Identificación del expediente

Resolución de procedimiento sancionador núm. PS 34/2022, referente a la Sociedad Catalana para la Movilidad, SA.

Antecedentes

1 . En fechas 05/10/2021,06/10/2021,07/10/2021, y 26/10/2021 tuvieron entrada en la Autoridad Catalana de Protección de Datos, hasta seis denuncias formuladas de forma separada por personas ciudadanas contra la Autoridad del Transporte Metropolitano (en adelante, la ATM), y una denuncia formulada contra la Sociedad Catalana para la Movilidad, SA, (en adelante, SocMobilitat), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, las personas denunciantes se quejaban de que en fecha 05/10/2021 se había detectado una vulnerabilidad de seguridad en el portal T-mobilitat.atm.cat, (https://t-mobilitat.atm.cat) que debería permitido el acceso por parte de terceros a sus datos personales allí registrados, facilitados para darse de alta como usuarios de la nueva tarjeta T-Mobilitat. Asimismo, se quejaban de que la vulnerabilidad detectada permitía la modificación de la información de los usuarios allí contenida. A fin de justificar los hechos denunciados, las personas denunciantes aportaban documentación diversa.

2 . Asimismo la ATM, en cumplimiento de lo que prevé el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstos (en adelante, RGPD), y en su condición de responsable de tratamiento, notificó a esta Autoridad en fecha 06/10/2021, la violación de seguridad de los datos sufridos (NVS 86 /2021), consistente en la vulnerabilidad detectada en el portal T-mobilitat.atm.cat, que comprometió datos personales de los usuarios allí registrados. Las actuaciones llevadas a cabo en el marco de la notificación de dicha violación de seguridad (NVS 86/2021), se incorporaron a la fase de información previa abierta con motivo de las denuncias presentadas ante la Autoridad por los mismos hechos.

3 . En fecha 10/01/2022, la Directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra SocMobilitat -(...)-, a fin de dirimir su presunta responsabilidad en la vulneración del principio de seguridad de los datos en el despliegue del portal web T-Mobilitat, y consiguiente vulneración de su confidencialidad que había sido objeto de denuncia.

Este procedimiento se inició contra SocMobilitat , dado que del resultado de las actuaciones de indagación llevadas a cabo en el marco de la información previa abierta por esta Autoridad, se desprendía que los hechos objeto de imputación recaían en el ámbito de su responsabilidad, en virtud del contrato de encargo del tratamiento de datos personales suscrito entre la ATM (responsable del tratamiento) y SocMobilitat (adjudicataria del contrato y encargado del tratamiento) en fecha 30/09/2021, para la prestación del servicio de implantación y gestión del nuevo sistema tarifario integrado con tecnología sin contacto (tarjeta T-movilidad).

4. De la documentación aportada por SocMobilitat en la tramitación del procedimiento sancionador -(...)-, se constató que los hechos denunciados, es decir, la presunta

vulneración del principio de seguridad de los datos en el despliegue del portal T -Movilidad y consiguiente vulneración de su confidencialidad , debido a la falta de implementación de medidas de seguridad de nivel básico, eran imputables a Indra Sistemas SA en el marco del contrato de encargo del tratamiento de datos personales suscrito entre SocMobilitat (encargada del tratamiento) e Indra Sistemas SA (socia accionista de SocMobilitat y subencargada del tratamiento), para la prestación de servicios en la fase de implantación y gestión de la T-movilidad (entre ellos, el despliegue del portal web) , de acuerdo con el régimen de responsabilidad en materia de protección de datos establecido en el artículo 28.10 del RGPD, que es también aplicable al subencargado del tratamiento de conformidad con los artículos 28.4 del RGPD y 70.1.b) LOPDGDD .

Así, en el contrato de encargo del tratamiento de datos personales suscrito entre SocMobilitat e Indra en fecha 30/09/2021 se estipulaban las medidas de seguridad que Indra debía adoptar para la prestación objeto del encargo:

"7. Obligaciones del encargado del tratamiento (...)
"7.5. Seguridad del Tratamiento
*El encargado del Tratamiento implantará las Medidas apropiadas respecto a la seguridad del Tratamiento , que se correspondan con las de la Administración contratante y que se ajustan al Esquema Nacional de Seguridad (**NIVEL BÁSICO**).*

En todo caso, el Encargado deberá implantar mecanismos para:
a. Garantizar la confidencialidad , integridad , disponibilidad y resiliencia permanentes de los sistemas y servicios de Tratamiento .
b. Restaurar la disponibilidad y el acceso a las Datos personales de forma rápida , en caso de incidente físico o técnico .
c. Verificar, evaluar y valorar de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento .
d. Seudonimizar y cifrar las Datos personales , en su caso.

En conjunto, deberá adoptar todas aquellas otras Medidas que, teniendo en cuenta el conjunto de tratamientos que lleva a cabo, sean necesarias para garantizar un nivel de seguridad adecuado al riesgo .

La documentación relacionada con la gestión de los riesgos , incluyendo el resultado de las auditorías periódicas que se realicen , puede ser solo solicitada en cualquiera momento por el responsable del Tratamiento .(...)."

Tal y como se hizo constar en el acuerdo de incoación del procedimiento sancionador (...) referente a SocMobilitat , las medidas de seguridad que se vulneraron en la configuración del control de acceso al portal de la T-movilidad, que propiciaron que el acceso quedara abierto, ya su vez, accesible a terceros, son de nivel básico (apartado 4.1.2 "Arquitectura de Seguridad", apartado 4.2 relativo al control de acceso, y apartado 4.3.2 relativo a la "configuración de seguridad") del Esquema Nacional de Seguridad (ENS) aprobado por Real Decreto 3/2010, al que se hace referencia.

A la vista de todo lo anterior, y de conformidad con el artículo 20.1.c) del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad de Cataluña, en fecha 27/05/2022 la Directora de la Autoridad Catalana de Protección de Datos resolvió, atendiendo al principio de congruencia

que rige en el procedimiento sancionador, declarar el sobreseimiento del procedimiento (...) iniciado contra SocMobilitat , dado que esta entidad no sería responsable de la falta de aplicación de las medidas de nivel básico que se le exigió adoptar en Indra , como se estipulaba en el contrato de encargo de tratamiento suscrito entre ambas entidades en fecha 30/09/2021.

Sin embargo, de la documentación obrante en el expediente se desprendía, como corrobora el informe de fecha 11/05/2022 del Área de Tecnología y Seguridad de la Información de la Autoridad, que SocMobilitat no habría categorizado o determinado de forma adecuada el nivel de riesgo del sistema de información (categorizado de nivel básico en el punto 7.5 antes transcrito del contrato de encargado del tratamiento) para la prestación de los servicios encomendados a Indra en la fase de implantación y gestión de la tarjeta T-movilidad, por lo que, en dicha resolución, se acordó también iniciar un nuevo procedimiento sancionador contra SocMobilitat , a efectos de dirimir su responsabilidad por presunta vulneración del artículo 32 del RGPD en la determinación de las medidas adecuadas al riesgo que comporta el tratamiento de datos encargado a Indra , e incorporar al expediente, las actuaciones y documentación obrante en el procedimiento sancionador (...).

5. En fecha 01/06/2022, se inició, por Acuerdo de la directora de la Autoridad Catalana de Protección de Datos el presente procedimiento sancionador contra SocMobilitat , por una presunta infracción prevista en el artículo 83.4.a), en relación en el artículo 32.2; todos ellos del RGPD. Este acuerdo de iniciación se notificó a la entidad imputada en fecha 06/06/2022.

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, plazo que fue ampliado en 5 días más a petición de SocMobilitat .

6. En fecha 27/06/2022, SocMobilitat formuló alegaciones al acuerdo de iniciación .

7 . En fecha 09/09/2022, la 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 SocMobilitat una multa de 10.000 euros como responsable , de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.2, en lo que se refiere al principio de seguridad de los datos, ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 13/09/2022 y se concedía un plazo de 10 días para formular alegaciones.

8. En fecha 27/09/2022, la entidad imputada presentó un escrito de alegaciones a la propuesta de resolución.

Hechos probados

En fecha 30/09/2021 la Sociedad Catalana para la Movilidad, SA, formalizó un contrato de encargado del tratamiento con la sociedad Indra Sistemas, SA, para la prestación de servicios en el marco del Proyecto Tecnológico T-mobilitat, de acuerdo con las tareas encomendadas en los contratos de prestación de servicios para la fase de implantación y gestión de fecha 24/07/2014, y sus posteriores modificaciones (cláusula 2ª del contrato de encargo “Condiciones y finalidades del tratamiento ”):

"2. Condiciones y finalidades del tratamiento
2.1 "El tratamiento consistirá en las prestaciones técnicas dentro del Proyecto tecnólogico de la T-Movilidad atribuidas y asumidas por INDRA en los contratos de Prestación de Servicios para la fase de implantación para la T-Movilidad y en el de Prestación de servicios para la fase de gestión para la T-Movilidad suscritos entre SOC MOVILIDAD y INDRA en fecha 21 de julio de 2014 y sus posteriores modificaciones addendas ."

La ejecución de estos servicios, comportaba que Indra accedía y gestionaba los datos personales de los usuarios de la T-movilidad, que incluiría datos de carácter sensible, e incluso categorías especiales de datos, de acuerdo con lo estipulado en la cláusula 3ra del contrato de encargo (" Identificación de la información afectada, objeto de tratamiento ").

En cuanto a las medidas de seguridad que Indra debía implementar o adoptar para la prestación de los servicios objeto de encargo, en el contrato de encargado del tratamiento suscrito entre SocMobilitat e Indra se exigían las siguientes medidas de seguridad:

"7. Obligaciones del encargado del tratamiento (...)
"7.5. Seguridad del Tratamiento
El encargado del Tratamiento implantará las Medidas apropiadas respecto a la seguridad del Tratamiento , que se correspondan con las de la Administración contratante y que se ajustan al Esquema Nacional de Seguridad (***NIVEL BÁSICO*** *) (...)."*

Así pues, SocMobilitat categorizó el sistema como básico. Ahora bien el análisis de dicho contrato de encargo, así como de los contratos de prestación de servicios para la fase de implantación y gestión de la T-movilidad, y el hecho de que el proyecto T-Mobilitat implica el tratamiento de un elevado volumen de datos personales de las personas usuarias del transporte, que incluiría categorías especiales de datos, y que el propio sistema debe proporcionar servicios críticos (interrelación con usuarios a través del portal web, funcionamiento del billete y procesamiento de los datos mediante el CPD, etc.) para la prestación de un servicio especialmente relevante como es un servicio de movilidad por toda la red de transporte público, lleva a concluir que la categorización por parte de SocMobilitat del sistema de información requeriría una categorización de nivel superior , de conformidad con las determinaciones del Esquema Nacional de Seguridad (ENS), y por tanto, que no se ha determinado de forma adecuada las medidas de seguridad que Indra debía aplicar en la ejecución del contrato.

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.

2. La entidad imputada ha formulado alegaciones tanto en el acuerdo de iniciación como en la propuesta de resolución, en esta resolución se analizan el conjunto de estas alegaciones.

2.1 Sobre la carencia de competencia de la Autoridad en la categorización del sistema de información y en la determinación de las medidas de seguridad aplicables.

En sus alegaciones a la propuesta de resolución, SocMobilitat aduce que la categorización de un sistema de información en materia de seguridad, y la consiguiente determinación de las medidas de seguridad a adoptar, es una competencia que, de acuerdo con lo que disponen los artículos 28 y 41 del Real Decreto 311/2022 por el que se regula el ENS (así como los artículos 27 y 44 del anterior ENS- Real Decreto 3/2010), corresponde en "exclusiva" al responsable del tratamiento" (responsable de seguridad), que es quien dispone de la información necesaria para llevar a cabo dicha categorización, en base a la importancia de la información que se trata en el sistema, los servicios que se prestan y el esfuerzo de seguridad requerido en función de los riesgos a que está expuesto (artículo 44 del ENS), sin que la Autoridad tenga competencia alguna para hacerlo, ni disponga tampoco de los elementos necesarios para llevar a cabo dicha valoración, corriendo el riesgo , sí así se hace, " *de operar con presunciones y con juicios de inferencia contrarios todos ellos a los principios de legalidad y tipicidad."*

Al respecto, cabe decir que, efectivamente, es el responsable o el encargado del tratamiento, al que corresponde, o mejor dicho, quien tiene el deber legal de categorizar o evaluar de forma adecuada el nivel de riesgo que presenta un sistema de información y, en base a esta evaluación, determinar las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de datos que se quiere llevar a cabo, en cumplimiento de la obligación establecida en el artículo 32 de el RGPD.

Dicho esto, cabe remarcar que corresponde a la Autoridad Catalana de Protección de Datos, que es el organismo que tiene legalmente atribuida la competencia de supervisar la aplicación del RGPD y hacerlo cumplir, determinar si se ha producido un incumplimiento de la normativa de protección de datos, y en el supuesto que nos desempeña, en el ejercicio de las funciones que tiene encomendadas, y mediante la instrucción del correspondiente expediente sancionador donde han quedado plenamente justificados los motivos de su incoación (apartado de hechos probados) y que fundamentan la presente resolución, ha concluido que SocMobilitat ha incumplido la obligación del artículo 32 del RGPD, debido a que en el contrato de encargo de tratamiento suscrito con Indra en fecha 30/09/2021 , para la prestación de servicios en la fase de implantación y de gestión de la T-movilidad, SocMobilitat indicó a Indra que la categorización del sistema era de nivel básico (cláusula 7.5), lo que llevó a exigirle la implementación de medidas de seguridad de nivel básico.

Así, del análisis de dicho contrato de encargado del tratamiento, así como de los contratos de prestación de servicios para la fase de implantación y gestión de la T-movilidad suscritos entre SocMobillitat e Indra , obrantes en el expediente, se desprende que el proyecto T-movilidad implica el tratamiento de un elevado volumen de datos personales de las personas usuarias del transporte, que incluye categorías especiales de datos, y que el propio sistema debe proporcionar servicios críticos (interrelación con usuarios a a través del portal web, funcionamiento del billete y procesamiento de los datos mediante el CPD, etc.), para la prestación de un servicio especialmente relevante como es un servicio de movilidad por toda la red de transporte público. El conjunto de estas circunstancias concurrentes en el tratamiento de datos, plasmadas en las conclusiones del informe del Área de Tecnología y Seguridad de la Autoridad, y reproducidas en el apartado de hechos imputados tanto del acuerdo de incoación como de la propuesta de resolución, no han sido rebatidas en ningún momento por SocMobilitat , y son las que han llevado a la Autoridad a concluir que la categorización del sistema de información como básico, no es suficiente, de conformidad

con las determinaciones del ENS, y que, por tanto, SocMobilitat no ha determinado de manera adecuada en el contrato de encargo, las medidas de seguridad que Indra debía aplicar en la ejecución de las tareas encomendadas.
Es por ello , que la afirmación de SocMobilitat en el sentido de que la Autoridad no es competente para determinar que la categorización del sistema como básico resulta en este caso insuficiente, y que esta valoración la habría efectuado sobre presunciones o prueba insuficiente, se desmiente en base a las consideraciones expuestas en este apartado.

2.2 Sobre la carencia de comisión de la conducta infractora.

SocMobilitat reitera en sus alegaciones a la propuesta de resolución, como ya lo hacía ante el acuerdo de incoación, que no ha cometido la conducta que se le imputa en el presente procedimiento, es decir, que no es cierto que no haya categorizado de forma apropiada el nivel de riesgo para el tratamiento de datos encomendado a Indra y, consecuentemente, que no haya determinado de forma adecuada en el contrato de encargo de tratamiento, las medidas de seguridad que Indra debía aplicar en l ejecución del contrato para garantizar un nivel de seguridad adecuado al riesgo, en tanto que:

-es un hecho probado que SocMobilitat llevó a cabo un análisis de riesgos, tal y como exige el artículo 32.2 del RGPD, así como la ATM (responsable del tratamiento) en el contrato de encargo suscrito en fecha 31/ 09/2021, análisis de riesgo fechado en el mes de octubre de 2020 y que SocMobilitat facilitó a la Autoridad en el marco de las actuaciones del PS (...), cuestión diferente, aduce SocMobilitat , es su valoración la Autoridad en el presente procedimiento, y que no comparte.

- que es también un hecho probado que SocMoblitat determinó, de forma clara, las medidas de seguridad que Indra debía adoptar en el contrato de encargo, haciendo referencia expresamente a la necesidad de aplicar las medidas de seguridad que se ajusten al Esquema Nacional de Seguridad (NIVEL BÁSICO) así como cualesquiera otras medidas adicionales que fueran necesarias para garantizar la seguridad de acuerdo al riesgo, cuestión que, según dice, no suscitó a Indra ninguna duda interpretativa .

Es decir, lo que vendría a sostener SocMobilitat , es que a través del análisis de riesgo se habrían visto “compensadas” las posibles deficiencias derivadas de una categorización inadecuada del sistema de información.

Al respecto, tal y como se ponía de manifiesto en la propuesta de resolución, la cuestión es hasta qué punto es compensable el hecho de que, tal y como sostiene SocMobilitat: “Se establecieron en los contratos de subencargados de tratamiento *en cuanto a la seguridad del tratamiento que estas empresas implantaran las medidas apropiadas respecto a la seguridad del tratamiento que se correspondieran con las de la Administración contratante y que se ajustaran al Esquema Nacional de Seguridad (Nivel Básico)”* . Una compensación que SocMobilitat intenta atribuir al referido análisis de riesgo, oa que a pesar de la categorización de básico “[...] *en todo caso, el encargado debía implementar mecanismos para:*

a. *Garantizar la confidencialidad , integridad , disponibilidad y resiliencia permanentes de los sistemas y servicios del tratamiento .*
b. *Restaurar la disponibilidad y el acceso a los datos personales de forma rápida , en caso de incendio físico o técnico .*

c. *Verificar, evaluar y valorar, de forma rígida, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento .*
d. *Seudonomizar y cifrar los datos personales , si procede .*

En conjunto, debía adoptar todas aquellas otras medidas que, teniendo en cuenta el conjunto de tratamientos que realiza, fuesen necesarias para garantizar un nivel de seguridad adecuado al riesgo. "

En primer lugar procede exponer que la categorización del sistema prevista en el ENS debe ser el resultado de valorar el impacto sobre las informaciones y servicios que discurren sobre el sistema de información objeto de análisis -art. 43 y Anexo I-. Por el contrario, el análisis de riesgo es el resultado de analizar el riesgo derivado de determinadas amenazas que se proyectan hacia los activos más valiosos del sistema – medida op.pl.1-.

En consecuencia, mientras que en la categorización del sistema se valora la criticidad de un determinado sistema de información (a partir de las informaciones y servicios), en el análisis de riesgo únicamente se analiza la criticidad de determinadas amenazas en relación con los propios activos que configuran el sistema.

El hecho de que el ámbito de análisis sea distinto se traslada también a la incidencia de la valoración. Así, mientras que la categorización del sistema implica el establecimiento de un nivel mínimo de seguridad que cristaliza en todas las medidas de seguridad previstas en el ENS – anexo II, el análisis de riesgo únicamente implica, para aquellos casos en que se considere que el riesgo de un determinado elemento del sistema sea inaceptable, implementar alguna medida concreta que permita su traslado por debajo del nivel máximo de tolerancia al riesgo.

Así, la propia categorización del sistema incide en la medida de seguridad específica "análisis de riesgo" de tal forma que una incorrección en la propia categorización afecta no sólo a todas las medidas de seguridad sino también a la correspondiente al análisis de riesgo (op. pl.1).

Lo cierto es que el análisis de riesgo se configura como un elemento adicional o complementario. Una mera observación sistemática de la norma jurídica ya permite observar que mientras que la categorización del sistema constituye el eje central y vertebrador de la misma constituyendo un capítulo -el X- y el primero de los anexos del ENS, el análisis de riesgo es únicamente una de las 75 medidas previstas en el ENS.

En definitiva, la categorización del sistema implica definir hasta qué punto el sistema es crítico y, a partir de la categoría resultante, determinar qué medidas y en qué grado deben ser necesariamente aplicadas, precisamente en atención a la información y servicios vinculados al sistema objeto de análisis. Las implicaciones prácticas del establecimiento de este mínimo afectan pues a un número significativo de medidas diferentes y en "cómo" deben ser particularmente aplicadas, de acuerdo con la previsión efectuada por el legislador.

La disfunción asociada pues a una categorización errónea del sistema no puede ser compensada ni a través de una modulación, que únicamente comprenderá aquellas medidas indispensables para reducir un riesgo inaceptable de algún "activo" del sistema, ni tampoco con una mera referencia genérica a la necesidad de garantizar las distintas dimensiones de seguridad, etc. Y esto porque cuando el encargado deba concretar "qué

medidas" necesariamente debe aplicar y "cómo debe hacerlo", la categorización erróneamente efectuada le inducirá a error, ya la inaplicación efectiva de medidas que, en el marco de una adecuada categorización del sistema, serían obligatorias.

Así, ya modo de ejemplo, en el articulado contractual antes transcrito de entre las referencias genéricas se encuentra la siguiente indicación: *b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incendio físico o técnico.* " Pues bien, cuando el encargado deba dirimir con cierto grado de precisión qué medidas concretas deben aplicarse, la referencia ineludible la constituirá la propia categorización errónea del sistema (**básica)** que le viene contractualmente fijada.

El ENS prevé hasta 15 medidas que específicamente afectan "exclusivamente" a la disponibilidad (hay que tener en cuenta que otras muchas también inciden en ellas si bien no sólo a la dimensión Disponibilidad). La determinación del nivel asociado a la dimensión de disponibilidad forma parte del proceso de categorización del sistema de información. Tanto es así que el hecho de que se categorice el sistema de información de categoría básica implica a su vez que el nivel máximo relativo a "Disponibilidad" no sea superior al "bajo", lo que comporta que, eventualmente, sólo serían exigibles. las 15 medidas que el ENS prevé en relación específicamente a "disponibilidad".

Por último, el propio análisis de riesgo al que se refiere SocMobilitat a sus alegaciones y que facilitó a la Autoridad, como se ha dicho, en el marco del PS (...) (incorporado a las presentes actuaciones como se hace constar en el antecedente 2º de esta resolución), también corrobora el hecho de que el análisis incide únicamente en un reducido abanico de medidas de seguridad, por lo que no posibilita en ningún caso compensar el mínimo garantizado en cuanto a medidas de seguridad que deriva de la categorización del sistema (y de la correcta valoración de los niveles de seguridad correspondiente a cada una de las dimensiones que configuran el proceso de categorizar el sistema de seguridad). Así, únicamente se apunta, y de forma poco específica, que había que llevar a cabo 6 actuaciones/medidas (p. 18), mientras que el ENS recoge 75. Además, no hay garantías de que estas 6 actuaciones satisfagan las exigencias derivadas de la categorización que eventualmente correspondería. Y, siguiendo con el ejemplo anterior relativo a la "disponibilidad", se constata que a través de estas 6 medidas en modo alguno se compensarían las carencias asociadas a la no aplicación oa la incorrecta aplicación de las 12 medidas previamente señaladas.

En resumen, la categorización del sistema en el marco del ENS es el aspecto principal para poder determinar las medidas de seguridad a aplicar, y subcategorizar el sistema tiene unas implicaciones en términos de falta de protección que no se pueden compensar ni en el plano teórico, ni en el práctico, ni a través de un análisis de riesgo o una mera declaración genérica sobre, por ejemplo, la necesidad de proteger determinadas dimensiones de seguridad; pues precisamente el objetivo perseguido del ENS consiste en especificar las medidas de seguridad concretas que es necesario necesariamente aplicar y cómo debe llevarse a cabo esta aplicación de manera específica.

Por todo lo expuesto hasta aquí, no puede lograr la alegación de SocMobilitat , en el sentido de que a través del análisis de riesgo se habrían visto "compensadas" las posibles deficiencias derivadas de una categorización inadecuada del sistema de información en el contrato de encargado del tratamiento suscrito con Indra , y que, por tanto no se habría cometido la conducta infractora que es objeto de imputación, lo que hace decaer también la siguiente alegación.

2.3 Sobre la ausencia de culpabilidad y la debida diligencia.

En la línea de lo anterior, SocMobilitat esgrime que, en tanto que cumplió con las "exigencias del artículo 32 del RGPD" y "desplegó en todo momento una actividad diligente", desde el momento en que, según a su juicio, valoró de forma adecuada el nivel de riesgo para el tratamiento de datos que implicaba la ejecución del encargo, y que, consiguientemente, determinó de forma adecuada las medidas de seguridad que el encargado del tratamiento debía 'implementar, de mantenerse la imputación efectuada en la propuesta de resolución, se estaría sancionando a SocMobilitat por la materialización de un incidente, (el incidente que sufrió Indra vinculado con las credenciales del sistema de configuración del portal de acceso) y, por tanto, por unos resultados y no por la falta de determinación de medidas adecuadas. Es decir, afirma que se estaría considerando que la seguridad de los datos es una obligación de resultados y no de medios, por lo que carecería el elemento de culpabilidad necesario para poder exigirle responsabilidades en la infracción que se le imputa , tal y como establece el artículo 28 de la Ley 40/2015 de Régimen Jurídico del Sector Público y la jurisprudencia que invoca.

Al respecto, cabe poner de manifiesto en primer lugar que, efectivamente, se coincide con la entidad imputada en la que el principio de culpabilidad, es decir, la necesidad de que exista dolo o culpa en la acción punitiva, es plenamente aplicable al derecho administrativo sancionador.

Ahora bien, de acuerdo con lo que ya se ha dicho de forma reiterada en esta resolución, lo que se imputa a SocMobilitat en el presente procedimiento no es la falta de adopción de medidas de nivel básico en la configuración del portal de acceso de la T-movilidad que dio lugar al incidente de seguridad notificado por accesos indebidos, ni tampoco el hecho de que se haya materializado este incidente, sino, como se ha dicho también de forma reiterada, el no haber evaluado de forma adecuada el nivel de riesgo para el tratamiento de datos derivado de las prestaciones técnicas encargadas a Indra para la implantación y gestión de la T-movilidad, ya partir de ahí el no haber determinado de forma adecuada en el contrato de encargo de tratamiento, las medidas de seguridad técnicas y organizativas que Indra debía adoptar para garantizar un nivel de seguridad adecuado al riesgo del tratamiento objeto de encargo. Y esta conducta infractora se ha materializado, con independencia de la conducta de Indra , de la actuación del tercero que puso de manifiesto la vulnerabilidad del sistema, y del propio incidente de seguridad provocado por la falta de aplicación por parte de 'Indra de las medidas de seguridad de nivel básico exigidas.

Así pues, con base en todo lo expuesto, e incluso si la conducta que se imputa a SocMobilitat pudiera obedecer a un error documental en el momento de la configuración del contrato de encargado del tratamiento, como parecía apuntar en la segunda alegación ante el acuerdo de incoación cuando hacía referencia a una "categorización documental errónea" , se observa una clara falta de diligencia por falta de verificación de las obligaciones que encomendaba al subencargado del tratamiento en el contrato en lo que se refiere a la seguridad de los datos.

Ésta es la doctrina del Tribunal Supremo cuando pone de manifiesto, entre otros en la sentencia de 25/01/2006 dictada en materia de protección de datos, que " *el principio de culpabilidad consiste en la falta de diligencia observada por la entidad recurrente al tratar de forma automatizada una fecha relativa a la ideología del denunciante , resultando irrelevantes las invocaciones que se hacen (...) acerca de la ausencia de intencionalidad oa la existencia del error, y eso por cuanto el elemento culpabilístico del tipo sancionador*

aplicado concurre cuando se incluye la expresada fecha sobre la ideología , no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado ".

En definitiva, para determinar la concurrencia del elemento culpabilístico no es necesario que los hechos se hayan producido con dolo o intencionalidad, sino que es suficiente " *la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de archivos o del tratamiento de datos de extremar la diligencia..* ." (Sentencia de la Audiencia Nacional de 12/11/2010, recurso n. 761/2009), como es el supuesto aquí analizado, donde ha quedado acreditado que existe un claro incumplimiento del artículo 32 del RGPD en la categorización del nivel de seguridad exigido en el tratamiento de datos en cuestión, atribuible al menos a una falta de diligencia en el cumplimiento de las obligaciones que en materia de medidas de seguridad impone la normativa de protección de datos

Y este deber de diligencia es máximo cuando se realizan actividades que afectan a derechos fundamentales, como es el derecho a la protección de datos de carácter personal. Así lo ha declarado la Audiencia Nacional en su sentencia de 05/02/2014 (recurso n. 366/2012), cuando sostiene que la condición de responsable de tratamiento de datos personales "impone *un deber especial de diligencia a la hora de llevar a cabo el uso o tratamiento de las datos personales o su cesión a terceros , en lo que concierne al cumplimiento de los deberes que la legislación sobre protección de datos establece para garantizar los derechos fundamentales y las libertades públicas de las personas físicas , y especialmente su honor e intimidad personal y familiar, cuya intensidad se encuentra potenciada por la relevancia de los bienes jurídicos protegidos por aquellas normas ".*

En conclusión, en el presente caso es clara la concurrencia del elemento culpabilístico en la conducta de SocMobilitat , exigido por la normativa y la jurisprudencia para poder exigirle responsabilidades en la comisión de la infracción imputada en el presente procedimiento sancionador, sin que en esta conclusión incida su carencia de intencionalidad.

3 . En relación con la conducta descrita en el apartado de hechos probados, es preciso acudir al artículo 32 del RGPD reiteradamente citado en esta resolución, que prevé lo siguiente en cuanto a la seguridad del tratamiento:

"1. Teniendo en cuenta el estado de la técnica , los costes de aplicación , y la naturaleza , el alcance , el contexto y las fines del tratamiento , así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas , el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo , que en su caso incluya , entre otros :
a) la seudonimización y el cifrado de datos personales ;
b) la capacidad de garantizar la confidencialidad , integridad , disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento ;
c) la capacidad de restaurar la disponibilidad y el acceso a las datos personales de forma rápida en caso de incidente físico o técnico ;
d) un proceso de verificación , evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento .

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos , en particular como consecuencia de la destrucción , pérdida o alteración accidental o ilícita de datos personales transmitidos ,

conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos ."

Así pues, queda claro que el artículo 32, incidiendo especialmente en el apartado 2, establece la obligación de llevar a cabo una evaluación de riesgos de los tratamientos de datos personales que se prevea realizar, a fin de poder determinar las medidas de seguridad apropiadas para garantizar su seguridad y los derechos de las personas afectadas.

Por tanto, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y las finalidades del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento deben establecer o determinar las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo del tratamiento.

En el caso que nos ocupa, ha quedado acreditado que en el contrato de encargo de tratamiento suscrito entre SocMobilitat e Indra en fecha 30/09/2021 para la prestación de servicios en la fase de implantación y gestión de la T- movilidad, por cuenta de ATM, la entidad SocMobilitat indicó a Indra que las medidas de seguridad que debía implementar para la prestación de los servicios objeto de encargo eran de nivel básico (*El encargado del Tratamiento implantará las*
Medidas apropiadas respecto a la seguridad del Tratamiento , que se correspondan con las de la Administración contratante y que se ajustan al Esquema Nacional de Seguridad (***NIVEL BÁSICO*** *).(...)" (* cláusula 7.5) *,* es decir, que se categorizó el sistema como básico, cuando, de acuerdo con las circunstancias concurrentes en el tratamiento objeto de encargo el nivel básico no sería suficiente, es decir, que SocMobilitat no determinó de forma adecuada las medidas de seguridad que el encargado de tratamiento debía implementarse para la prestación objeto de encargo, lo que implica un incumplimiento de las previsiones del artículo 32 del RGPD.

Este hecho imputado, es decir, el hecho de no determinar de forma adecuada las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo, es constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"* , entre las cuales, las previstas en el artículo 32 RGPD, el apartado 2 del que vincula de forma clara la correcta determinación del nivel de seguridad del tratamiento a la evaluación de los riesgos que éste presenta.

4 . Al no meterse la entidad SocMobilitat , jefe de los sujetos previstos en el artículo 77.1 del LODGDD , resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD .

El artículo 83.4 del RGPD prevé para las infracciones allí previstas, se sancionen con una multa administrativa de 10.000.000 de euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 2% 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 establecen los artículos 83.2 RGPD y 76.2 LOPDGDD, y también de conformidad con el principio de proporcionalidad consagrado en el artículo 29 de la Ley

40/2015, tal y como indicaba la persona instructora en la propuesta de resolución, procede imponer la sanción de 10.000 euros (diez 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:

- La falta de intencionalidad (art.83.2.b) RGPD).
- La falta de comisión de infracciones anteriores (art.83.2.e) del RGPD), al no constar que SocMobilitat haya sido sancionada con anterioridad por una vulneración de la normativa de protección de datos.
- La falta de constancia de la obtención de beneficios como consecuencia de la infracción (art. 83. 2. k) RGPD y 76.2.c) LOPDGDD).

Por el contrario, como criterios agravantes, hay que tener en cuenta los siguientes elementos :

- La naturaleza, gravedad y duración de la infracción (art.83.2.a).
- La vinculación de la actividad de SocMobilitat con la realización de tratamientos de datos personales, en tanto que SocMobilitat es la empresa que tiene el encargo de la ATM de Barcelona de desarrollar e implementar la tecnología de pago sin contacto en el transporte público de el ámbito del sistema tarifario integrado; y la integración de otros de movilidad en el futuro.

5 . Ante la constatación de las infracciones previstas en el art. 83 del RGPD en relación con ficheros o tratamientos 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 también las medidas oportunas para que cesen o se corrijan sus efectos.

En virtud de esta facultad, procede requerir SocMobilitat para que lo antes posible, y en todo caso en el plazo máximo de 1 mes a contar desde el día siguiente de la notificación de esta resolución, adopte la medida correctora consistente en instar en Indra , en base a una adecuada categorización del riesgo del sistema de información, a la adopción de las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo para la prestación objeto de encargo, de conformidad con lo que establecen los artículos 28 y 32 del RGPD, dado que las medidas correspondientes al nivel básico del ENS resultan insuficientes.

Una vez adoptada la medida correctora descrita en el plazo señalado, en el plazo de los 10 días siguientes SocMobilitat debe informar a la Autoridad, sin perjuicio de la facultad de inspección de esta Autoridad para efectuar las verificaciones correspondientes .

Por todo esto, resuelvo:

1. Imponer a SocMobilitat la sanción consistente en una multa de 10.000.- euros (diez mil euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.2, ambos del RGPD.

2. Requerir SocMobilitat para que adopte la medida correctora señalada en el fundamento de derecho 5º y acredite ante esta Autoridad las actuaciones llevadas a cabo para cumplirla.

3 . Notificar esta resolución a SocMobilitat .

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.