Identificació de l'expedient

Resolució del procediment sancionador núm. PS 35/2022, referent a Indra Sistemas, SA.

Antecedents

1. En dates 05/10/2021, 06/10/2021, 07/10/2021, i 26/10/2021 van tenir entrada a l'Autoritat Catalana de Protecció de Dades, fins a sis denúncies (dues d'elles per remissió de l'Agència Espanyola de Protecció de Dades) formulades de manera separada per persones ciutadanes contra l'Autoritat del Transport Metropolità (en endavant, l'ATM), i una denúncia formulada contra la Societat Catalana per a la Mobilitat, SA, (en endavant, SocMobilitat), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, les persones denunciants es queixaven que en data 05/10/2021 s'havia detectat una vulnerabilitat de seguretat en el portal T-mobilitat.atm.cat, (https://t-mobilitat.atm.cat) que hauria permès l'accés per part de tercers a les seves dades personals allà enregistrades, facilitades per donar-se d'alta com a usuaris de la nova targeta T-Mobilitat (nom i cognoms, DNI, adreça postal i correu electrònic). Així mateix, es queixaven que la vulnerabilitat detectada permetia la modificació de la informació dels usuaris allà continguda.

Per tal de justificar els fets denunciats, les persones denunciants aportaven la següent documentació:

-Captura de pantalla del fil del tuit publicat per un ciutadà en data 05/10/2021 (a les 15: 39 h) on es mostra l'escletxa de seguretat i la manera en què es podia accedir a la informació de terceres persones, i s'indicava els passos a seguir (https://twitter.com (...)).

-Notícia publicada als mitjans de comunicació en data 05/10/2021 "*Un error en la web de la T-Mobilitat deja al descubierto datos de los usuarios".*

- Tuits publicats per T-Mobilitat al seu canal en dates 05/10/2021, i 06/10/2021, respectivament, en relació a l'incident objecte de denúncia:

"*Hem detectat un error operatiu al web de la T-Mobilitat, en etapa de proves. L'errada ha permès durant temps limitat l'accés a dades no sensibles. L'ATM obrirà un expedient informatiu a l'empresa responsable d'aquest desenvolupament web*" (05/10/2021 a les 17:00 h).

"*L'accés al web T-mobilitat.cat en aquesta fase de proves ha quedat suspès temporalment. Hem decidit fer, amb l'Agència de Ciberseguretat, una anàlisi exhaustiva per descartar qualsevol altra vulnerabilitat no detectada*." (06/10/2021 a les 18.00 h).

2. L'Autoritat va obrir una fase d'informació prèvia, d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador, i les persones presumptament responsables.

3. L'ATM, en compliment del que preveu l'article 33 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD), i en la seva condició de responsable de tractament va notificar a aquesta Autoritat en data 06/10/2021, la violació de seguretat de les dades patida (NVS 86/2021), consistent en la vulnerabilitat detectada en el portal T-mobilitat.atm.cat, que va comprometre dades personals dels usuaris allà registrades. Les actuacions dutes a terme en el marc de la notificació de la dita violació de seguretat (NVS 86/2021) es van incorporar a la fase d'informació prèvia oberta amb motiu de les denúncies presentades davant l'Autoritat pels mateixos fets.

4. En la fase d'informació prèvia, en data 15/11/2021 es va requerir l'ATM perquè donés compliment al següent:

- D'una banda que informés si es disposava de nova informació que modifiqués en algun aspecte les manifestacions efectuades, en el marc de la notificació a l'Autoritat de la violació de seguretat, en relació al resultat de l'anàlisi sobre l'incident efectuat per l'Agència de Ciberseguretat, i recollit en "l'informe sobre la vulnerabilitat de seguretat detectada en el portal T-mobilitat.atm.cat el 05/10/2021", i en el seu annex, i en concret respecte a:

"Cronologia de la incidència
El dia 5 d'octubre del 2021 a les 15:39 un ciutadà publica al Twitter una vulnerabilitat detectada en el portal T-mobilitat.atm.cat
A les 16:24 ATM indica la vulnerabilitat al proveïdor SOC Mobilitat.
Es convoca un comitè tècnic urgent per revisar-la i procedir al seu mitigament.
A les 16:40 es mitiga la vulnerabilitat.

"Accés a dades
Les dades compromeses són el nom, cognoms i identificador de usuari, no de la paraula de pas d'entrada al portal web. Recalcar que no hi ha hagut afectació en les dades ubicades en els Sistemes Centrals del sistema T-mobilitat sinó únicament en aquelles corresponents al portal web. Tampoc hi ha hagut afectació a la integritat de les dades.
L'abast de les dades compromeses ha estat confirmat per l'Agència de Ciberseguretat de Catalunya com a conclusió de l'anàlisi de dades que han realitzat en base a la informació proporcionada per ATM (Veure Annex 1).
El volum de dades compromeses és de 2.161 registres, dels quals 1.046 són interns de test del sistema.

Causa de la vulnerabilitat
En la infraestructura de tecnologia Liferay del portal T-mobilitat.atm.cat havia quedat configurat l'usuari, paraula de pas, i la possibilitat nativa d'entrar que ve per defecte del fabricant.
D'aquesta manera es podia accedir des de Internet a les pàgines de configuració del propi portal i entrar amb l'usuari per defecte.

Accions de mitigació realitzades
Les següents accions s'han realitzat sobre la infraestructura de tecnologia Liferay del portal T-mobilitat.atm.cat:
• *Deixar només un usuari administrador i canviar-li la paraula de pas.*
• *Desconnectar la possibilitat nativa d'entrar a Liferay*.

• *Comprovar a través d'un script que no s'ha modificat cap contingut del portal. En aquest cas s'ha confirmat que no hi ha hagut cap modificació."*

-D'altra banda, que confirmés si la violació de seguretat de les dades patida, s'hauria produït en el marc d'un encàrrec encomanat a la Societat Catalana per a la Mobilitat, SA. En cas de resposta afirmativa, aportés còpia del contracte d'encarregat de tractament subscrit amb dita entitat.

5. En data 22/11/2021, l'ATM va respondre l'anterior requeriment, a través d'escrit en què exposava el següent:

- Que no s'havia produït cap modificació, respecte la informació aportada en la notificació de la violació de seguretat, que "era correcta i s'ajustava a la realitat dels fets ocorreguts."

- Que la violació de seguretat, es va produir *"*en el marc d'un encàrrec encomanat a la Societat Catalana per a la Mobilitat SA.*"*

S'adjuntava el contracte d'encàrrec del tractament subscrit entre l'ATM (responsable del tractament) i SocMobilitat (encarregat del tractament) el 30/09/2021 per a la prestació de serveis per a la fase d'implantació i de gestió de la T-Mobilitat.

6. D'acord amb els antecedents que s'han relacionat fins aquí i amb el resultat de les actuacions d'indagació dutes a terme en el marc de la informació prèvia, que engloba tant les denúncies interposades contra l'ATM (a les que s'assignà núm. IP 394/2021, 395/2021, 400/2021, 403/2021, 431/2021 i 432/2021) com la denúncia interposada contra Soc Mobilitat (a la que s'assignà núm. IP 397/2021), la Directora d'aquesta Autoritat va acordar en data 10/01/2022 iniciar un procediment sancionador contra l'encarregat del tractament Soc Mobilitat (PS (...)), per la presumpta vulneració del principi de seguretat de les dades en el desplegament del portal T-Mobilitat i conseqüent vulneració de la seva confidencialitat, i d'acord amb el règim de responsabilitat en matèria de protecció de dades previst a l'article 28.10 de l'RGPD, que preveu que l'encarregat del tractament és responsable davant l'autoritat de control, de les presumptes vulneracions de la normativa de protecció de dades que es puguin cometre en el desenvolupament de l'encàrrec que incompleixin el que s'estableix a l'encàrrec. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 17/01/2022.

7. En data 04/02/2022,SocMobilitat va formular al·legacions a l'acord d'iniciació aportant junt amb el seu escrit documentació diversa. Entre aquesta documentació, el contracte d'encarregat de tractament subscrit entre SocMobilitat i Indra Sistemas SA (en endavant, Indra), en data 30/09/2021 per a la prestació de serveis tècnics en el marc del Projecte Tecnològic T-mobilitat adjudicat a SocMobilitat (document núm.2), entre els quals, i segons manifesta, el desplegament del portal T-mobilitat, i l"Informe jurídico en relación a la brecha de seguridad del portal extranet de T-Mobilitat" (document núm.6).

8. A la vista de les al·legacions formulades, i de l'anàlisi de la documentació aportada per l'entitat imputada, en data 26/04/2022 es va requerir a SocMobilitat l'aportació de documentació addicional, més concretament:

-Còpia dels contractes de prestació de serveis per a la fase d'implantació i de gestió per a la T-Mobilitat subscrits entre SocMobilitat i Indra en data 21/07/2014, i de les seves posteriors

modificacions o addendes, a què feia referència el contracte d'encarregat del tractament subscrit entre SocMobilitat i Indra en data 30/09/2021 (clàusula 2a: "Condiciones y finalidades del tratamiento":

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

-Còpia de l'avaluació o de l'anàlisi de riscs efectuat per SocMobilitat pel que fa al tractament de dades derivat de les prestacions tècniques encomanades a Indra en dits contractes. Al respecte, en el contracte d'encarregat del tractament es feia constar el següent:

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

9. En data 03/05/2022 l'entitat SocMobilitat va donar compliment a dit requeriment i aportà còpia dels contractes de prestació de serveis per a la implantació i gestió de la T-Mobilitat subscrits entre SocMobilitat i Indra en data 21/07/2014 i de les seves modificacions, i còpia de l'anàlisi de riscos.

En dits contractes de prestació de serveis per a la implantació i gestió de la T-Mobilitat subscrits entre SocMobilitat i Indra en data 21/07/2014, consta com a tasca assignada a Indra el desplegament del portal web de la T-mobilitat.

10. De l'anàlisi de tota la documentació aportada per SocMobilitat en la tramitació del procediment sancionador (...), es va constatar que els fets que van motivar la seva incoació, és a dir, la vulneració del principi de seguretat de les dades en el desplegament del portal T-Mobilitat i conseqüent vulneració de la seva confidencialitat, per manca d'aplicació de determinades mesures de seguretat, era imputable a Indra Sistemas, SA en el marc del contracte d'encàrrec del tractament de dades personals subscrit entre SocMobilitat (adjudicatària del contracte i encarregada del tractament) i Indra (sòcia accionista de SocMobilitat i sotsencarregada del tractament), per a la prestació de serveis en la fase d'implantació i de gestió de la T-mobilitat.

En aquest sentit, en el contracte d'encàrrec del tractament de dades personals subscrit entre SocMobilitat i Indra en data 30/09/2021 s'estipulaven les mesures de seguretat que Indra havia d'adoptar per a la prestació objecte d'encàrrec:

"7. Obligaciones del encargado del tratamiento (...)

"7.5. Seguridad del Tratamiento

*El encargado del Tratamiento implantarà las Medidas apropiadas respecto a la seguridad del Tratamiento, que se correspondan con las de la Administración contratante y que se ajusten 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 los 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 los 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." (...).

Dit això, les mesures de seguretat que es van vulnerar en la configuració del portal de la T-mobilitat, que van propiciar que l'accés quedés obert, i al seu torn, accessible a tercers, són de nivell bàsic (apartat 4.1.2 "Arquitectura de la Seguridad"),4.2 relatiu al control d'accés, i apartat 4.3.2 relatiu a la "configuració de seguretat") de l'Esquema Nacional de Seguretat (ENS) aprovat pel Reial Decret 3/2010, a què s'hi fa referència.

A la vista de tot l'anterior i de conformitat amb l'article 20.1.c) del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat de Catalunya, en data 27/05/2022, la Directora de l'Autoritat Catalana de Protecció de Dades va acordar sobreseure el procediment núm. (...) iniciat contra SocMobilitat, en considerar que no es podia atribuir a SocMobilitat la responsabilitat de la manca d'aplicació de les mesures tècniques apropiades per garantir la seguretat de les dades objecte de tractament, atès que l'adopció d'aquestes mesures de seguretat, i en concret les de nivell bàsic, era una obligació que corresponia a Indra, com a sotsencarregat del tractament, tal i com s'estipula en el contracte d'encàrrec del tractament de dades personals subscrit en data 30/09/2021 entre SocMobilitat i Indra. En la mateixa resolució de sobreseïment es va acordar incoar un expedient sancionador a Indra Sistemas, SA, per tal de determinar la seva presumpta responsabilitat en la manca d'aplicació de mesures tècniques de nivell bàsic en la implantació del portal web T-mobilitat, exigides per SocMobilitat, que va propiciar que terceres persones poguessin accedir a les dades personals dels usuaris allà enregistrades.

En aquest sentit, cal tenir en compte que el règim de responsabilitat en matèria de protecció de dades establert a l'article 28.10 de l'RGPD, a què abans s'ha fet referència, és també aplicable al sotsencarregat del tractament, d'acord amb el que disposa l'article 28.4 de l'RGPD i 70.1.b) LOPDGDD (que es considera, en tot cas, un encarregat de l'encarregat del tractament), i, per tant, és també responsable, davant l'autoritat de control, de les presumptes vulneracions de la normativa de protecció de dades que pugui cometre en el desenvolupament de l'encàrrec que incompleixin el que s'estableix a l'encàrrec.

11. En data 01/06/2022, es va iniciar, per l'Acord de la directora de l'Autoritat Catalana de Protecció de Dades, el present procediment sancionador contra Indra, per una presumpta

infracció prevista a l'article 83.4.a), en relació a l'article 32.1; tots ells de l'RGPD. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 02/06/2022.

A l'acord d'iniciació es concedia a l'entitat imputada un termini de 10 dies hàbils per formular al·legacions i proposar la pràctica de proves que considerés convenients per defensar els seus interessos.

12. En data 15/06/2022, Indra va formular al·legacions a l'acord d'iniciació.

13. En data 09/09/2022, la instructora d'aquest procediment va formular una proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades imposés a Indra una multa de 25.000 euros com a responsable, d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32.1, pel que fa la principi de seguretat de les dades, ambdós de l'RGPD.

Aquesta proposta de resolució es va notificar en data 10/09/2022 i es concedia un termini de 10 dies per formular al·legacions.

14. En data 22/09/2022, l'entitat imputada va presentar un escrit d'al·legacions a la proposta de resolució.

Fets provats

En data 30/09/2021 la Societat Catalana per a la Mobilitat, SA, va formalitzar un contracte d'encarregat del tractament amb la societat Indra Sistemas, SA, per a la prestació de serveis en la fase d'implantació i de gestió de la T-mobilitat (entre d'altres, el desplegament del portal T-mobilitat).

L'execució d'aquest contracte, comportava que Indra accedia i gestionava les dades personals dels usuaris de la T-Mobilitat, i se li exigia l'adopció de mesures de nivell bàsic de l'ENS.

En el marc d'aquest encàrrec, el sotsencarregat del tractament, Indra, no va aplicar mesures tècniques de seguretat de nivell bàsic exigides per SocMobilitat, atès que en configurar el control d'accés al portal web de la T-Mobilitat no es va modificar la contrasenya que per defecte assigna el fabricant de la infraestructura de tecnologia "Liferay" a l'administrador (credencial d'accés pública), de tal manera que l'accés quedava obert, i al seu torn, accessible a tercers, mesura que l'ENS exigeix per als sistemes categoritzats de nivell bàsic.

Així doncs, des de la posada en marxa del portal T-Mobilitat (a les 08:00 del dia 04/10/2021), fins a les 16:40 h del dia 05/10/2021, qualsevol persona podia accedir a través d'internet a les pàgines de configuració del portal web T-mobilitat, i a la informació personal de tercers allà continguda, així com modificar-la, si s'introduïa la paraula de pas o contrasenya que per defecte assigna el fabricant de la infraestructura de tecnologia "Liferay" (software utilitzat per a la gestió de les targetes t-Mobilitat) a l'administrador. En concret les dades personals dels usuaris a què es va accedir eren: nom i cognoms, identificador d'usuari, i al propi fet que havien sol·licitat la nova targeta T-Mobilitat.

Així, consta acreditat l'accés per part d'un tercer a dites dades en data 05/10/2021 a les 15:39 h (ciutadà/usuari del portal que va publicar el tuit).

Fonaments de dret

1. Són d'aplicació les previsions de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (l'LPAC), i l'article 15 del Decret 278/1993, d'acord amb la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. La resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades, de conformitat amb els articles 5 i 8 de la Llei 32/2010.

2. L'entitat imputada ha formulat al·legacions tant a l'acord d'iniciació com a la proposta de resolució. En aquesta resolució s'analitzen el conjunt d'aquestes al·legacions.

2.1. Sobre l'accessibilitat al sistema per part de tercers.

Indra esgrimeix que reconeix que en configurar el control d'accés al portal web de la T-Mobilitat, no va modificar la contrasenya que per defecte assigna el fabricant de la infraestructura de tecnologia "Liferay" a l'administrador, però nega que això fos el que provoqués que, des de la posada en marxa del portal T-mobilitat fins a les 16:40 h del dia 05/10/2021, l'accés al portal quedés obert, i que qualsevol persona pogués accedir a través d'internet a la informació allà enregistrada.

En aquest sentit, Indra defensa, com ja exposava en les al·legacions a l'acord d'incoació, que des del moment de la posada en marxa del portal web, havia implementat un sistema d'identificació i autenticació d'usuaris protegit amb credencials, i que si bé és cert que l'accés havia quedat configurat amb la possibilitat nativa d'entrar amb les credencials que venen per defecte del fabricant, aquestes credencials estaven sota el control exclusiu de l'usuari administrador, i torna a reiterar que el que va provocar que deixessin d'estar sota el seu control exclusiu va ser l'actuació maliciosa d'un tercer que, aprofitant-se dels seus coneixements informàtics, va vulnerar les mesures de seguretat implementades per Indra, i mitjançant proves de penetració no autoritzades va endevinar la paraula de pas, va accedir a les dades reservades d'ATM, i va fer públiques les credencials de l'administrador a través de les xarxes socials, moment a partir del qual les credencials van deixar d'estar sota el control exclusiu de l'usuari administrador, i l'accés al sistema va quedar obert.

Al respecte, val a dir, com s'analitzarà amb detall en la propera al·legació i com ja es posava de manifest a la proposta de resolució, que no és pot admetre que el sistema d'identificació i autenticació implementat per Indra estigués protegit amb credencials que estaven sota el control exclusiu de l'administrador, i que el que va ocasionar que la porta d'entrada al sistema quedés oberta fos l'actuació d'un tercer que va vulnerar dit sistema, tenint en compte que és un fet no discutit que, per descuit o error, s'havia deixat activada (o no s'havia retirat) la contrasenya estàndard assignada per defecte pel fabricant a l'administrador (extrem, s'insisteix, reconegut per Indra), de tal manera que qualsevol persona podia entrar amb la dita contrasenya, sense que, per tant, l'administrador tingués en cap moment el "control exclusiu" sobre la dita contrasenya, com sosté Indra, doncs és evident que des del moment en què aquestes eren de caràcter públic (publicades a la documentació tècnica del fabricant i accessibles a internet per qualsevol persona), l'administrador no tenia cap control sobre les mateixes.

És per això que no pot prosperar l'al·legació esgrimida per Indra en el sentit que el que va provocar que l'accés quedés obert i accessible a tercers, va ser la vulneració de les mesures de nivell bàsic implementades per Indra, en tant que no es pot sostenir que tingués implementades dites mesures, quan el sistema de control d'accés no disposava d'un sistema d'autenticació d'usuaris protegit amb credencials configurades pel propi administrador, per tal de garantir que només podien accedir a les dades les persones autoritzades.

A l'últim cal recordar que, com ja es va posar de manifest per part de la persona instructora a la proposta de resolució, la imputació a Indra en el present procediment no deriva del fet que s'hagi materialitzat un accés a les dades per part d'un tercer no autoritzat, sinó que la conducta que se l'imputa és no haver implementat les corresponents mesures de seguretat en la configuració del control d'accés al portal web per garantir la confidencialitat de les dades allà enregistrades i assegurar la seva protecció front intents d´accessos indeguts, i en concret mesures de nivell bàsic de l'ENS que li van ser expressament exigides per SocMobilitat en el contracte d'encàrrec subscrit en data 30/09/2021.

2.2. Sobre l'incompliment de les mesures de seguretat per part d'Indra.

2.2.1 El deure de preservar la confidencialitat mitjançant la implementació de les mesures tècniques adequades.

Les al·legacions formulades per Indra, es centren exclusivament en discutir l'aplicació de les mesures de seguretat corresponents a l'ENS, i obvia tota referència a les obligacions que dimanen directament de l'RGPD, l'eix central del conjunt de la normativa de protecció de dades, més concretament, a l'obligació de mantenir la confidencialitat de les dades personals que es tracten, que és un deure recollit com a principi rector en l'article 5.1 f) de l'RGPD, invocat de manera constant tant en l'acord d'incoació com a la proposta de resolució, i que imposa que les dades han de ser:

> "*tratados de tal manera que se garantice una seguridad adecuada de los 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 («integridad y confidencialidad»)*"

Aquesta obligació es veu reforçada a l'art. 32.1 de l'RGPD, l'incompliment del qual s'imputa en el present procediment:

> "*1. 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, 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:*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento (...)*".

En relació a aquesta obligació no és una qüestió que estigui en discussió, que l'obligació de garantir la confidencialitat de les dades personals mitjançant l'aplicació de les adequades

mesures de seguretat, es va recollir expressament en el propi contracte d'encarregat del tractament subscrit entre SocMobilitat i Indra, és a dir, Indra, havia d'implementar les mesures de seguretat corresponents al nivell bàsic de l'ENS, i dur a terme les accions indispensables per garantir en tot moment la confidencialitat de la informació tractada, cosa que no va fer com s'analitza en els següents subapartats. Com tampoc és discutible que canviar la contrasenya que hi havia per defecte al software de gestió de "Liferay", no suposa anar més enllà de l'estat de la tècnica actual ni comporta costos d'implementació significatius.

En aquest marc, l'objecte de l'ENS és, justament, "assegurar el acceso, **integridad**, disponibilidad, autenticidad, **confidencialidad,** trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias". (art. 1.2).

Efectuades amb caràcter previ aquestes consideracions, s'analitzen a continuació els arguments esgrimits per Indra per intentar justificar que, en la configuració del control d'accés al portal web de la T-mobilitat, va complir amb les mesures de seguretat de nivell bàsic exigides per SocMobilitat.

2.2.2 El deure que el control d'accés sigui efectiu mitjançant l'ús de claus secretes (contrasenyes).

Una de les al·legacions principals d'Indra ,com ja s'avançava al punt 2.1 d'aquesta resolució, consisteix en assegurar que comptava amb un sistema de control d'accés adequat ja que "*Ninguna de estas normas* [cita prèviament un seguit de normes d'antecedents i coetànies a l'ENS] *establece expresamente qué se entiende por proteger el sistema de manera que nadie acceda a los recursos sin autorización, más allà de citar la necesidad de configurar un sistema de autenticación basado, por ejemplo, en usuario y contraseña* [...]".

No obstant quan, com reconeix Indra, s'està fent referència a la necessitat que el sistema d'accés es basi en la combinació d'usuari i contrasenya ja s'està especificant la naturalesa de la protecció que s'exigeix. Doncs "contraseña" implica, segons la definició de la RAE "una *seña* ***secreta*** *que permite el acceso a algo, a alguien o a un grupo de personas* ***antes inaccessible***".

De fet, aquest mateix caràcter secret també s'estableix en la pàgina 4 "Guia de Seguridad de las TIC CCN-STIC 821. Apéndice V: Normas de creación y de uso de contraseñas NP40": "*Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata*". Es tracta d'un instrument particularment vàlid com a mitjà d'interpretació de l'ENS, atès que les instruccions tècniques del CCN-STIC estan expressament previstes per aquesta finalitat en el propi ENS (apartat 7è de l'Annex II).

En altres termes, per tal que un sistema d'autenticació pugui considerar-se mínimament efectiu com a protecció, cal que exigeixi un usuari i una contrasenya entesa com una informació secreta. Per tant, en cap cas el sistema implementat per Indra podia ser considerat vàlid en la mesura que no complia amb quelcom essencial com era que la contrasenya fos secreta, ja que al ser la que incorporava per defecte el fabricant era públicament accessible.

La mesura 4.1.2 “Arquitectura de seguridad [op.pl.2]” de l’ENS indica que també pels sistemes de categoria bàsica caldrà detallar un sistema d’identificació i autenticació d’usuaris, i la mesura 4.2 “Control de acceso. [op.acc]” detalla les característiques indispensables tant de la identificació [op.acc.1] com de l’autenticació [op.acc.5]; ambdues mesures (4.1.2 i 4.2), citades expressament a l’acord d’incoació i la proposta de resolució.

La imputació fàctica a Indra consisteix justament en haver omès el deure de canviar la contrasenya que el fabricant establia per defecte en la funcionalitat Liferay. En conseqüència, resulta especialment transcendent i clarificador tot allò referit específicament a l’autenticació d’usuaris.

Certament, la mesura “4.1.2 Arquitectura de seguridad [op.pl.2]” estableix diferents opcions per a la identificació i autenticació d’usuaris, entre les quals les “contraseñas”. En qualsevol cas, si s’opta per l’opció de l’ús de contrasenyes és inherent al mateix concepte, tal i com s’ha exposat, que la mateixa tingui caràcter “secret”; característica que, com és obvi, s’incompleix si es tracta d’una contrasenya que un determinat fabricant incorpora per defecte en les seves solucions, doncs aquella contrasenya és coneguda per múltiples clients de la mateixa solució i pot fins i tot, com en aquest cas, haver-se fet pública a través d’internet.

L’apartat 4.2.5 que tracta específicament l’autenticació reforça així mateix la conclusió que el manteniment (no canvi) d’una contrasenya que es troba en una solució tecnològica per defecte per part del fabricant incompleix l’ENS. I és que sigui quina sigui l’opció emprada per a l’autenticació d’usuaris, s’ha de complir per tal de garantir-ne la “seguretat” que (i) “***1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario***”, i (ii) ***Las credenciales estarán bajo el control exclusivo del usuario.”*** Cap d’aquests dos requisits inexcusables es satisfan, s’insisteix, si es tracta de contrasenyes que per defecte havia implementat el fabricant de la corresponent solució tecnològica, doncs les credencials en cap moment estan sota el control exclusiu de l’usuari en la mesura que es tracta d’una clau coneguda per tercers (altres adquirents de la solució, el propi productor de la mateixa, qui hi tingui accés per internet, etc.).

En termes més planers, el propi RGPD i, en un grau major de concreció l’ENS, el que estableixen és que -entre altres dimensions - cal protegir la confidencialitat de la informació. Això s’aconsegueix principalment establint mecanismes d’accés (porta) de tal manera que únicament pugui accedir a la informació qui estigui autoritzat per fer-ho (qui tingui la clau per obrir la porta). Aquest mecanisme de protecció esdevindria ineficaç si aquestes claus fossin conegudes per tothom (fabricant, internautes, altres compradors de la solució, etc.). És evident que ni de l’RGPD ni de l’ENS es pot extreure la conclusió que una situació com la descrita pugui ser vàlida, atès que confrontaria directament amb el propòsit perseguit de protecció de la confidencialitat i, a més, aniria en contra del que quan es defineixen particularment les mesures d’autenticació s’exigeix: contrasenyes com a quelcom intrínsecament secret i, per tant, de control “exclusiu” per part de l’usuari. Exigir col·locar una porta que pogués obrir qualsevol no tindria cap sentit pràctic més enllà de generar una mera aparença de seguretat quan aquesta és inexistent.

En resum, l’ús de contrasenya com a mitjà d’autenticació requereix que la informació emprada sigui “secreta” ja que és una propietat que li és inherent, perquè si la contrasenya és coneguda s’incompleix el requisit que aquesta informació/clau estigui sota el control exclusiu de l’usuari.

2.2.3 L'aplicació integral de l'obligació d'establir un control d'accés eficaç.

L'última de les al·legacions plantejada per Indra per tal d'intentar sostenir que no hauria incomplert les mesures de seguretat de nivell bàsic exigides, consisteix en apuntar que l'obligació que la contrasenya sigui secreta i sota el control exclusiu de l'usuari no resultaria d'aplicació en la mesura que: (i) únicament estaria previst pels "equips" i que, (ii) tenint en compte – al seu parer – que els equips no tenen software, aquesta obligació no resultaria d'aplicació a l'assumpte objecte de l'expedient ja que Liferay és un software.

Amb caràcter preliminar cal contextualitzar que, tal i com ja s'ha exposat, l'obligació de protecció de la confidencialitat es projecta per tots els tractaments de protecció de dades en virtut de l'RGPD i, en conseqüència, no depèn de quin element tècnic concret s'utilitzi per dur a terme el tractament. Similarment, les mesures indicades de l'ENS (4.1.2 i 4.2 – i singularment el 4.2.5.-) fan referència de forma consistent al conjunt del sistema d'informació i als seus propis recursos:

> 4.1.2 "*La Seguridad del sistema serà objeto de un planteamiento integral detallando, al menos, los siguientes aspectos* [...]"
>
> 4.2 "*El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción*"
>
> 4.2.5 "*Los mecanismes de autenticación frente al sistema* [...]"

Es constata que aquestes exigències no són susceptibles de veure's alterades en funció de la naturalesa específica de quin element específic s'utilitzi. De fet, tenint en compte que Indra assumeix que Liferay és en qualsevol cas un component del sistema (p.10 de les al·legacions a l'acord d'incoació), les mesures 4.1.2 i 4.2 -i singularment la 4.2.5- li serien indubtablement d'aplicació. Més quan, justament en relació amb els "components del sistema, l'apartat 4.2.2 Requisits d'accés [op.acc.2] reforça la importància de controlar els accessos justament als diferents components del sistema (apartat c):

> "*c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.*"

En conseqüència, aquesta al·legació no pot desvirtuar les consideracions que s'han exposat als dos subapartats precedents. I això perquè Liferay forma part del sistema, que el propi ENS s'encarrega de definir en el seu annex IV com el "*Conjunto organizado de recursos para que la información se pueda recoger, almacenar, processar o tratar, mantenir, usar, compartir, distribuir, poner a disposición, presentar o transmitir*." És a dir, que quan les mesures indicades fan referència a la protecció del sistema de la informació implica l'assegurament del conjunt de recursos que s'utilitzen per dur a terme el tractament de la informació inclòs el software (Liferay).

Dit d'una altra manera, és incorrecte afirmar que el canvi de contrasenyes només afecta una tipologia específica "equips", quan la protecció de la informació té una vocació de ser integral en el sentit que la protecció del conjunt del sistema passa, òbviament, per assegurar el conjunt d'elements que el conformen (un dels quals, segons Indra, el software) i, tal i com s'ha explicat en els dos subapartats anteriors, la protecció de la confidencialitat, i les

obligacions específiques de l'ENS, comporten necessàriament canviar les contrasenyes que hi poguessin haver instal·lades per defecte per part del fabricant.

En definitiva, la imputació de la infracció a Indra d'incomplir la normativa de protecció de dades ni incorre ni pot fer-ho en una interpretació extensiva de cap concepte específic, ja que l'obligació que les contrasenyes siguin secretes i sota el control de l'usuari no presenta cap dependència sobre quin element es tracti (hardware o software...), únicament que formi part del sistema que tracti la informació.

Malgrat que entrar a donar resposta a la resta d'al·legacions formulades per part d'Indra no resultaria necessari a partir de l'anterior consideració, s'estima oportú fer-ho amb un ànim, novament, de completesa i, també, per evidenciar la incorrecció del seu plantejament.

Així, Indra apunta que cal efectuar una separació entre equips i software situant-los com a conceptes antagònics. Res més lluny de la realitat. La RAE defineix "equip" com el "Conjunto de aparatos constituido por una computadora y sus periféricos" i "computadora [electrónica]" com a "Máquina electrónica que, mediante determinados programas, permite almacenar y tratar información y resolver problemas de diversa índole".

És a dir, novament, afirma que és inherent a "equip" que hi hagi programes per tal que es pugui dur a terme funcions informàtiques/electròniques vinculades al tractament de dades.

S'arriba a la mateixa conclusió d'analitzar la pròpia mesura apuntada en el marc d'aquest expedient "4.3.2 Configuración de Seguridad [op.exp.2]", consistent en l'obligació de retirar les contrasenyes estàndard dels "equips" amb caràcter previ a la seva entrada a producció. Doncs la pròpia existència d'una contrasenya en un entorn informàtic, com és el cas, implica la presència d'un software que permeti justament contrastar si la contrasenya introduïda és vàlida o no.

Així doncs, l'error de base de caràcter tècnic en l'al·legació d'Indra condueix també a que la interpretació indegudament reduccionista que intenta efectuar perdi qualsevol sentit, ja no només estructural (Liferay és un element del sistema), sinó també material (no és possible contraposar software a equip ja que el software constitueix un aspecte essencial de qualsevol equip informàtic).

Retornant al principi d'aquest subapartat, fins i tot pel cas erroni que algú considerés que "equip" és quelcom antagònic a "software", cal recordar que Indra assumeix que el software en qualsevol cas és un "component del sistema", de tal manera que les obligacions que s'estableixen a nivell de sistema li són, sense cap dubte, d'aplicació. Així, quan l'RGPD i l'ENS (art. 1.2) exigeixen que es protegeixi la confidencialitat de la informació i quan l'ENS especifica que cal establir un control d'accés a nivell de sistemes (4.2.op.acc) és clar que tal obligació es projecta també envers el programa Liferay.

Des d'un punt de vista material, defensar el contrari equival a sostenir que la confidencialitat es troba adequadament preservada encara que les contrasenyes per accedir com a administrador al software-i per tant per poder-hi efectuar els canvis de màxima transcendència- siguin conegudes per part dels fabricants, altres compradors i per internautes en general.

I, des d'una òptica jurídica, assumir la posició d'Indra contravindria el propi esperit i funcionalitat última de la norma així com múltiples preceptes com els indicats i, fins i tot, altres que recullen aquest mateix esperit: protecció d'accés remot [op.acc.7] *"que nadie accederá a recursos sin autorización.*"

En definitiva, totes i cadascuna de les mesures específiques a les quals ha fet referència la instrucció d'aquest expedient tenen caràcter "bàsic", i li eren exigibles a Indra, tenint en compte que en el contracte d'encàrrec subscrit amb SocMobilitat es recollia expressament l'obligació d'implementar en tot cas les mesures de seguretat que corresponguessin a un sistema de categoria bàsica.

2.3 Sobre l´absència de culpabilitat.

En la línia de l'anterior, Indra esgrimeix que de mantenir-se la imputació efectuada en la proposta de resolució, s'estaria sancionant a Indra per la materialització d'un accés indegut per un tercer, i no per la manca d'aplicació de mesures de seguretat, és a dir, s'estaria considerant que la seguretat de les dades és una obligació de resultats i no de mitjans, per la qual cosa mancaria l'element de culpabilitat necessari en la seva conducta per poder-li exigir responsabilitats en la infracció que se li imputa, tal com disposa l'article 28 de la Llei 40/2015 de Règim Jurídic del Sector Públic i la jurisprudència que invoca.

Al respecte, cal posar de manifest en primer lloc que, efectivament, es coincideix amb l'entitat imputada en què el principi de culpabilitat, és a dir, la necessitat que existeixi dol o culpa en l'acció punitiva, és plenament aplicable al dret administratiu sancionador. Ara bé, d'acord amb el que ja s'ha dit de manera reiterada en aquesta resolució, la conducta de vulneració de seguretat de les dades que s'imputa a Indra és, precisament, la manca d'implementació de barreres de seguretat exigides per SocMobilitat per tal de protegir la confidencialitat de les dades enregistrades al portal web, i és un fet no discutit que el sistema va entrar en fase de producció amb dades reals d'usuaris, deixant activades les credencials que venien per defecte del fabricant.

Així doncs, és clar que en tant que Indra no va implementar mesures de seguretat de nivell bàsic que li eren exigibles, en la seva condició de sotsencarregada del tractament, va incomplir l'obligació establerta a l'article 32.1 de l'RGPD de protegir la seguretat de les dades, i aquesta sens dubte és una obligació de mitjans, sent doncs, responsable de la infracció que se li imputa en aquest procediment, perquè la seva comissió es va materialitzar amb independència de les actuacions dutes a terme pel tercer per accedir a les dades tractades. Dit d'una altra manera, la comissió de la infracció seria també imputable a Indra tot i que no s'hagués produït l'accés indegut d'aquest tercer.

En resum, l'element objectiu del tipus infractor de l'article 83.4.a) de l'RGPD, es perfecciona des del moment en què el sistema va entrar en fase de producció i no va implementar mesures de caràcter tècnic i organitzatiu necessàries que garantissin la seguretat de les dades de caràcter personal i n'evités l'alteració, la pèrdua, el tractament o l'accés no autoritzat, i més concretament mesures de nivell bàsic, d'acord amb el que preveu l'esmentat article 32.1 de l'RGPD i el contracte que estipulava les obligacions d'Indra.

I no resulta tampoc admissible el seu argument que el sistema es trobava en un entorn de proves, i que va ser el responsable o l'encarregat de tractament, però en cap cas Indra, qui va ordenar que entrés en producció. I això perquè es tractava d'un entorn de proves dut a terme per Indra amb dades reals d'usuaris que estaven exposades a internet (portal extranet), i les proves de software amb dades personals constitueixen igualment un

tractament subjecte a les obligacions que estableix l'RGPD i, evidentment, també les establertes a l'article 32.1 de l'RGPD pel que fa a la seguretat de les dades.

En resum, Indra tenia el deure de complir amb les obligacions de seguretat estipulades en el contracte subscrit amb SocMobilitat i actuar amb la diligència necessària per tal que la seguretat de les dades personals no es veiés compromesa, garantint que només accedien a les dades tractades les persones autoritzades, el que l'obligava a establir un mecanisme que permetés la identificació de forma inequívoca i personalitzada de qualsevol usuari que intentés accedir al sistema d'informació, circumstàncies que no es complien en el present cas, en què, ja fos per descuit o per "un error operatiu", com es deia als Tuits publicats per T-Mobilitat al seu canal en dates 05/10/2021 i 06/10/2021 (antecedent 1r), no es va modificar la contrasenya de caràcter públic que per defecte assigna el fabricant a l'administrador, en la fase de proves de la implementació de la targeta de la T-mobilitat, el que va comportar una porta oberta a la informació que contenia la plataforma.

Al respecte cal fer referència a la doctrina jurisprudencial que sosté que no es requereix una conducta dolosa de l'infractor, sinó que és suficient "la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..." (Sentència de l'Audiència Nacional de 12/11/2010, recurs n. 761/2009).

En la mateixa línia es pronuncia el Tribunal Suprem, entre d'altres, en la sentència de 25/01/2006, dictada també en l'àmbit de protecció de dades, quan afirma que "el principio de culpabilidad consiste en la falta de diligencia observada por la entidad recurrente al tratar de forma automatizada un dato relativo a la ideología del denunciante, resultando irrelevantes las invocaciones que se hacen (...) acerca de la ausencia de intencionalidad o a la existencia del error, y ello por cuanto el elemento culpabilístico del tipo sancionador aplicado concurre cuando se incluye el expresado dato sobre la ideología, no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado".

En definitiva, per tal de determinar la concurrència de l'element culpabilístic no és necessari que els fets infractors s'hagin produït amb dol o intencionalitat, sinó que és suficient que hagi intervingut negligència o una manca de diligència en el compliment de les obligacions que li són exigibles legalment, com seria el supòsit aquí analitzat, en què ni tan sols va implementar mesures de seguretat de nivell bàsic que li havien estat concretament exigides per via contractual. I, val a dir, aquest deure de diligència és màxim quan es fan activitats que afecten drets fonamentals, com és el dret a la protecció de dades de caràcter personal.

Així ho ha declarat la Sentència de l'Audiència Nacional de 05/02/2014 (recurs n. 366/2012) dictada en matèria de protecció de dades, que sosté que la condició de responsable de tractament de dades personals "impone un deber especial de diligencia a la hora de llevar a cabo el uso o tratamiento de los datos personales o su cesión a terceros, en lo que atañe 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 el present cas, la manca de diligència és evident davant el fet indiscutit que es va deixar configurat l'accés al portal web amb la contrasenya que ve per defecte del fabricant quan s'estaven tractant dades d'usuaris reals, el que constitueix un clar incompliment de les seves obligacions pel que fa a les mesures de seguretat que tenia el deure d'implementar, i que és

imputable a Indra, tot i que derivi d'un error humà d'un treballador, d'acord amb el sistema de responsabilitat previst a l'RGPD, i particularment a l'article 70 de l'LOPDGDD, en què s'estableix que la responsabilitat per les infraccions a la normativa de protecció de dades recau, entre d'altres, sobre els responsables, o en el seu cas, sobre els encarregats dels tractaments, i no sobre el seu personal.

En conclusió, en el present cas és clara la concurrència de l'element culpabilístic en la conducta d'Indra, exigit per la normativa i la jurisprudència per poder -li exigir responsabilitats en la comissió de la infracció imputada en el present procediment sancionador, atesa la seva manca de diligència en el compliment de les obligacions que li eren exigibles.

2.4 Sobre l'adopció de mesures immediates.

Al respecte, Indra esgrimeix que un cop va tenir coneixement de la vulnerabilitat, que va ser publicada a les 15:39 h del mateix dia 05/10/2021 a les xarxes socials, va procedir de manera immediata a solucionar l'incident.

En aquest sentit, Indra posa de manifest que en tant sols 61 minuts des què es va tenir coneixement de la fuita de dades, va bloquejar "qualsevol accés per part de tercers no autoritzats", i va dur a terme les següents accions sobre la infraestructura de tecnologia Liferay del portal T-mobilitat, per tal de mitigar les possibles conseqüències adverses per a les persones afectades, i eliminar els riscs de nous accessos, i en concret:

• Es va deixar només un usuari administrador i se li va canviar la contrasenya.
• Es va desconnectar la possibilitat nativa d'entrar a "Liferay".
• Es va realitzar una auditoria d'anàlisis de gestió de continguts de "Liferay", per verificar el total de continguts del portal i ordenar-los per data de modificació. "*De esta manera se pudo certificar que durante el período de tiempo en las que se accedió al portal como administrador hasta que se mitigó la incidiencia, no se realizó ninguna modificación sobre ningun contenido.*

Sobre això, cal posar de manifest que les actuacions dutes a terme per part d'Indra de manera immediata i tan bon punt va tenir coneixement de l'incident, no permeten desvirtuar la infracció que se li imputa per la vulneració de la seguretat de les dades, si bé es tenen en compte com a circumstància atenuant en la quantificació de la sanció, d'acord amb l'anàlisi que es realitza en el fonament de dret 5è d'aquesta resolució, i despleguen efectes quant el fet que en el present procediment no s'hagi d'exigir l'adopció de mesures correctores per corregir els efectes de la infracció comesa.

2.5 Sobre la manca de danys i perjudicis.

A l'últim, en l'apartat de conclusions, i com a darrera al·legació per tal de justificar la seva sol·licitud de sobreseïment del procediment, Indra esgrimeix que l'incident de seguretat que es va produir no hauria tingut conseqüències negatives per a les persones afectades, és a dir que no s'haurien generat danys i perjudicis.

Al respecte, cal dir que entre els elements objectius que conformen el tipus infractor previst a l'article 83.4.a) de l'RGPD no s'inclou la necessitat que la persona titular de les dades, en relació a les quals s'ha produït la infracció, consideri vulnerada la seva privacitat o intimitat.

El tipus només requereix, com s'ha dit, la falta d'adopció de les mesures tècniques i organitzatives per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32.1 de l'RGPD.

En tot cas, cal recordar que en el present expedient sancionador consten fins a set denúncies de persones que han entès vulnerada la privacitat de les seves dades arran la infracció imputable a Indra.

Per tot el que s'ha exposat fins aquí, no poden reeixir les al·legacions formulades per l'entitat imputada a la proposta de resolució.

3. En relació amb la conducta descrita a l'apartat de fets provats, relativa a la manca d'aplicació de les mesures de seguretat de nivell bàsic exigides per garantir un nivell de seguretat adequat al risc, cal acudir, com s'ha dit, a l'article 32.1 de l'RGPD, el qual disposa que:

"1. 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, 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 los 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."

Com s'ha dit també, respecte la conducta descrita als fets provats, es considera que Indra ha vulnerat mesures de seguretat,de nivell bàsic, de l'Esquema Nacional de Seguretat (ENS) aprovat pel Reial Decret 3/2010, i aplicable a Indra, d'acord amb la disposició addicional primera de l'LOPDGDD (Mesures de seguretat en l'àmbit del sector públic), per raó del contracte d'encàrrec signat amb SocMobilitat, que li van ser exigides en dit contracte. I en concret es van vulnerar les mesures que es detallen a continuació:

1. L'apartat 4.1.2 *"Arquitectura de Seguridad"* de l'Annex II ("Mesures de Seguretat") de l'ENS, determina el següent:

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:
Categoría BÁSICA
a) (…)
d) Sistema de identificación y autenticación de usuarios:

1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
(...)

2. L'apartat 4.2 relatiu al control d'accés, determina el següent:

"El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.

En todo control de acceso se requerirá lo siguiente:
a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].
c) Que la utilización de los recursos esté protegida [op.acc.2].
d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
f) Que la identidad de la entidad quede suficientemente autenticada [op.acc.5].
g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext])."

3. I a l'últim, l'apartat 4.3.2 relatiu a la "Configuración de Seguridad", que determina el següent:

"Se configurarán los equipos previamente a su entrada en operación, de forma que:
a) Se retiren cuentas y contraseñas estándar.
b) Se aplicará la regla de "mínima funcionalidad": (…)"

Així doncs, en el cas que ens ocupa ha quedat acreditat que el sotsencarregat del tractament, Indra, no va aplicar mesures tècniques de nivell bàsic, exigides per SocMobilitat per garantir un nivell de seguretat adequat al risc (tendents a evitar que a aquestes dades hi poguessin accedir persones no autoritzades), atès que en configurar el control d'accés al portal web de la T- Mobilitat, no es va modificar la contrasenya que per defecte assigna el fabricant de la infraestructura de tecnologia "Liferay" a l'administrador, de tal manera que l'accés quedava obert, i al seu torn, accessible a tercers.

Aquest fet recollit a l'apartat de fets provats constitueix la infracció prevista a l'article 83.4.a) de l'RGPD, que tipifica com a tal la vulneració de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"*, entre les quals hi ha la prevista a l'article 32.1 de l'RGPD.

Dit això, la conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.f) de l'LOPDGDD, en la forma següent:

"f) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32.1 del Reglament (UE) 2016/679."

4. En el contracte d'encarregat del tractament subscrit entre SocMobilitat i Indra, com s'ha dit també, s'estipulava, que Indra havia d'adoptar les mesures de nivell bàsic de l'ENS per garantir un nivell de seguretat adequat al risc, i així es feia constar el següent:

"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 ajusten 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 los 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 los 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 auditorias periódicas que se realicen, puede ser solo solicitada en cualquir momento por el responsable del Tratamiento."

A aquest respecte, l'apartat desè de l'article 28 de l'RGPD, disposa el següent:

" 10. Sens perjudici del que disposen els articles 82, 83 i 84, si un encarregat del tractament infringeix el present Reglament en determinar els fins i els mitjans del tractament, se l'ha de considerar responsable del tractament pel que fa a dit tractament."

Això és també aplicable al sotsencarregat del tractament, d'acord amb el que disposa l'article 28.4 de l'RGPD i 70.1.b) LOPDGDD (que es considera, en tot cas, un encarregat de l'encarregat del tractament), i, per tant, és també responsable, davant l'autoritat de control, de les presumptes vulneracions de la normativa de protecció de dades que pugui cometre en el desenvolupament de l'encàrrec (prestacions tècniques encomanades), i en concret de la manca d'aplicació de les mesures de nivell bàsic exigides al mateix encàrrec, en la configuració del portal d'accés a la T-Mobilitat, sense que calgui requerir, com s'ha dit, l'adopció de cap mesura correctora, ja que Indra ha acreditat haver pres les mesures adequades per solucionar l'incident de seguretat detectat en la plataforma.

5. En no encabir-se l'entitat Indra Sistemas SA, en cap dels subjectes previstos a l'article 77.1 de l'LODGDD, resulta d'aplicació el règim sancionador general previst a l'article 83 de l'RGPD.

L'article 83.4 de l'RGPD preveu per a les infraccions allà previstes, se sancionin amb una multa administrativa de 10.000.000 d'euros com a màxim, o tractant-se d'una empresa, d'una quantia equivalent al 2 % com a màxim del volum de negoci total anual global de l'exercici financer anterior, optant-se per la de major quantia.

Dit això, correspon determinar la quantia de la multa administrativa que escau imposar. Segons el que estableix l'article 83.2 de l'RGPD, i també de conformitat amb el principi de proporcionalitat consagrat a l'article 29 de la Llei 40/2015, correspon imposar la sanció de 23.500 euros (vint-i-tres mil cinc-cents euros). Aquesta quantificació de la multa, en un import minorat respecte el proposat per la instructora del procediment, després de considerar que no concorre una de les circumstàncies agreujants contemplades en la proposta de resolució, es basa en la ponderació dels criteris agreujants i atenuants que a continuació s'indiquen:

Com a criteris atenuants, s'observa la concurrència de les causes següents:

- La naturalesa, gravetat i duració de la infracció (art.83.2.a).

- Haver dut a terme mesures immediates per corregir els efectes de la infracció.

- La manca d'intencionalitat (art.83.2.b) RGPD).

- La manca de constància de l'obtenció de beneficis com a conseqüència de la infracció (art. 83. 2. k) RGPD i 76.2.c) LOPDGDD).

No resulten d'aplicació altres criteris atenuants invocats per Indra en la seva al·legació cinquena, en concret l'atenuant prevista a l'article 83.2.g) de l'RGPD, i la prevista a l'art.76.2.d) de l'LOPDGDD, en tant que, pel que fa al primer, la naturalesa de dades afectades ja s'ha tingut en compte a l'hora d'aplicar l'atenuant prevista a l'art.83.2.a) de l'RGPD, i que, pel que fa al segon, l'actuació d'un tercer no ha tingut cap incidència en la comissió de la infracció que aquí s'imputa, com ja s'ha dit de manera reiterada.

Per altra banda, com a criteri agreujant, cal tenir en compte el següent element:

- La vinculació de l'activitat d'Indra amb la realització de tractaments de dades personals, al tenir com a activitat principal la prestació de serveis de consultoria en diferents àmbits, que implica el tractament de dades personals en les operacions i projectes que executa per als seus clients (com consta al web https://www.indracompany.com/es/indra/privacidad-proteccion-datos).

Nogensmenys, no resulta d'aplicació el criteri agreujant contemplat a la proposta de resolució referent a l'article 83.2.e) de l'RGPD, en tant que ha quedat acreditat que l'entitat sancionada amb anterioritat, era Indra BMB Servicios Digitales S.L, que té personalitat jurídica independent de l'entitat aquí imputada, el que ha de comportar la reducció de la quantia de la sanció proposada per la persona instructora.

Per tot això, resolc:

1. Imposar a Indra Sistemas, SA la sanció consistent en una multa de 23.500.- euros (vint-i-tres mil cinc-cents euros), com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32.1, ambdós de l'RGPD, sense que calgui requerir mesures correctores d'acord amb el que s'ha exposat al fonament de dret quart.

2. Notificar aquesta resolució a Indra Sistemas, SA.

3. Ordenar que es publiqui aquesta resolució al web de l'Autoritat (apdcat.gencat.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de l'LPAC. També pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Si l'entitat imputada manifesta a l'Autoritat la seva intenció d'interposar un recurs contenciós administratiu contra la resolució ferma en via administrativa, la resolució se suspendrà cautelarment en els termes previstos a l'article 90.3 de l'LPAC.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.