Identificació de l'expedient

Resolució del procediment sancionador núm. PS 38/2022, referent al Centre de Telecomunicacions i Tecnologies de la Informació

Antecedents

1. En data 25/11/2020, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava denúncia contra l'Institut Obert de Catalunya (en endavant, l'IOC), que és l'institut d'ensenyament a distància del Departament d'Educació, amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la persona denunciant, exposava que en data 24/11/2020, quan realitzava el tràmit de preinscripció telemàtica a l'IOC, va refrescar la pàgina web i "*van aparèixer les dades personals d'una altra persona que no conec: el seu nom i cognoms, el seu telèfon, la seva adreça, la seva data de naixement, el seu DNI i el seu e-mail*". La persona denunciant va aportar documentació sobre els fets denunciats, en concret, una imatge de la pantalla de l'ordinador en el moment en què li va aparèixer la informació relativa a *"Dades de l'alumne"* corresponent a una tercera persona.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 361/2020), 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.

3. En aquesta fase d'informació, en data 18/12/2020 es va requerir l'entitat denunciada perquè informés sobre els motius que el dia 24/11/2020, quan la persona aquí denunciant tramitava la preinscripció telemàtica a l'IOC, li aparegués en pantalla les dades personals d'un altre usuari, i, també, sobre les mesures de seguretat implementades per l'entitat per protegir la confidencialitat de les dades personals dels alumnes que realitzin la preinscripció via telemàtica, per evitar l'accés de tercers a aquestes dades personals.

4. En data 04/01/2021, el Departament d'Educació va respondre el requeriment esmentat a través d'escrit en què exposava, entre d'altres, el següent:

- Que *"El dia 25 de novembre de 2020, la delegada de protecció de dades del Departament rep una comunicació de la direcció de l'IOC on se li informa que durant el matí (del mateix dia 25 de novembre) havien tingut constància de l'existència de dos incidents relacionats amb les dades que tractaven dels futurs alumnes en la Secretaria virtual*."

- Que "*Davant d'aquesta possible violació de seguretat i com a responsables del tractament de les dades afectades, el director del centre havia realitzat les següents actuacions:*
  a) Va indicar als alumnes que s'estava gestionant la queixa, i que s' els informaria de la resolució de la incidència quan estigués solucionada.
  b) Va notificar la incidència i sol·licitar ***al Gestor de solucions al Departament d'Educació del CTTI que donés instruccions immediates de bloquejar l'accés a***

la Secretaria *on s'havien detectat les incidències. Ho van notificar també a la Subdirecció general d'Administració i Organització de Centres Públics.*
c) Va recollir evidències i informació relativa a l'abast de la incidència (nombre d'alumnes, tipus de dades a què s'havia accedit,...).
d) Va ***requerir al Gestor de solucions al Departament d'Educació del CTTI perquè es gestionés la resolució de la incidència*** *al més aviat possible i els confirmés, que estava solucionada i es podia novament reobrir la Secretaria virtual en condicions segures. (...).*

- Que l'entitat va realitzar una sèrie d'actuacions d'investigació sobre els fets denunciats, *"segons el Procediment proposat per l'AEPD en la Guía para la gestión y notificación de brechas de seguridad",* del resultat de les quals va concloure que no era necessari notificar la violació de seguretat a l'autoritat de control.

- Que "*El mateix dia 25 de novembre a la tarda, el CTTI va comunicar que ja havia trobat la incidència dins l'aplicació, que també s'havia revisat la base de dades per veure quants casos podrien estar afectats i que només tenien un (el de referència) i ja s'havia solucionat. Així mateix, es va preparar un paquet de desplegament de l'aplicació per tal que quedés corregida l'errada i no es pogués produir cap més vegada amb la previsió que tot estaria pujat a l'endemà a primera hora."*

- Que "*El dia 26 de novembre, la delegada de protecció de dades del Departament rep del CTTI l'explicació tècnica detallada del problema que ja havia quedat resolt: el 24/11/2020, l'alumne AAA AAA AAA es va donar d'alta dues vegades de la matrícula, una, amb un DNI X i els seu nom i cognoms i una altra amb un DNI Y i els seu nom i cognoms. Atès que el DNI és l'identificador únic per la creació de fitxa, tots dos registres es van crear. Lligat a la matrícula, hi ha el procés de creació del username (que també ha de ser únic), i que es fa amb la combinació de nom i cognom. En el primer cas es crea el username correcte, però en el segon, com ja existeix, el sistema dona un error generant un username buit (" "). Per un altre costat, l'estudiant BBB BBB BBB es registra per la matrícula correctament i consulta l'estat de la seva matrícula. Mentrestant, fa altres activitats, de manera que li salta el time out de la pàgina. El problema en aquest cas és que en comptes de fer fora a l'estudiant de la seva sessió, com fan altres pàgines de la Secretaria (com ara la d'itineraris), la variable de username deixa de tenir valor, és a dir passa a ser buit. Al tenir aquest username buit, quan l'usuari refresca la pàgina, es genera una incongruència entre el valor de la variable i el registre buit inserit en la doble matrícula anterior (de l'AAA AAA AAA) i recupera les dades d'una altre alumne (de forma aleatòria), que ha estat les de la CCC CCC CCC. D'aquí que l'alumna BBB BBB BBB pogués veure les dades de l'alumna CCC CCC CCC.*"

- Que "*Per resoldre la incidència es van realitzar les següents accions:*
Es va eliminar el valor buit de la base de dades per tal que no es pogués reproduir la situació.
Es va modificar el codi font de l'aplicació a fi que, a part de controlar que no es generessin usernames amb valor nul, tampoc es poguessin generar amb valor " "). Aquesta modificació va dur-se a terme durant el mateix matí del dia 26 de novembre, deixant el problema definitivament resolt."

- L'entitat tanca les al·legacions amb la conclusió següent:
"*CONCLUSIÓ:*

La causa de la violació de seguretat no va provenir directament de l'IOC sinó del seu proveïdor informàtic: el CTTI, que va tenir un problema tècnic que va causar la fallada de seguretat.
La solució també va venir del proveïdor informàtic que va detectar la causa tècnica i va posar-hi la solució en un termini molt breu .
L'IOC va limitar-se a traslladar d'immediat la incidència al proveïdor informàtic, el CTTI i al Departament d'Educació, en va informar la delegada de protecció de dades, a més de prendre les mesures de prevenció oportunes (bloquejar l'accés a la Secretaria virtual) per impedir que es produïssin de noves mentre se cercava la solució, i, finalment, es va excusar davant de la persona denunciant en nom propi i del Departament."

5. En data 22/03/2022, arran de la resposta de l'IOC del Departament d'Educació en la qual assenyalava al Centre de Telecomunicacions i Tecnologies de la Informació (en endavant CTTI) com a possible responsable dels fets, es va considerar necessari requerir informació al CTTI, perquè informés, entre d'altres, sobre el següent:

- si la bretxa de seguretat patida, que hauria propiciat que una persona en el moment de la preinscripció telemàtica a l'IOC pogués, a través de la web, accedir a les dades vinculades a tercers, s'hauria produït en el marc d'un encàrrec encomanat al CTTI, i en tal cas, aportés la documentació acreditativa d'aquesta circumstància (contracte d'encarregat subscrit amb l'IOC).
- els motius que explicarien que el dia 24/11/2020, quan la persona aquí denunciant tramitava la preinscripció telemàtica a l'IOC, li aparegués en pantalla les dades personals d'un altre usuari.
- sobre les mesures de seguretat implementades pel CTTI en l'aplicació desenvolupada per realitzar les preinscripcions telemàtiques a l'IOC, per evitar l'accés de tercers a aquestes dades personals.

6. En data 26/04/2022, atès que s'havia superat en escreix el termini concedit sense que el CTTI aportés la informació requerida, es reitera el requeriment al CTTI i es concedeix un nou termini de 5 dies per donar-hi resposta, amb l'advertiment exprés que si no es compleix es podria incórrer en una infracció de la normativa sobre protecció de dades de caràcter personal.

7. En data 02/05/2022, el CTTI va donar compliment a aquest requeriment per mitjà d'escrit a través del qual manifestava, entre d'altres, el següent:

- Que "*la bretxa de seguretat patida s'hauria produït dins del marc de la prestació dels serveis TIC que el CTTI realitza a la Generalitat de Catalunya i el seu Sector Públic. En concret, en el marc de l'encàrrec que el Departament d'Educació encomana al CTTI, ja que l'IOC depèn d'aquest, més concretament, penja de la Direcció General de Centres Públics. Per aquest motiu us adjuntem l'acord d'encàrrec de tractament de dades de caràcter personal vigent entre el CTTI i el Departament d'Educació*."

- Que "*arrel d'una amenaça en el control de tancament de sessió de l'aplicatiu, heretada en el codi de l'aplicatiu de l'anterior proveïdor d'aplicacions del CTTI degut a l'obsolescència de versions en el codi de l'aplicació, es va detectar una falta de control de la mateixa pel que fa a la fitxa de dades personals dels alumnes. Aquest fet provocava que quan un alumne perdia la sessió, degut a haver transcorregut un temps superior a deu minuts, l'aplicatiu no el redirigia a la plana de sessió caducada en la qual havia de tornar a iniciar*

sessió, en comptes d'això, l'alumne quedava a la fitxa de dades personals i el codi de l'aplicatiu carregava les dades del següent alumne del filtre de cerca d'aquests estudis."

- Que "*sobre les mesures de seguretat implementades, es va crear una nova funció en l'aplicatiu que controla el temps de sessió de cada alumne que entra a la fitxa de dades personals, amb un temps màxim de 600 segons (10 minuts), la qual en cas d'exhaurir el temps indicat, redirigeix als alumnes a la plana de sessió expirada de la secretaria de l'IOC."*

- Que "*arrel d'aquest fet, es va realitzar un anàlisi en tots els estudis que poguessin patir aquesta mancança en el control de sessions, per tal d'aplicar els mateixos canvis a les fitxes de dades i altres parts de l'aplicatiu on es tracten dades de caràcter personal i sensible. Finalment, només va ser necessari aplicar-ho en la fitxa dels estudis reportats.*

  Finalment, indicar que tant l'Agència de Ciberseguretat com el CTTI actuen proactivament mitjançant un pla de mitigació de riscos al respecte de la obsolescència tecnològica."

El CTTI va aportar juntament amb el seu escrit de resposta, còpia del document "*Acord d'encàrrec de tractament de dades de caràcter personal entre l'Administració de la Generalitat, mitjançant el Departament d'Ensenyament i el Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya"*, formalitzat en data 30/03/2016.

En el dit Acord, s'establia a la clàusula primera que l'objecte de l'encàrrec de tractament era el següent:

"*Mitjançant aquest acord d'encàrrec s'habilita al CTTI, en qualitat d'encarregat del tractament (en endavant, encarregat), per tractar, per compte del responsable del tractament (d'ara endavant, responsable) les dades de caràcter persona necessàries per a la gestió centralitzada, transversal i coordinada de les solucions TIC de conformitat amb l'Acord de Govern de 18 d'octubre de 2011*".

Així mateix, a la clàusula tercera, relativa a les obligacions de l'encarregat del tractament, s'establia, entre d'altres obligacions, el següent:

"i) Complir amb les mesures de seguretat que corresponen al nivell de seguretat que el responsable ha declarat en l'annex I d'aquest encàrrec, segons el que estableix la LOPD i el RLOPD i, d'acord amb les especificacions següents:
(...)
i.7) A banda d'aquestes especificacions, l'encarregat ha d'implantar el conjunt de mesures previstes per al nivell de seguretat alt en el títol VIII del Reglament de la Llei orgànica de protecció de dades de caràcter personal, aprovat pel Reia decret 1720/2007, de 21 de desembre."

A l'annex I d'aquest Acord d'encàrrec, on es relacionen els fitxers i nivells de protecció objecte de l'encàrrec de tractament, s'estableix un nivell de seguretat alt pels fitxers relatius als alumnes dels quals en sigui responsable del fitxer la Direcció de l'IOC.

8.En data 07/06/2022, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra el Centre de Telecomunicacions i Tecnologies de la Informació per una presumpta infracció prevista a l'article 83.4.a), en relació a l'article 32.1.b); tots ells 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). Aquest acord d'iniciació es va notificar a l'entitat imputada en data 09/06/2022.

9. En data 20/06/2022, el CTTI va formular al·legacions a l'acord d'iniciació, i va aportar una còpia del document "Informe incidència del servei", de data 15/06/2022.

10. En data 23/09/2022, la persona 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 amonestés al Centre de Telecomunicacions i Tecnologies de la Informació com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32.1, ambdós de l'RGPD.

Aquesta proposta de resolució es va notificar en data 23/09/2022 i es concedia un termini de 10 dies per formular al·legacions.

11. El termini s'ha superat amb escreix i no s'han presentat al·legacions.

Fets provats

El Departament d'Educació (responsable del tractament), en virtut de l'Acord d'encàrrec formalitzat en data 30/03/2016, va encarregar al CTTI (encarregat del tractament) tractar per compte del responsable del tractament, les dades personals necessàries per a la gestió centralitzada, transversal i coordinada de les solucions TIC.

En aquest Acord, el Departament d'Educació establia que el CTTI havia d'implementar les mesures de seguretat previstes a l'annex I de l'acord, per cadascun dels fitxers allà detallats. En el cas dels alumnes de l'IOC es preveia que el CTTI havia d'implementar les mesures de seguretat per al nivell alt, de conformitat amb el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, RLOPD i LOPD, respectivament)

El CTTI no va adoptar les mesures de seguretat adequades per garantir els alumnes de l'IOC no poguessin accedir a dades personals d'altres persones alumnes. En concret, en data 24/11/2020, mentre la persona denunciant realitzava la preinscripció telemàtica a una formació oferta per l'IOC, li va aparèixer en pantalla les dades personals relatives a un altre alumne.

Fonaments de dret

1. Són d'aplicació a aquest procediment el que preveuen l'LPAC, i l'article 15 del Decret 278/1993, segons el que preveu la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la

resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.

2. L'entitat imputada no ha formulat al·legacions a la proposta de resolució, però sí que ho va fer a l'acord d'iniciació. Respecte d'això, es considera oportú reiterar a continuació el més rellevant de la resposta motivada de la persona instructora a aquestes al·legacions.

Al respecte, cal dir que al·legacions que es van formular a l'acord d'iniciació no són al·legacions en sí mateixes tendents a qüestionar o desvirtuar la realitat dels fets que van motivar la incoació del procediment, ni la seva qualificació jurídica, sinó que se centraven, principalment, a exposar la mesura correctora implementada per l'entitat per tal de garantir que fets com els aquí provats no tornin a succeir.

En aquest sentit, l'entitat, per una banda, reconeix de forma literal "*la seva responsabilitat respecte els fets imputats com a encarregat del tractament de les dades de caràcter personal de l'IOC relacionades en l'Annex 1 de l'Acord d'encàrrec de tractament signat entre el CTTI i el Departament d'Educació en data 30 de març de 2016",* i de l'altra, aporta el document "*Informe incidència del servei*", on es recull la cronologia dels fets, les actuacions dutes a terme i les accions correctives i millores implementades per tal de garantir que l'incident de seguretat no es torni a repetir, i que els alumnes de l'IOC no puguin accedir telemàticament a dades personals d'altres alumnes. També, informa que, arran dels fets denunciats, l'entitat va realitzar un anàlisi de la resta d'aplicacions del sistema susceptibles de poder patir el mateix incident de seguretat, i el resultat final va ser que en cap dels casos es repetia la vulnerabilitat de seguretat que hauria propiciat que succeïssin els fets aquí provats. A l'últim, el CTTI informa, que amb l'Agència de Ciberseguretat actuen proactivament mitjançant un pla de mitigació de riscos envers l'obsolescència tecnològica, i també, sobre l'aprovació durant el primer trimestre del 2021 del "*Primer Programa de Seguretat del Departament d'Educació*", on s'estableix la creació d'un comitè de seguretat per poder realitzar un seguiment molt més acurat dels riscos existents en la ciberseguretat.

A aquest respecte, cal assenyalar que, aquesta Autoritat valora positivament les diferents mesures implementades per l'entitat, però cal assenyalar que l'adopció d'aquestes mesures no desvirtuen la realitat dels fets imputats ni la correcció de la seva qualificació jurídica.

3. En relació amb els fets descrits a l'apartat de fets provats, cal acudir a l'article 5.1.f) de l'RGPD, que regula el principi d'integritat i de confidencialitat determinant que les dades personals seran *"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)".*

Per la seva banda, l'article 32.1 de l'RGPD, referent a la seguretat de les dades, disposa que *"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".

En aquest cas, en l'Acord d'encàrrec del tractament de data 30/03/2016, el responsable del tractament establia que les mesures de seguretat aplicables als fitxers relatius als alumnes de l'IOC havien de ser mesures de seguretat de nivell alt de conformitat amb l'RLOPD.

A aquest respecte, cal tenir en compte que en la data dels fets denunciats, el contingut de l'Acord d'encàrrec del tractament de data 30/03/2016 era totalment vigent, atès que segons disposa la disposició transitòria cinquena de la LOPDGDD, els contractes d'encarregat del tractament subscrits abans del 25/05/2018 a l'empara del que disposa l'article 12 de la LOPD, mantenien la seva vigència fins a la data de venciment que assenyalin i en cas que s'hagi pactat de manera indefinida, fins al 25/05/2022.

Així les coses, i atès que la vigència del referenciat Acord d'encàrrec està vinculada a l'encara vigent Acord de Govern de 18/10/2011, i, que no consta que cap de les dues parts hagin instat la modificació de l'Acord d'encàrrec per adequar-lo al que disposa l'article 28 de l'RGPD, cal considerar que el dit Acord d'encàrrec va continuar vigent fins el dia 25/05/2022, sense que li fos exigible adequar el seu contingut a l'article 28 de l'RGPD.

No obstant això, cal indicar que, amb independència de la vigència del referenciat Acord d'encàrrec, a partir de l'entrada en vigor de l'RGPD (25/05/2018), sí que havien de ser aplicades les mesures de seguretat derivades de l'RGPD. És a dir, aquelles mesures de seguretat les quals, arran d'una prèvia valoració de riscos (art. 32 de l'RGPD), es consideressin apropiades per garantir un nivell de seguretat adequat al risc.

Per tant, el CTTI havia d'implementar, en relació amb el tractament de les dades personals dels alumnes de l'IOC, les mesures de seguretat de nivell alt que comportava el seu tractament.

A aquest respecte, cal tenir en compte que la disposició addicional primera de l'LOPDGDD estableix el següent: "*L'Esquema Nacional de Seguretat ha d'incloure les mesures que s'hagin d'implantar en cas de tractament de dades personals per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, amb l'adaptació dels criteris de determinació del risc en el tractament de les dades al que estableix l'article 32 del Reglament (UE) 2016/679*".

Doncs bé, respecte la conducta descrita a l'apartat de fets provats, s'infereix que l'entitat imputada va vulnerar la mesura de seguretat prevista a l'article 16 de l'Esquema Nacional de Seguretat vigent en aquell moment (RD 3/2010, de 8 de gener), precepte que regula l'autorització i el control dels accessos en els següents termes: "*L'accés al sistema d'informació ha de ser controlat i limitat als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, restringint l'accés a les funcions permeses*."

En aquest sentit, cal indicar que quan es va formalitzar l'Acord d'encàrrec entre el Departament d'EDU i el CTTI (2016), el compliment de les mesures de seguretat relatives a l'autorització i al control d'accessos ja es recollia a l'Annex I del dit Acord d'encàrrec. Això és

així perquè a l'Annex I, ja s'establia que, en relació amb el tractament de les dades personals dels alumnes de l'IOC, s'havien d'implementar les mesures de seguretat de nivell alt. Al respecte, cal indicar que, en aquell moment, el compliment de les mesures de seguretat de nivell alt comportava de forma acumulativa el compliment de les mesures de seguretat de nivell bàsic i mig. Per tant, es considerava inclòs el compliment de les mesures de seguretat relatives al control d'accessos i la identificació i autenticació, previstes com a mesures de seguretat de nivell bàsic als articles 91 i 93 del RLOPD, respectivament.

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit a l'apartat de fets provats, que és constitutiu de 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"*, entre les quals es troba la recollida a l'article 32 .1.b de l'RGPD a dalt transcrit, referent a la seguretat del tractament que garanteixi la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis del tractament.

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:

"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 del Reglament (UE) 2016/679"

4. En tractar-se el CTTI d'una entitat de dret públic adscrita a la Secretaria de Polítiques Digitals del Departament de Territori, li resulta d'aplicació el règim previst a l'article 77 LOPDGDD per a determinades categories de responsables o encarregats del tractament, entre aquests, les entitats de dret públic vinculades o dependents de les administracions públiques.

En aquest sentit, l'article 77.2 LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'art. 77.1 LOPDGDD, l'autoritat de protecció de dades competent:

> *"(...) ha de dictar una resolució que les sancioni amb una amonestació. La resolució ha d'establir així mateix les mesures que escaigui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès.*
> *La resolució s'ha de notificar al responsable o encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si s'escau, i als afectats que tinguin la condició d'interessat, si s'escau."*

En termes similars a l'LOPDGDD, l'article 21.2 de la Llei 32/2010, determina el següent:

> *"2. En el cas d'infraccions comeses amb relació a fitxers de titularitat pública, el director o directora de l'Autoritat Catalana de Protecció de Dades ha de dictar una resolució que declari la infracció i estableixi les mesures a adoptar per a corregir-ne els efectes. A més, pot proposar, si escau, la iniciació d'actuacions disciplinàries d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. Aquesta resolució s'ha de notificar a la persona responsable del*

fitxer o del tractament, a l'encarregada del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha".

En el present cas, esdevé innecessari requerir mesures correctores dels efectes de la infracció atès que les mesures adoptades pel CTTI es consideren suficients i adequades per tal de garantir que en un futur es repeteixin fets similars als aquí provats.

Per tot això, resolc:

1. Amonestar al Centre de Telecomunicacions i Tecnologies de la Informació com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32.1, ambdós de l'RGPD.

No cal requerir mesures correctores per corregir els efectes de la infracció, de conformitat amb el que s'ha exposat al fonament de dret 4rt.

2. Notificar aquesta resolució al Centre de Telecomunicacions i Tecnologies de la Informació.

3. Comunicar la resolució al Síndic de Greuges, de conformitat amb el que preveu l'article 77.5 de l'LOPDGDD.

4. 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.

La directora,