Identificación del expediente

Resolución de procedimiento sancionador núm. PS 43/2022, referente a Badalona Serveis Asistencials, SA

Antecedentes

1. En fecha 04/01/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra Badalona Serveis Asistencials, SA (en adelante, BSA), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, la persona denunciante se quejaba sobre presuntos accesos indebidos en su historia clínica, llevados a cabo desde el Hospital Municipal de Badalona -gestionado por BSA- por personal de enfermería. Los referidos accesos se habrían realizado los días y horas que se señalan a continuación: 13 de abril de 2020, a las 03.09h; 16 de abril de 2020 a las 22.42h; y, 17 de abril de 2020 a las 23.39h.

La persona denunciante acompañaba su denuncia del escrito que en fecha 13/11/2021 dirigió a BSA, comunicando que se habrían realizado accesos indebidos a su historia clínica, y del escrito de respuesta del entidad denunciada de fecha 24/12/2021, confirmando que los tres accesos " *se han reputado como indebidos o no directamente vinculados con una tarea asistencial o epidemiológica".*

2. La Autoridad abrió una fase de información previa (núm. IP 3/2021), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 20/02/2021 se requirió a la entidad denunciada para que diera respuesta a diversas cuestiones relativas a los hechos denunciados, entre otros, la justificación de los accesos objeto de denuncia.

4. En fecha 26/02/2021, BSA respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- Que los tres accesos habían sido realizados por una misma persona con perfil de personal de enfermería.

- Que no se ha podido constatar que los accesos controvertidos *"sean justificados por la realización de un acto asistencial o de diagnóstico. Por tanto, BSA cataloga a los mismos como indebidos o no justificados en una tarea asistencial o de diagnóstico de la profesional quien los realizó. (...) También, se ha constatado que esta falta de justificación, a raíz de las entrevistas mantenidas desde el departamento de recursos humanos de la entidad con la profesional implicada los cuales acreditaron que la trabajadora no obró con motivo de la su labor profesional".*

- Que se está instruyendo *"el procedimiento sancionador laboral aplicable a la trabajadora autora de los accesos no justificados. (...)"*

El escrito de la entidad denunciada también ponía de manifiesto que, a raíz de los hechos denunciados, se estaban llevando a cabo una serie de medidas correctivas a efectos de evitar que vuelvan a producirse este tipo de conductas entre su personal. En concreto, destaca la preparación de acciones formativas, especialmente dirigidas a los profesionales con acceso a la historia clínica, así como informativas, sobre los buenos usos de la historia clínica y de las consecuencias laborales, administrativas y penales asociadas al mal uso de ésta información.

Por último, la entidad también informaba de las medidas de seguridad implementadas para garantizar los derechos de las personas usuarias de sus servicios. A título de ejemplo, la entidad afirmaba disponer de un registro de accesos a historia clínica, de sistemas de auditorías periódicas tendentes a la revisión de estos accesos, entre otros.

5. En fecha 28/06/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra BSA por una presunta infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1 f); todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 11/07/2022.

6. En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

7. En fecha 25/07/2022, BSA formuló alegaciones al acuerdo de iniciación, aportando con su escrito diversa documentación.

8. En fecha 10/11/2022, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos impusiera a BSA la sanción consistente en una multa de 2.000.- euros (dos mil euros), como responsable de la infracción prevista en el artículo 83.5 a) en relación con el artículo 5.1 f), todos ellos del RGPD.

Esta propuesta de resolución se notificó en fecha 11/11/2022 y se concedía un plazo de 10 días para formular alegaciones.

9. En fecha 21/11/2022, la entidad imputada presentó un escrito a la Autoridad mediante el cual reconoce su responsabilidad sobre los hechos imputados y adjunta el comprobante del pago voluntario adelantado de la sanción pecuniaria que la persona instructora proponía . En concreto, la entidad imputada satisfizo, en fecha 21/11/2022, 1.200,00 euros (mil doscientos euros), correspondientes a la sanción pecuniaria, una vez aplicadas las reducciones previstas en el artículo 85 de la ley 39/2015.

Hechos probados

Los días 13, 16 y 17 de abril de 2020, con el detalle indicado en el antecedente 1º, una persona con perfil de enfermería que prestaba servicios en el Hospital Municipal de Badalona – gestionado por Badalona Serveis Assistencials, SA – va acceder a la historia clínica de la persona aquí denunciando, sin su consentimiento, y sin que estos accesos estuvieran relacionados con ninguna actuación asistencial o de diagnóstico.

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC , y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

El tratamiento de datos denunciado recae dentro del ámbito competencial de la Autoridad en virtud del artículo 3.f) de la Ley 32/2010, en la medida en que el Hospital Municipal de Badalona, gestionado por BSA, forma parte del sistema integral de utilización pública de Cataluña – SISCAT – (Decreto 196/2010, de 14 de diciembre, del sistema sanitario integral de utilización pública de Cataluña), y en este sentido, presta servicios de salud pública concertados con el Servicio Catalán de la Salud.

2. De conformidad con el artículo 85.3 de la LPAC, tanto el reconocimiento de responsabilidad como el pago voluntario adelantado de la sanción pecuniaria propuesta comportan la aplicación de unas reducciones. La efectividad de estas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por vía administrativa contra la sanción. Para ambos casos, los apartados 1 y 2 del artículo 85 de la LPAC contemplan la terminación del procedimiento.

Aunque presentó alegaciones en el acuerdo de iniciación, la entidad imputada no ha formulado alegaciones a la propuesta de resolución, ya que se ha acogido a ambas opciones para reducir el importe de la sanción. Sin embargo, se considera oportuno reiterar a continuación lo más relevante de la respuesta motivada que la persona instructora dio a las alegaciones ante el acuerdo de iniciación.

2.1 Sobre el sujeto responsable de la infracción

La entidad imputada cuestionaba que se le atribuya la responsabilidad por la comisión de una infracción por unos hechos que materialmente habría llevado a cabo una de sus empleadas -que en el marco de la investigación interna habría reconocido haber accedido indebidamente a la historia clínica de la persona denunciante– e invocaba en este sentido la sentencia núm. 188/2022 de la Sala Tercera del Tribunal Supremo que, en términos literales, dispone:

> 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 la filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desarrollada por el responsable del fichero o del tratamiento".*

En relación con lo anterior, BSA aducía que, a diferencia de las obligaciones de resultado, en las obligaciones de medios, " *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 permita conseguir el resultado esperado con medios que de forma razonable, puedan calificarse de idóneos y suficientes para su consecución, por lo que se denominan "obligaciones de diligencia o comportamiento", las cuales han sido cumplidas por el responsable del tratamiento en este caso".*

Adjunto al escrito de alegaciones, la entidad imputada aportaba un comunicado firmado por el Director de personas, en fecha 05/03/2021, mediante el cual se informaba a la trabajadora que efectuó los accesos indebidos denunciados, de la imposición de una sanción de dos días de suspensión de empleo y sueldo, por la comisión de una falta menos grave.

Pues bien, tal y como recuerda la Sala Tercera del Tribunal Supremo, en la sentencia 188/2022, las personas jurídicas responden por la actuación de sus trabajadores de tal modo que, no se establece una responsabilidad objetiva, pero sí se traslada a la persona jurídica la carencia de diligencia de sus empleados (por todas, STC 246/1991, de 19 de diciembre fj2).

En relación con lo anterior, de las alegaciones de BSA se desprende que, la comisión de la infracción sería materialmente atribuible a una trabajadora que presta servicios a la suya organización. Sin embargo, de conformidad con el RGPD y, especialmente, con el artículo 70 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), la responsabilidad por las infracciones en materia de protección de datos recae sobre los responsables o encargados de los tratamientos, y no sobre sus empleados. En términos literales, la STS 188/2022 dispone:

> *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 fj 2. Este Tribunal Supremo en su STS nº 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 las 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 archivo [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 las 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 estamos 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 modo distinto a como sucede respecto de las personas físicas de modo que, como señala la doctrina constitucional que antes hemos reseñado - la reprochabilidad directa deriva - SsTC 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 está sujeta al cumplimiento de dicha norma".

De acuerdo con lo expuesto, está claro que el hecho de que una profesional de enfermería actuara de manera negligente, accediendo en tres ocasiones a la historia clínica del ahora denunciante, no exime a BSA de su responsabilidad como responsable del tratamiento datos de pacientes y usuarios del Hospital Municipal de Badalona.

2.2 Sobre la diligencia del responsable del tratamiento

La entidad imputada ponía de manifiesto haber actuado con diligencia, en relación con el tratamiento de datos personales, y haber llevado a cabo, periódicamente, auditorías para evaluar el grado de cumplimiento de la normativa de protección de datos.

Respecto a los hechos imputados, BSA explicaba que convocó las reuniones pertinentes y dirigió investigaciones internas a efectos de depurar responsabilidades y sancionar a la empleada que accedió indebidamente a la historia clínica del ahora denunciante.

En relación con lo anterior, BSA añadía que siempre se informa al personal que se incorpora a la empresa, de sus obligaciones en materia de privacidad, confidencialidad y protección de datos. Y, en relación con lo anterior, sostenía que, a raíz del incidente, se han realizado formaciones específicas y se han celebrado jornadas para concienciar de la importancia de la protección de datos en el ámbito sanitario.

Pues bien, esta Autoridad valora muy positivamente las actuaciones llevadas a cabo por la entidad imputada, a efectos de velar por el cumplimiento de la legislación de protección de datos. Sin embargo, sin perjuicio de lo establecido en el fundamento jurídico cuarto de esta resolución, estas circunstancias no pueden eximir a BSA de su responsabilidad por la vulneración de la normativa de protección de datos que aquí se sanciona.

2.3 Sobre el régimen sancionador aplicable

Seguidamente, la entidad imputada aducía que, a pesar de tener la forma jurídica de sociedad mercantil anónima, es una organización pública formada por capital íntegramente público, que se integra en el presupuesto del Ayuntamiento de Badalona y que está presidida por el propio Alcalde de Badalona. Asimismo, la entidad imputada argumentaba:

"Por las particularidades sobre su composición que hemos resaltado, BSA debería acomodarse dentro del régimen aplicable a las entidades recogidas en el artículo 77.1. En concreto, las del apartado d), siendo BSA una organización claramente dependiente de una administración pública como es el Ayuntamiento de Badalona. La imposición de una sanción económica a BSA supondría una sanción económica a los propios administrados, lo que implicaría un doble perjuicio: aquel originado de la propia infracción y ese derivado de hacer frente a la sanción económica. Parece ser la voluntad del legislador proteger al ciudadano de esa doble sanción que establece un régimen sancionador específico para el sector público"

Sobre esta alegación, en primer lugar, cabe aclarar que el artículo 70 del LOPDDDD determina cuáles son las entidades que quedan sujetas al régimen sancionador establecido en el RGPD y en el LOPDDDD, régimen que, por lo que aquí interesa, será de aplicación en BSA como responsable del tratamiento de los datos personales que ha dado lugar a la incoación de este procedimiento.
Dicho esto, BSA defiende que le es de aplicación el régimen especial del artículo 77.1 d) del LOPDDDD, que prevé no imponer sanciones económicas a determinados responsables o encargados del tratamiento que hayan vulnerado la normativa y, en concreto a los " *organismos públicos y las entidades de derecho público vinculadas o dependientes de las administraciones públicas".*

Al respecto, cabe señalar que, la relación de entidades prevista en el artículo 77.1 LOPDGDD se basa esencialmente en la forma/naturaleza jurídica que adopta el sujeto activo de la infracción, de tal modo que, si el legislador hubiera querido que las entidades dependientes o vinculadas a una administración pública, cualquiera que fuera su forma jurídica, estuvieran sujetas al régimen previsto en el artículo 77.1 de la LOPDDDD, las habría incluido expresamente en esta lista cerrada.

Por lo expuesto, dado que las sociedades anónimas, sea cual sea el origen de su capital social o la composición de su consejo social, no están incluidas en la lista prevista en el artículo 77.1 de la LOPDDDD, cabe concluir que los resulta de aplicación el régimen sancionador general previsto en el artículo 83 RGPD.

3. En relación con los hechos descritos en el apartado de hechos probados, relativos a los accesos indebidos por parte de una profesional de enfermería, se debe acudir al artículo 5.1. f) del RGPD, que regula el principio de integridad y de confidencialidad, determinando que los datos serán " *tratados de tal modo que se garantice una seguridad adecuada de las datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ".*

Por otra parte, el artículo 5 de la LOPDDDD, en relación con el deber de confidencialidad, establece:

"1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase del mismo están sujetos al deber de confidencialidad a que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable (...)".

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, que es constitutivo de la infracción prevista en el artículo 83.5.a) el RGPD, que tipifica la vulneración de " *los principios básicos para el tratamiento ",* entre los que se da lugar el principio de confidencialidad.

La conducta que aquí se aborda se ha recogido como infracción muy grave en el artículo 72.i) de la LOPDDDD, en la siguiente forma:

> *"La vulneración el principio de confidencialidad que establece el artículo 5 de esta Ley orgánica"*

4. Al no encajarse BSA en ninguno de los sujetos previstos en el artículo 77.1 del LOPDDDD , resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD.

El artículo 83.5 del RGPD prevé para las infracciones allí previstas, se sancionen con una multa administrativa de 20.000.000 de euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Dicho esto, corresponde determinar la cuantía de la multa administrativa que procede imponer.

Según lo que establece el artículo 83.2 del RGPD, y también de conformidad con el principio de proporcionalidad consagrado al artículo 29 de la Ley 40/2015, tal y como indicaba la persona instructora en la propuesta de resolución, procede imponer la sanción de dos mil euros (2.000 mil euros). Esta cuantificación de la multa se basa en la ponderación entre los criterios agravantes y atenuantes que a continuación se indican.

Como criterios atenuantes, se observa la concurrencia de las siguientes causas:

- El limitado número de accesos en el tiempo y que afectan a una sola persona (art. 83.2 en RGPD y 76.2 en LOPDGDD)
- El grado de responsabilidad del responsable o del encargado del tratamiento, teniendo en cuenta las medidas técnicas u organizativas que hayan aplicado en virtud de lo dispuesto en los artículos 25 y 32 del RGPD (art. 83.2.c RGPD).
- La falta de beneficios obtenidos como consecuencia de la comisión de la infracción (art. 83.2.k RGPD y art. 76.2.c LOPDGDD).
- El inmediato inicio de una investigación por parte de la entidad a efectos de depurar eventuales responsabilidades entre su personal (art. 83.2.k RGPD).

Por el contrario, como criterios agravantes, es necesario tener en cuenta los siguientes elementos:

- Naturaleza de la infracción (art 83.2 en RGPD). En la medida en que se imputa la vulneración del deber de confidencialidad, calificada como infracción muy grave de la normativa de protección de datos.
- La categoría de datos de carácter personal afectados por la infracción (art. 83.2 g RGPD).
- La vinculación de la actividad de BSA con la realización de tratamientos de datos personales (art. 83.2.k RGPD y 76.2 b LOPDGDD). Dado que la entidad imputada gestiona un Hospital municipal, cabe afirmar que existe una estrecha vinculación entre su actividad y el tratamiento de un número considerable de datos personales –no sólo de pacientes o usuarios, sino que también de personal sanitario, y otros profesionales que puedan prestar sus servicios a la entidad-.

5. Por otra parte, de conformidad con el artículo 85.3 de la LPAC y tal y como se adelantaba al acuerdo de iniciación, si antes de la resolución del procedimiento sancionador la entidad imputada reconoce su responsabilidad o hace el pago voluntario de la sanción pecuniaria, procede aplicar una reducción del 20% sobre el importe de la sanción provisionalmente cuantificada. Si concurren los dos casos mencionados, la reducción se aplicará de forma acumulada (40%).

Como se ha avanzado, la efectividad de dichas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por vía administrativa contra la sanción (art. 85.3 de la LPAC, in *fine)* .

Pues bien, tal y como se ha indicado en los antecedentes, mediante escrito de 21/11/2022, la entidad imputada ha reconocido su responsabilidad. Y, en la misma fecha, ha abonado de forma avanzada 1.200 euros (mil doscientos euros), correspondientes a la cuantía de la sanción resultante, una vez aplicada la reducción acumulada del 40%.

6. Ante la constatación de la infracción prevista en el art. 83 del RGPD en relación con ficheros o tratamiento de titularidad privada, el artículo 21.3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, faculta a la directora de la Autoridad para que la resolución que declara la infracción establezca las medidas oportunas para que cese o se corrijan sus efectos.

Sin embargo, en el presente caso resulta innecesario requerir medidas correctoras de los efectos de la infracción dado que la conducta se refiere a un hecho aislado y puntual, con el que se habrían consumado los efectos de la infracción.

Por todo esto, resuelvo:

1. Imponer a Badalona Serveis Assistencials, SA la sanción consistente en una multa de 2.000.- euros (dos mil euros), como responsable de una infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1 f), ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con el fundamento de derecho 6º.

2. Declarar que Badalona Serveis Asistencials ha hecho efectivo el pago adelantado de 1.200 euros (mil doscientos euros), que corresponde al importe total de la sanción impuesta, una vez aplicado el porcentaje de deducción del 40% correspondiente a las reducciones previstas en el artículo 85 de la LPAC.

3. Notificar esta resolución a Badalona Serveis Assistencials SA .

4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat) , de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,