y apellidos, datos económicos, de domiciliación bancaria y firma).

SEGUNDO. Mediante Auto de 8 de abril de 2021 se admitió el recurso de casación declarando que la cuestión que presenta interés casacional objetivo para la formación de la jurisprudencia, consiste en determinar si las infracciones de la Ley de Protección de Datos por fallos de las medidas de seguridad que puedan cometer los empleados de una persona jurídica, deben examinarse en atención al resultado y, por lo tanto, imputarse a la persona jurídica de la que dependa el empleado, con independencia de los medios y medidas de prevención que hubiera podido adoptar.

TERCERO. El escrito de interposición argumenta, en síntesis, que:

La recurrente, COMMCENTER, comienza afirmando que trabaja a tres niveles distintos:

1. En la compra y venta de productos de telefonía, comunicaciones y asimilados, actúa por su cuenta y riesgo, con sus propios programas y tarifas, y formalizando una relación directa entre COMMCENTER y el cliente.

2. En cuanto a las altas de línea y otros productos ofertados por Movistar, actúa en nombre y por cuenta de Movistar, haciendo de intermediario en la formalización de la relación contractual entre TELEFONICA DE ESPAÑA S.A.U. y el Cliente.

3. En cuanto a la financiación, actúa en nombre y por cuenta de TELEFÓNICA CONSUMER FINANCE, S.A.U., haciendo de intermediario en la formalización de la relación contractual entre ésta y el Cliente.

COMMCENTER tiene contratos de distribución y representación tanto con MOVISTAR como con TELEFÓNICA CONSUMER FINANCE.

Los empleados que trabajan en tiendas de COMMCENTER actúan bajo multitud de directrices impuestas por contrato: de imagen, de atención al cliente, de protocolos y, como no puede ser de otra manera, de cumplimiento normativo (como la Protección de Datos de Carácter Personal). Independientemente de las relaciones mencionadas, COMMCENTER tiene plena consciencia de que queda bajo su esfera de responsabilidad la recogida, introducción y envío de datos también cuando trabaja en nombre y por cuenta de MOVISTAR y/o TELEFÓNICA CONSUMER FINANCE.

Si nos centramos en concreto en el caso de los contratos de financiación, COMMCENTER se encarga tanto de la toma de datos como del envío que se hace tanto a TELEFÓNICA CONSUMER FINANCE como al afectado para que tenga una copia, pues normalmente habrá rellenado una solicitud de financiación con un dispositivo electrónico (tipo tableta).

Las medidas de seguridad relativas al sistema informático no dependen de COMMCENTER, puesto que es un sistema que está ubicado, controlado y gestionado por TELEFÓNICA CONSUMER FINANCE, y también los protocolos de uso del Software los imponen ellos.

Aduce como irregularidad del procedimiento que ni en el acta de inspección ni en el informe de actuaciones previas se pone de manifiesto en ningún momento el incumplimiento de ninguna medida de seguridad por parte de COMMCENTER. La AEPD acuerda iniciar procedimiento sancionador a

COMMCENTER, alegando, que los hechos expuestos pueden suponer la comisión por parte de COMMCENTER de una infracción del artículo 4.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

Todas las alegaciones y pruebas aportadas respondían a la necesidad de desvirtuar la concurrencia de la eventual vulneración del artículo 4.3 de la LOPD. Entendiendo que la instrucción del proceso se había acordado para determinar si había lugar a sancionar la recurrente por un presunto ilícito que le era imputable, cometido por una empleada por el acto de introducir datos personales inexactos en los contratos de financiación.

En fecha 05/09/2018, sin más diligencias de investigación y sin solicitar más documentación a mi mandante, la AEPD emitió Propuesta de Resolución para sancionar a COMMCENTER, por una supuesta infracción del artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma.

Imponiendo una sanción por, supuestamente, no mantener los ficheros con las debidas condiciones de seguridad. Y en el antecedente tercero de la resolución sancionadora se comete la errata de señalar que el procedimiento sancionador a COMMCENTER se inició por presunta infracción del artículo 9.13 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (en lo sucesivo LOPD).

La AEPD impone sanción por una infracción del art. 9.1 LOPD tipificada como grave en atención al art.44.3.h) obviando por completo y sin examinar las medidas de diligencia en la Protección de los datos personales implantadas por la recurrente. Ni siquiera para modular la intensidad de la sanción.

Y en cuanto a la ausencia de culpa o dolo, la AEPD obvió los argumentos en relación al alcance restringidísimo y la ausencia total de daños. Con un total de 14 afectados por la pretendida brecha cuyos datos habían sido accedidos por una única persona, el denunciante. Y que, a mayor abundamiento, se había producido indudablemente por una acción conjunta acordada de forma irregular entre una empleada y las personas afectadas. Valga insistir que los contratos fueron enviados a la cuenta de correo que había sido autorizada y verificada como propia por parte de todas las personas afectadas.

En fecha 27/09/2018 la representación de COMMCENTER presentó escrito de alegaciones a la propuesta de resolución, en la línea de lo anteriormente argumentado, añadiendo, además, que también se obviaba una posible causa atenuante y que era la eventual responsabilidad de TELEFÓNICA CONSUMER FINANCE por el diseño del programa facilitado para la remisión de las solicitudes de financiación, que no disponía de un sistema de verificación de la veracidad del correo electrónico (sistema conocido como doble *opt-in*) algo que a día de hoy se considera básico en materia de seguridad de la información, que no dependía en ningún caso de mi mandante y que sin duda hubiera evitado que se hubiera producido la fuga objeto de autos.

Sentadas estas consideraciones previas aduce los siguientes motivos de impugnación:

Primero. El art. 9 de la LOPD 15/1999 no establece una obligación de resultado respecto de las medidas de seguridad.

Se alega, en primer lugar, que la sentencia recurrida establece, en relación con el artículo 9.1 LOPD (Medidas de Seguridad), una clarísima obligación de resultado que extiende *ultra vires*, la *ratio legis*. La parte recurrente entiende que esta obligación de resultado entra en contradicción con la legislación y jurisprudencia, que vienen a establecer una obligación de medios, considerando que el sujeto obligado a cumplir con la normativa de protección de datos debe diseñar e implantar las medidas de seguridad para evitar las eventuales brechas de seguridad y evitar ser sancionado por su incumplimiento. Al margen de que por un hecho fortuito o un acontecimiento de imposible previsión

se cree una brecha de seguridad que el sujeto no hubiera podido evitar siquiera aplicando las más estrictas medidas.

La sentencia recurrida establece que "Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen, o acaben en manos de terceros [...] y por tanto debe dar una explicación adecuada y razonable de cómo los datos personales han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues también es responsable de que las mismas se cumplan con rigor".

En definitiva, la sentencia (igual que las resoluciones administrativas emitidas por la AEPD) considera insuficientes por inoperantes todas las medidas de seguridad que hayan podido aplicarse, siempre que tenga lugar una brecha de seguridad de los datos, sea ésta de la naturaleza que sea. Pero no se examinan o valoran si las medidas de seguridad de los datos que tenía realmente implementadas la recurrente eran las adecuadas para cumplir con la normativa.

Configurarlo como una obligación de resultado invalida de facto todo esfuerzo e inversión tecnológica y organizativa que pudiere ser implementado en materia de seguridad de datos. Ni siquiera se tiene en cuenta para graduar la sanción.

Ni la LOPD 15/1999 (arts. 9 y 44.3 h) ni el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el reglamento de desarrollo (art. 79 a 100) hablan de una obligación de resultado, sino que hacen referencia a medios. Y lo mismo sucede con las previsiones contenidas en normas posteriores a estos hechos como el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y la LO 3/2018, de 5 de diciembre en los que se pone énfasis en la responsabilidad proactiva del obligado que debe adoptar las medidas que sean necesarias (medios) que en ningún caso se refiere a obligaciones de resultado.

En otras sentencias de la Audiencia Nacional se han anulado sanciones similares por no haberse acreditado el fallo en las medidas de índole técnica y organizativas que justifiquen la sanción.

Y en este caso se pregunta ¿Qué medidas de seguridad de los datos implementadas por Commcenter resultaron ser inadecuadas? ¿Acaso fue deficiente la formación en materia de protección de datos ofrecida a la trabajadora? O ¿Qué medidas podría haber implementado la recurrente para evitar la sanción?

Segundo. Inexistencia de una responsabilidad objetiva o sin culpa.

Como ha señalado el Tribunal Constitucional no resulta admisible en el derecho administrativo sancionadora la responsabilidad objetiva o sin culpa.

El art. 9.1 de la LOPD regula la obligación de la empresa de establecer las medidas de seguridad pertinentes para evitar que los datos sean expuestos o se ponga en peligro la integridad, confidencialidad y/o disponibilidad de los datos. Es un mandato directo a la empresa, no susceptible de ser cumplido por cualquier empleado, incluso regulándose hasta dónde llega la obligación de la empresa con sus empleados, explicando qué debe hacer para garantizar que las medidas se cumplen debidamente (art. 89 RDLOPD): "Artículo 89. Funciones y obligaciones del personal.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento".

En el presente supuesto se ha probado por parte de COMMCENTER que los empleados firman un compromiso de confidencialidad, que reciben una normativa de COMMCENTER sobre el tratamiento de datos, que reciben formación y que, adicionalmente, reciben protocolos emitidos por las empresas vinculadas al grupo Movistar y la AEPD consideró innecesario entrar a valorar las medidas implantadas

por la empresa. Por ello, es imposible imputar culpa directa y objetiva a la empresa por la infracción prevista en el art. 44.3 de la LOPD porque esto no se ha examinado ni se ha probado por parte del órgano sancionador.

La cuestión dudosa parece ser si ¿existe una responsabilidad subjetiva por una vulneración del artículo 9.1 LOPD por parte de la empleada (que se hará extensible por lo tanto a la empresa)?

La demandante considera que las circunstancias concretas del caso permiten extraer la conclusión de que no puede existir culpa o negligencia por parte de la empleada por vulneración del artículo 9.1 de la LOPD, ni, por extensión, de COMMCENTER, por varias razones:

1.º En primer lugar, podría discutirse una conducta culposa de la empleada si se hubiera alegado una eventual violación del artículo 4.3 LOPD (exactitud de los datos) o incluso del artículo 10 LOPD (deber de secreto), puesto que un empleado es susceptible de actuar unilateralmente y al margen de la empresa incluyendo intencionadamente o con falta de diligencia datos incorrectos o inexactos, como también podría, en las mismas condiciones, comunicar datos protegidos a terceros.

Pero, a entender de la recurrente, resulta extraño y contrario a la filosofía de la norma pretender afirmar que un empleado pueda vulnerar de forma culposa la obligación de la empresa de adoptar medidas de seguridad, obligación claramente dirigida a la empresa, pues implica el establecimiento de medidas de seguridad, corporativas y estructurales, en muchos casos tecnológicas o de procedimiento, cuyo diseño o implantación nunca quedará en manos de empleados no directivos o no vinculados con la implantación corporativa de medidas de seguridad técnicas u organizativas, y que por lo tanto no es una norma susceptible de ser cumplida o incumplida por empleados no vinculados a la implantación de estas medidas.

2.º En segundo lugar, estamos ante una ausencia de evento dañoso. Consideramos que hubiera sido dañoso el acceso no consentido a los datos personales de los 14 afectados por el destinatario del correo electrónico DIRECCION000. Pero medió no sólo el consentimiento del afectado, sino orden expresa y por escrito en todos los casos. Por todo lo anterior, esta parte considera que el elemento subjetivo necesario para imputar la responsabilidad a COMMCENTER es inexistente.

Tercero. Ausencia de modulación de la sanción por disminución cualificada de culpa.

La AEPD omite la apreciación de los criterios atenuantes previstos en los artículos 45.4 h), i, y j) y de los artículos 45.5. a), b) y c) de la LOPD. No puede aplicar atenuantes debido a que no analizó los mecanismos de seguridad de los datos habida cuenta de que, en el momento de la inspección, los funcionarios de la AEPD efectuaban las comprobaciones pertinentes en aras a acreditar (o desvirtuar) una posible infracción del art. 4.3 de la LOPD y no una infracción del art. 9.1 de la LOPD.

Y la AEPD no aplica el criterio de volumen reducido de datos (14 contratos) como atenuante sino como agravantes, desconociéndose los criterios utilizados por la Agencia para aplicar atenuantes o gravantes lo cual es contrario a la seguridad jurídica.

CUARTO. El Abogado del Estado se opone al recurso.

La contestación a la demanda transcribe parte de la STS de 15 de febrero de 2021 (rec. 1916/2020) referida a la responsabilidad de una Administración pública (en este caso, el Ayuntamiento de San Sebastián) en relación con las infracciones de la Ley de Protección de Datos que pudieran cometer los cargos y empleados públicos de la misma, y si tal responsabilidad puede o no ser atribuida a la Administración, con independencia de la identificación del cargo o empleado que materialmente haya cometido la infracción.

Reproduce el siguiente párrafo "Lo anterior no significa, claro es, que estemos proyectando sobre el Ayuntamiento recurrente un principio de responsabilidad objetiva, ni que se vulnere el principio de presunción de inocencia, ni que demos por buena una suerte de inversión de la carga de la prueba.

Sencillamente sucede que, estando admitida en nuestro Derecho Administrativo la responsabilidad directa de las personas jurídicas, a las que se reconoce, por tanto, capacidad infractora, el elemento subjetivo de la infracción se plasma en estos casos de manera distinta a como sucede respecto de las personas físicas, de manera que, como señala la doctrina constitucional que antes hemos reseñado -SsTC STC 246/1991, de 19 de diciembre (F.J. 2) y 129/2003, de 30 de junio (F.J. 8)- la reprochabilidad directa deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma".

Y a la vista de lo afirmado en él alcanza la conclusión de que el art. 9.1 de la LOPD contiene una obligación de resultado y no de medios, tal y como resulta de la propia redacción literal del precepto "el responsable del fichero, y, en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal [...]". De modo que, a su juicio, no basta con hacer los mejores esfuerzos, sino que cuando se produce una brecha, como aquí ha ocurrió, se produce un resultado lesivo para los afectados siempre y en todo caso.

La empresa recurrente realiza una actividad empresarial sobre datos personales y asume el riesgo de que dichos datos puedan ser tratados de manera contraria a la ley y ha de soportar las consecuencias. No basta con establecer unas medidas o que corresponda a la AEPD probar cual fue el fallo que permitió la brecha. La recurrente dice que la brecha se dio pero que no es su responsabilidad, sino de una empleada suya. Frente a ello, cabe oponer que la esencia de la actuación de una persona jurídica es que lo que hace a través de personas físicas, por lo que la actuación de estas se trasmite a aquella directamente, no solo en el ámbito de protección de datos sino en todos los ámbitos del derecho administrativo sancionador.

El actual Reglamento de la UE 2016/679 de Protección de datos (considerando 74) dispone que "debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizada por él mismo o por su cuenta" y en el 78 en la redacción de los arts. 24 o 28.1 del Reglamento de la Unión.

En definitiva, la infracción es de resultado, pero sin negar que haya de existir culpa que en el caso de autos provienen de la falta de supervisión de la empleada imputable directamente a la empresa recurrente.

QUINTO. Quedaron las actuaciones pendientes de señalamiento para votación y fallo, fijándose al efecto el día 11 de enero de 2022, continuando la deliberación en varias sesiones del mes de enero y febrero, habiéndose observado las formalidades legales referentes al procedimiento.

FUNDAMENTOS DE DERECHO

PRIMERO. El presente recurso de casación impugna la sentencia de la Sección Primera de la Sala de lo Contencioso-administrativo de la Audiencia Nacional, de fecha 22 de julio de 2020, por la que se desestima el recurso contencioso- administrativo (n.º 136/2019) interpuesto por la mercantil Commcenter, S.A. contra la resolución de la Directora General de la Agencia Española de Protección de Datos (AEPD) de 27 de noviembre de 2018, que desestima el recurso de reposición interpuesto contra la anterior resolución de 3 de octubre de 2018, que impone a dicha entidad una sanción de 40.001 € por la infracción del artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tipificada como grave en el artículo 44.3.h) de la misma.

La resolución sancionadora consideró acreditado que:

- Commcenter es distribuidor oficial y exclusivo de Movistar, entidad con la que tiene suscritos los correspondientes contratos para dichos servicios

- Los clientes que adquieren productos en la tienda tiene la opción de financiar su compra, financiación que se realiza a través de Telefónica Consumer Finance, entidad con la que Commcenter ha suscrito los correspondientes contratos de prestación de servicios. Para la realización del contrato de financiación Commcenter dispone de una aplicación web, facilitada por Telefónica Finance, a través de la cual gestiona las solicitudes. El acceso a dicha aplicación requiere la introducción de un código de usuario y una contraseña que es único para tienda.

- El formulario exige rellenar diversos datos: del producto, económicos y personales del solicitante de financiación. Entre ellos se incluye la dirección de correo electrónico, obligatoria para poder continuar con la operación, ya que es a dicho correo al que se envía la copia del contrato de financiación y las condiciones generales.

- El denunciante (un particular con la dirección de correo electrónico " DIRECCION000") recibió 14 contratos de financiación de productos con Telefónica Consumer en los que figuran datos de los solicitantes de financiación (nombres, domicilios, teléfonos, estado civil, familiares a cargo, ingresos, situación laboral, cargos, números de cuentas corrientes, importes financiados, mensualidades y la firma del contratante).

- La empresa Commcenter alegó que toda apunta a que lo acontecido es que a la hora de rellenar en el formulario de solicitud de financiación de algunos clientes, una de las trabajadores al rellenar el formulario incluyó la dirección de correo electrónico " DIRECCION000", cuenta que la trabajadora creyó inexistente, al referirse a la provincia donde se encuentra sita la tienda con la única intención de no ver bloqueado con el procedimiento de financiación.

La resolución administrativa imputa a la Commcenter la vulneración del principio de seguridad de los datos personales, establecido en el art. 9.1 de la LOPD. Argumenta que Commcenter estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas que impidan el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros y la entidad incumplió esta obligación como lo demuestra que las solicitudes de financiación fueran remitidos a la dirección del correo del denunciante, afirmando que en esta materia se impone una obligación de resultado.

Por ello, la resolución impugnada considera que se ha cometido la infracción grave prevista en el art. 44.3 h) de la LOPD por la vulneración del principio de seguridad de los datos, recogido en el artículo 9 de la LOPD.

SEGUNDO. Sobre la delimitación de la cuestión controvertida.

La sentencia impugnada, interpretando el art. 9.1 de la LOPD, considera que dicho precepto impone una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, de forma que toda entidad responsable de un fichero (o encargado de tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios, o cualesquiera otros datos de carácter personal, puedan llegar a manos de terceras personas. Bajo esta premisa, la sentencia declara (f.j quinto) "La aplicación de la anterior doctrina al supuesto de autos implica que la infracción del deber de seguridad deba ser apreciada por la Sala, pues ha resultado acreditado y no desvirtuado mediante prueba alguna en contrario que Commcenter, al contratar los servicios y/o productos de telefonía, incumplió su obligación de comprobar de forma fehaciente, tal y como resulta obligado a tenor de la normativa de protección de datos expuesta, la veracidad de la documentación aportada por los clientes.

De modo negligente, en las solicitudes de financiación figuraba una dirección de correo electrónico que no correspondía a los clientes-solicitantes (a pesar de ser un dato que necesariamente debía figuran en tales solicitudes), solicitudes en todas las cuales se estableció como dirección de correo electrónico la de DIRECCION000, que correspondía al denunciante. La consecuencia de ello fue que se permitió el acceso no autorizado por parte de terceros, al menos a 14 solicitudes de financiación, en las que obraban datos personales de los clientes (nombre y apellidos, datos económicos, de domiciliación bancaria y firma) con claro incumplimiento del deber de seguridad regulado en el artículo 9. 1 LOPD en relación con lo previsto en el artículo 93 de dicha LOPD en relación con el artículo 5.2.b) del Reglamento de desarrollo de la LOPD".

Por el contrario, la empresa recurrente en casación entiende que la adopción de las medidas de seguridad es una obligación de medios y no de resultado, sin que sea posible apreciar una responsabilidad objetiva o sin culpa y que los empleados de la empresa no pueden incurrir en una vulneración del artículo 9.1 LOPD que se haga extensible a la empresa.

El Auto de admisión considera que la cuestión que reviste interés casacional consiste en determinar si las infracciones de la Ley de Protección de Datos por fallos de las medidas de seguridad que puedan cometer los empleados de una persona jurídica deben examinarse en atención al resultado y, por lo tanto, imputarse a la persona jurídica de la que dependa el empleado, con independencia de los medios y medidas de prevención que hubiera podido adoptar.

La respuesta a esta cuestión exige algunas consideraciones generales sobre el tipo de obligación que implica la adopción de las medidas de seguridad en materia de protección de datos, la responsabilidad de las personas jurídicas en relación con las medidas de seguridad y por los incumplimientos imputables a sus empleados, para finalmente analizar el incumplimiento que se imputa a la empresa y el tipo infractor que se le aplica.

TERCERO. Sobre las medidas de seguridad en materia de protección de datos y las personas jurídicas.

La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.

En las obligaciones de resultado existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad.

En las obligaciones de medio s el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".

La diferencia radica en la responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

En estas últimas, la suficiencia de las medidas de seguridad que el responsable ha de establecer ha de ponerse en relación con el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados, pero no se garantiza un resultado. Como establece el art. 17.1 de la Directiva 95/46/CE respecto a la seguridad del tratamiento el responsable del tratamiento tiene la obligación de aplicar las medidas técnicas y organizativas adecuadas "Dichas

medias deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de aplicación, un nivel de seguridad apropiados en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse". Y en el mismo sentido se pronuncia en la actualidad el art. 31 del Reglamento de la Unión Europea 2016/679, del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, al establecer respecto a la seguridad del tratamiento que las medidas técnicas y organizativas apropiadas lo son "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas [...]".

Y así debe interpretarse el artículo 9 de la LOPD cuando establece que "1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberá 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".

No basta con diseñar los medios técnicos y organizativos necesarios también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de la diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso.

Esta distinción también tiene su reflejo tanto en el Reglamento de la Unión Europea 2016/679, del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, como en la LOPD 3/2018 de 5 de diciembre, (aun cuando son normas posteriores a los hechos enjuiciados y que, por lo tanto, no resultan de aplicación), al diferenciar como obligaciones e infracciones autónomas entre la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento (art. 73 apartados d, e y f) y la falta de la debida diligencia en la utilización de las medidas técnicas y organizativas implantadas (art. 73. g).

Por último, resulta oportuno recordar que las personas jurídicas responden por la actuación de sus empleados o trabajadores. No se establece por ello una responsabilidad objetiva, pero si es trasladable a la persona jurídica la falta de diligencia de sus empleados, en tal sentido STC 246/1991, de 19 de diciembre f.j 2.

Este Tribunal Supremo en su STS n.º 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) ha tenido ocasión de abordar la responsabilidad de una Administración por incumplimiento del deber de seguridad de los datos personales por actos propios de empleados. En ella se compartía el parecer de la Sala de instancia cuando afirmaba que "[...] la responsabilidad de la Administración titular y encargada del fichero [Ayuntamiento de San Sebastián] no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados o cargos, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las mencionadas obligaciones de protección del carácter reservado de los datos personales la que fundamenta la responsabilidad de la primera en el ámbito sancionador de cuya aplicación se trata; por actos "propios" de sus empleados o cargos, no de terceros[...]". Añadiéndose más adelante que "Lo anterior no significa, claro es, que estemos proyectando sobre el Ayuntamiento recurrente un principio de responsabilidad objetiva, ni que se vulnere el principio de presunción de inocencia, ni que demos por buena una suerte de inversión de la carga de la prueba. Sencillamente sucede que, estando admitida en nuestro Derecho Administrativo la responsabilidad directa de las personas jurídicas, a las que se reconoce, por tanto, capacidad infractora, el elemento subjetivo de la infracción se plasma en estos casos de manera distinta a como

sucede respecto de las personas físicas, de manera que, como señala la doctrina constitucional que antes hemos reseñado -SsTC STC 246/1991, de 19 de diciembre (F.J. 2) y 129/2003, de 30 de junio (F.J. 8)- la reprochabilidad directa deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma".

CUARTO. Sobre la infracción en el caso enjuiciado.

Corresponde ahora analizar el supuesto que nos ocupa.

Es un hecho no controvertido que fallaron las medidas de seguridad y los contratos de financiación de 14 particulares que contenían datos personales -nombres, domicilios, teléfonos, estado civil, familiares a cargo, ingresos, situación laboral, cargos, números de cuentas corrientes, importes financiados, mensualidades y la firma del contratante- se enviaron a un tercero ajeno a la relación contractual.

La empresa denunciada apuntó como explicación más probable que una de las trabajadoras de la tienda a la hora de rellenar el formulario de solicitud de financiación de algunos clientes incluyó la dirección de correo electrónico " DIRECCION000", correo que la trabajadora creyó inexistente al referirse a la provincia donde se encuentra sita la tienda, con la única intención de no ver bloqueado el procedimiento de financiación dado que el sistema técnico diseñado no le permitía continuar con el contrato de financiación si no se introducía una dirección de correo electrónico.

La resolución sancionadora considera que la empresa recurrente incumplió las medidas de seguridad en los términos previstos en el art. 9.1 de la LO 15/1999 y le imputa la comisión de la infracción prevista en el art. 44.3.h) consistente en "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen [...]". Le reprocha a la empresa que la aplicación implantada para la recogida de datos personales de los compradores era defectuosa y no cumplía los requisitos técnicos y de seguridad requeridos, al permitir un acceso no autorizado de un tercero. A tal efecto, razona que el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, vigente en el momento en que se produjeron los hechos, establecía en su artículo 81 tres niveles de seguridad vinculados con el tipo de datos que se trataba de proteger. Considera, y no es objeto de controversia, que en atención a los datos tratados le correspondía adoptar las medidas del nivel básico, previstas en los artículos 89 a 94 de dicha norma, entre las que se encuentra que "el responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios" y en este caso "la aplicación implantada para la recogida de datos de carácter personal era defectuosa y no cumplía los requisitos técnicos y de seguridad requeridos" al permitir un acceso no autorizado.

Por su parte, la sentencia de la Audiencia Nacional impugnada considera que "Commcenter, al contratar los servicios y/o productos de telefonía, incumplió su obligación de comprobar de forma fehaciente, [...] la veracidad de la documentación aportada por los clientes".

Ya hemos razonado que la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Pues bien, el programa utilizado para la recogida de los datos de los clientes no contenía ninguna medida de seguridad que permitiese comprobar si la dirección de correo electrónico introducida era real o ficticia y si realmente pertenecía a la persona cuyos datos estaban siendo tratados y prestaba el consentimiento para ello. El estado de la técnica en el momento en el que se produjeron estos hechos permitía establecer medidas destinadas a comprobar la veracidad de la dirección de email, condicionando la continuación del proceso a que el usuario recibiese el contrato en la dirección proporcionada y solo desde ella prestase el consentimiento necesario para su recogida y tratamiento. Medidas que no se adoptaron en este caso.

La propia empresa en el escrito de alegaciones presentado a la propuesta de resolución puso de manifiesto que el programa no disponía de un sistema de verificación del correo electrónico. En efecto, en el 2018 existía un sistema de verificación del correo electrónico conocido como "doble *opt-in* " consistente en un proceso de aceptación de unas normas o condiciones de uso cuyo principal objetivo es el de verificar que los usuarios son quienes dicen ser y no son ni robots creando suscripciones automáticas, ni correos Spam, o terceras personas generando suscripciones fraudulentas utilizando correos electrónicos que no son de su propiedad. Se trata de un proceso de doble verificación que asegura que los usuarios han aceptado la política de tratamiento de datos y/o las condiciones de privacidad antes de recibir cualquier tipo de comunicación y evita que los documentos vayan a una dirección equivocada. En definitiva, se trata de comprobar que la información recogida es correcta y veraz.

La propia empresa recurrente considera este sistema como básico en materia de seguridad de la información añadiendo que "[...] sin duda hubiera evitado que se hubiera producido la fuga objeto de autos".

De modo que, en el momento en que se produjeron estos hechos, existían medidas técnicas referidas al proceso de registro, que hubiesen evitado la filtración de datos personales producida. Ello implica que las medidas técnicas adoptadas incumplían las condiciones de seguridad en los términos exigidos en el art. 9.1 de la LO 15/1999, incurriéndose por tanto en la infracción prevista en el art. 44.3.h) consistente en "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen [...]".

Se afirma que las medidas técnicas de seguridad referidas al programa informático incumbían a Telefónica Consumer Finance que diseño el programa y era la responsable del fichero y del tratamiento, y que la empresa sancionaba tan solo actuaba por cuenta de ésta recabando los datos de los clientes que optaban por la financiación. Lo cierto es que el encargado del tratamiento -la persona física o jurídica que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento art. 4 apartado 8 del Reglamento como el art. 3.g) de la LOPD 15/1999, y la recogida de datos implica un tratamiento (art. 3.c)- también deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, así lo dispone el art. 32.1 del Reglamento (UE) 2016/679 del Parlamento y del Consejo y el art. 9.1 de la LOPD y está sujeto al régimen sancionador establecido en la Ley (art. 43 de la LOPD 15/1999).

La empresa recurrente trataba los datos de los clientes por cuenta del responsable del fichero por lo que implantó y utilizó dicho programa siendo conocedora, o hubiera debido serlo, de que éste carecía de las medidas de seguridad necesarias para comprobar la veracidad y exactitud de la dirección de email a la que se enviaba la copia del contrato de financiación. Pero lo que es más importante, el programa de tratamiento de datos diseñado tampoco se utilizó de forma adecuada, lo cual hubiese evitado la filtración. La empresa encargada de recopilar los datos que se incluían en el fichero estaba obligada a controlar que no se burlaban las medidas de seguridad existentes para registrar los datos de los usuarios. Sin embargo, una empleada hizo un mal uso reiterado del programa, introduciendo datos inexactos de forma voluntaria, puesto que rellenó una dirección de email inventada para poder

continuar con el proceso de registro aun a sabiendas que el contrato se enviaría a dicha dirección. El hecho de que fuese la actuación negligente de una empleada no le exime de su responsabilidad en cuanto encargado de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de registro de datos diseñado. Como ya sostuvimos en la STS n.º 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros.

Se alega por la recurrente la ausencia de evento dañoso puesto que los afectados prestaron su anuencia a los datos incorporados a la ficha, de forma expresa y por escrito. El hecho de que los interesados firmasen el formulario no exonera la responsabilidad de la empresa obligada a comprobar a la veracidad de la dirección de correo electrónico utilizada sin perjuicio de que esta circunstancia pueda ser tomada en consideración para graduar la sanción.

QUINTO. Sobre la graduación de la sanción.

El recurso plantea también la modulación de la responsabilidad por disminución cualificada de la culpa en aplicación de los criterios de graduación previstos en los artículos 45.4 h), i, y j) de la LOPD, así como la aplicación de los criterios de disminución de responsabilidad previstos en los artículos 45.5. a), b) y c) de la LOPD.

Conviene empezar por señalar que la resolución sancionadora apreció diferentes criterios agravantes: el carácter continuado de la infracción, el volumen de los tratamientos afectados, la vinculación de la actividad del infractor con la realización de tratamiento de datos de carácter personal y el volumen de negocio o actividad del infractor.

La aplicación al caso que nos ocupa de estas circunstancias no ha sido rebatida de forma concreta en casación, salvo la circunstancia referida al volumen de datos filtrados por entender que al tratarse de tan solo 14 contratos de financiación nos encontramos ante un número muy reducido de datos que debe aminorar la sanción. Lo cierto es que la filtración de 14 contratos de financiación con numerosos datos personales sensibles como las cuentas corrientes, lugar de trabajo y datos personales y familiares no puede considerarse una filtración que ni por su importancia ni por el volumen merezca ser atenuada.

Por otra parte, aduce que pueden existir otros criterios atenuantes tales como: la naturaleza de los perjuicios causados a las personas interesadas o a terceras personas (art. 45.4. h); la acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor (art.45.4 i); o cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora (previsto en el art. 45.4 j).

De nuevo se aprecia la falta de toda argumentación que explique las concretas razones que justificarían la aplicación de los criterios de atenuación invocados. Por otra parte, ya hemos descartado que los procedimientos de seguridad que tenía implantados fuesen adecuados para la recogida y tratamiento seguro de los datos de carácter personal, y debe rechazarse también que la filtración de datos fuese debida a una anomalía en el funcionamiento de los procedimientos.

Es cierto que los clientes afectados firmaron el formulario con la dirección de correo electrónico falsa, circunstancia que puede ser tomada en consideración para graduar la sanción, pero que ni excluye la

responsabilidad de la empresa ni puede encuadrase como una disminución sensible de su antijuricidad, a la que le sea aplicable el art. 45. 5 de la LOPD 15/1999, entonces vigente ("c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción") pues no puede considerarse que el cliente indujese a la comisión de la infracción, máxime cuando ese comportamiento y la dirección se ha reiterado en otros muchos clientes.

Esta circunstancia, pese a la existencia de otras agravantes, ha contribuido sin duda a que se aplicase la sanción mínima prevista en el art. 45 de la LOPD (40.001 €), que permitía castigar las infracciones graves con multa de 40.001 a 300.000 euros,

SEXTO. Costas.

De conformidad con lo dispuesto en el art 93.4 LJ cada parte abonará las costas causadas a su instancia y las comunes por mitad sin que se aprecien razones de temeridad o mala fe en el presente litigio que justifiquen la imposición de las costas a ninguna de las partes intervinientes.

Por lo que respecta a las costas de instancia no procede su imposición a ninguna de las partes litigantes. Y ello porque, aunque se confirma finalmente la sanción impuesta y el resultado del proceso en instancia, la cuestión controvertida planteaba serias dudas de derecho sobre la naturaleza de las obligaciones de seguridad en materia de protección de datos, de hecho se acoge la argumentación de la parte referida a que nos encontramos ante una obligación de medios y no de resultado aunque ello no se traduzca en la anulación de la sanción impuesta.

F A L L O

Por todo lo expuesto, en nombre del Rey y por la autoridad que le confiere la Constitución, esta Sala ha decidido de acuerdo con la interpretación de las normas establecida en el fundamento jurídico tercero:

1.º Desestimar el recurso de casación interpuesto por la entidad "Commcenter, S.A" contra la sentencia de la Sección Primera de la Sala de lo Contencioso-administrativo de la Audiencia Nacional de 22 de julio de 2020 (rec. 136/2019), confirmando la sanción impuesta.

2.º No hacer expresa condena en costas ni en instancia ni en casación.

Notifíquese esta resolución a las partes e insértese en la colección legislativa.

Así se acuerda y firma.