Identificació de l'expedient

Resolució del procediment sancionador núm. PS 69/2023, referent a l'Ajuntament de Girona.

Antecedents

1. En data 24/02/2023, va tenir entrada a l'Autoritat Catalana de Protecció de Dades una denúncia contra l'Ajuntament de Girona (d'ara endavant, l'Ajuntament), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, el denunciant (Sr. (...)) hi exposava que, en data 18/07/2022, va accedir amb el seu certificat electrònic a la carpeta ciutadana d'una altra persona (Sr. (...)), en la qual es visualitzaven diverses dades relatives a aquesta persona.

El denunciant acompanyava l'escrit de denúncia amb la documentació següent, entre d'altra:

— Captura de pantalla de la carpeta ciutadana de la seu electrònica de l'Ajuntament de Girona, de data 20/07/2022, a les 10:35:11 hores. Aquest document conté les dades següents: usuari connectat: (cognoms i nom d'una persona diferent del denunciant); data últim accés: 18/07/2022 17:38; expedients en tràmit: 7; documents: 0; adreça padró: (carrer, número, pis i porta).

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 108/2023), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador, d'acord amb el que preveuen 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 (LPAC).

En aquesta fase d'informació, en data 13/06/2023 es va requerir l'entitat denunciada perquè, entre d'altres qüestions, respongués les següents:

— Informés sobre la vulnerabilitat detectada per la persona denunciant a la seu electrònica de l'Ajuntament, les circumstàncies que l'haurien propiciat i si ja s'havia esmenat.

— Assenyalés quines accions havia dut a terme per garantir que la carpeta ciutadana estigui correctament vinculada al certificat electrònic de cada persona usuària.

3. En data 22/06/2023, l'Ajuntament va respondre el requeriment amb un escrit en què exposava:

— Que "s'ha identificat que tant la persona denunciant com la persona amb les dades presumptament compromeses van iniciar sessió [a la seu electrònica de l'Ajuntament] al mateix moment, hora, minut i segon (...)."

— Que "Tot i que els identificadors de sessió per a cadascun dels usuaris era diferent, des del Servei de Sistemes i Tecnologies de la Informació [de l'Ajuntament] es dedueix que el problema podria haver-se produït pel fet de la connexió simultània i

que el servei WAF (Web Application Firewall) que fa de frontal davant d'atacs maliciosos i també fa de memòria cau per a documents estàtics com imatges o pàgines d'estil css, podria haver tingut algun problema puntual en servir correctament aquests continguts."

— Que "(...) s'ha pogut comprovar que cada usuari va poder consultar expedients seus i fins i tot el registre d'entrada 2022065660 presentat a les 10:25 també es va presentar per l'interessat corresponent. Per tant, es dedueix que el problema va ser únicament en la pàgina de la consulta de la posició global, la que es presenta com a captura de pantalla."

— Que "Al llarg de l'any 2022 es van realitzar 112.026 identificacions a la carpeta ciutadana a través de certificat electrònic o idCAT mòbil, i durant el 2023 ja hi ha més de 63.000, i ni el SSTI ni per part de Protecció de Dades hem conegut cap més cas com aquest, ni tampoc s'ha pogut reproduir l'error."

— Que "S'ha desactivat qualsevol sistema de memòria cau de fitxers estàtics per si pot haver estat el causant d'aquest creuament."

— Que "(...) la carpeta ciutadana es vincula al certificat electrònic de la persona corresponent utilitzant el servei VALid de l'AOC que retorna el NIF de la persona. Aquest NIF queda vinculat a l'identificador de sessió, generat aleatòriament i assegurant que és un valor únic. La identificació de la sessió es guarda en les galetes del navegador de l'usuari mentre no caduqui i mentre no es tanqui el navegador. En cada accés a la carpeta ciutadana es valida que la sessió sigui vàlida i no hagi caducat o s'hagi desconnectat voluntàriament. El SSTI entén que aquest mecanisme és l'estàndard per a identificar correctament l'usuari que es connecta en l'entorn web i el protocol HTTPS."

— Que "(...) des del Servei de Sistemes i Tecnologies de la Informació, en no veure cap intent d'atac a nivell de tallafocs ni en el Web Application Firewall, no aconseguir reproduir l'error, veure que el registre d'entrada presentat era correcte, que els expedients consultats pertanyien als interessats que els van consultar, i que amb els més de 400.000 accessos a la Seu electrònica des de que es va posar en marxa i fins a la data en que es va comunicar aquest incident no se'ns havia comunicat cap cas similar, es va considerar que no va ser una vulnerabilitat ni un atac a la nostra Seu electrònica."

4. En data 08/11/2023, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'Ajuntament de Girona per la comissió de dues infraccions: una de prevista a l'article 83.5.*a* en relació amb l'article 5.1.*f*; i una altra, per la vulneració del deure de confidencialitat, prevista a l'article 83.4.*a* en relació amb l'article 25, 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 dades (RGPD).

Aquest acord d'iniciació es va notificar a l'entitat imputada en data 13/11/2023.

5. 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.

6. En data 22/11/2023, l'Ajuntament va formular al·legacions a l'acord d'iniciació, que s'aborden a l'apartat 2 dels fonaments de dret.

7. En data 31/01/2024, 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 declarés que l'Ajuntament havia incorregut, en primer lloc, en una infracció prevista a l'article 83.5.*a* en relació amb l'article 5.1.*f,* tots ells de l'RGPD.

També s'assenyalava que l'Ajuntament havia comès una altra infracció, per la vulneració de l'obligació de protecció de dades des del disseny i per defecte. Això no obstant, s'indicava que, en aquest cas, atès que s'estaria davant d'un supòsit de concurs medial d'infraccions, només se sancionaria la infracció més greu de les presumptament comeses; és a dir, la relativa a la vulneració del principi de confidencialitat.

A més, la persona instructora proposava que l'entitat imputada adoptés les mesures següents:

— Que justifiqués que havia desactivat qualsevol sistema de memòria cau de fitxers estàtics.

— Que, en cas que l'anterior justificació no fos possible, aportés les recomanacions del fabricant del WAF (Web Application Firewall) o bé informes de vulnerabilitats i exposicions comunes que es corresponguin amb la que s'ha produït o de similars, així com la justificació que s'havien aplicat les mesures que s'hi recomanen.

— Que justifiqués que tenen el WAF actualitzat en la darrera versió estable i recomanada pel fabricant.

Aquesta proposta de resolució es va notificar en data 02/02/2024 i es concedia un termini de 10 dies per formular al·legacions.

8. En data 06/02/2024, l'entitat imputada va presentar un escrit sobre el compliment de les mesures que es proposaven a la proposta de resolució. En aquest escrit, l'entitat exposava el següent:

— Que "L'Ajuntament de Girona utilitza l'aplicatiu Fortiweb Cloud de l'empresa Fortinet, el qual s'ofereix en modalitat Software as a Service (SaaS), com a tallafocs d'aplicacions pels diferents dominis que ofereix (...)."

— Que "Pel que fa al domini seu.girona.cat, que proporciona els serveis de carpeta ciutadana, les mesures que es van aplicar una vegada detectada la incidència i que s'han mantingut fins aleshores, s'indiquen tot seguit. (...) el tallafocs d'aplicacions Fortiweb Cloud disposa de tot un seguit de mòduls que es poden activar o desactivar. Un dels quals és el de "Caching and compression", que permet servir fitxers directament des de la memòria cau i servir-los comprimits per a reduir-ne el consum d'ample de banda. (...) el mòdul de memòria cau està desactivat en el tallafocs d'aplicacions, evitant que es faci cap mena de memòria intermèdia o de manipulació per la compressió de fitxers."

— Que "(...) la versió del tallafocs d'aplicacions és la 24.1 la qual es va alliberar el dia 1 de febrer del 2024."

Fets provats

1. Fet provat primer

En data 20/07/2022, a les 10:35:11 hores, el denunciant va accedir a la seu electrònica de l'Ajuntament de Girona amb el seu certificat electrònic. En lloc d'entrar a la seva carpeta ciutadana, com pretenia, el sistema li va mostrar la pantalla inicial de la carpeta ciutadana d'una tercera persona. Segons els registres aportats per l'Ajuntament, el denunciant i aquesta tercera persona van iniciar sessió a la seu electrònica simultàniament.

D'acord amb l'anterior, l'Ajuntament no va implementar les mesures tècniques i organitzatives adequades, des del disseny i per defecte, per impedir que, si dues persones entren simultàniament al sistema, cadascuna amb el seu certificat electrònic, es pugui accedir a la pantalla inicial de la carpeta ciutadana d'una altra persona.

2. Fet provat segon

El fet de no haver implementat les mesures tècniques i organitzatives adequades va comportar que, en data 20/07/2022, a les 10:35:11 hores, el denunciant accedís a la informació continguda a la pàgina inicial de la carpeta ciutadana d'una tercera persona; en concret, a les dades següents: nom i cognoms, adreça d'empadronament (carrer, número, pis i porta), data de l'últim accés: 18/07/2022, 17:38 hores; expedients en tràmit: 7; i documents: 0.

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.

En el seu escrit d'al·legacions a l'acord d'iniciació, l'Ajuntament exposava:

— "(...) ens remetem, i donem per reproduïdes (...), a les al·legacions (...) que consten en la IP 108/2023 d'aquesta autoritat de control" (detallades a l'antecedent 3).

— "Considerem que en aquest cas sí es van implementar les mesures tècniques i organitzatives adequades atès que s'havia creat un identificador únic de sessió vinculada a la identificació via servei VALId del Consorci d'Administració Oberta de Catalunya. Aquest servei es basa en un model d'entitat-relació on l'identificador únic de sessió està configurat com a clau primària de l'entitat de manera que impossibilita, per disseny, que hi hagi duplicitats en l'identificador de la sessió. Aleshores, el fet que no hi hagi

identificadors de sessió duplicats en el sistema de l'Ajuntament de Girona evidencia que la mesura estava ben implementada."

Tal com va palesar la persona instructora a la proposta de resolució, tot i que l'Ajuntament considerés que s'havien implementat les mesures tècniques i organitzatives adequades, el cert és que en el si del procediment s'ha acreditat que en data 20/07/2022, a les 10:35:11 hores, el denunciant va accedir a la informació continguda a la pàgina inicial de la carpeta ciutadana d'un tercer; això es va produir perquè el denunciant i aquest altre usuari van iniciar sessió a la seu electrònica simultàniament. Aquests fets evidencien que el disseny del sistema per accedir a la carpeta ciutadana no va impedir que les dades d'almenys un dels usuaris quedessin exposades; en conseqüència, es va produir una vulneració del deure de confidencialitat. Per tot això, les al·legacions presentades no poden prosperar.

3. En relació amb els fets descrits al punt primer de l'apartat de fets provats, relatius a la manca d'adopció de les mesures tècniques i organitzatives apropiades, cal acudir a l'article 25 de l'RGPD, que disposa el següent:

> "1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."

Durant la tramitació d'aquest procediment s'ha acreditat el fet descrit al punt 1r de l'apartat de fets provats, que és constitutiu de la infracció prevista a l'article 83.4.*a* de l'RGPD, que tipifica la vulneració de "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43". Entre aquestes obligacions hi ha la que recull l'article 25 de l'RGPD transcrit més amunt, referent a la protecció de dades des del disseny i per defecte.

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.*d* de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), de la manera següent:

> "d) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per aplicar de manera efectiva els principis de protecció de dades des del disseny, així com la no integració de les garanties necessàries en el tractament, en els termes que exigeix l'article 25 del Reglament (UE) 2016/679."

4. Pel que fa al fet descrit al punt 2 de l'apartat de fets provats, referent a la revelació de dades personals, cal acudir a l'article 5.1.*f* de l'RGPD, el qual disposa que:

> "1. Los datos personales serán: (…) f) 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)."

El fet que quan la persona denunciant va accedir a la seu electrònica de l'Ajuntament, mitjançant certificat digital, tingués accés a les dades d'una tercera persona va comportar la vulneració del principi de confidencialitat.

De conformitat amb el que s'ha exposat, el fet recollit al punt 2 de l'apartat de fets provats constitueix la infracció prevista l'article 83.5.*a* de l'RGPD, que tipifica la vulneració de "los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;" entre aquests principis hi consta el de confidencialitat.

Al seu torn, aquesta conducta s'ha recollit com a infracció molt greu a l'article 72.1.*i* de l'LOPDGDD, de la manera següent:

> "i) La vulneració del deure de confidencialitat que estableix l'article 5 d'aquesta Llei orgànica."

Com ja es va avançar a la proposta de resolució, en aquest cas es considera que s'està davant d'un supòsit de concurs medial d'infraccions, atès que les dues infraccions imputades estan vinculades estretament, en la mesura que una és un mitjà necessari per a la comissió de l'altra (la no implementació de mesures adequades d'acord amb la protecció de dades des del disseny i per defecte va propiciar la vulneració del principi de confidencialitat).

L'article 29.5 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic (LRJSP), estableix que "quan de la comissió d'una infracció derivi necessàriament la comissió d'una altra o altres, s'ha d'imposar únicament la sanció corresponent a la infracció més greu comesa." D'acord amb aquest precepte i a la vista de l'anterior, en aquest cas escau imposar només una sanció, la corresponent a la infracció més greu de les comeses, és a dir, la relativa a la vulneració del principi de confidencialitat, qualificada d'infracció molt greu.

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

> "(...) ha de dictar una resolució que declari la infracció i estableixi, si s'escau, les mesures que convingui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès, a excepció de la que preveu l'article 58.2.i del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016.
>
> La resolució s'ha de notificar al responsable o l'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 aquest cas es considera que no escau requerir la implementació de mesures correctores, ja que, en data 06/02/2024, l'Ajuntament ha justificat que ha adoptat que havia proposat la persona instructora en els termes exposats en l'antecedent 8; les quals es consideren adequades per evitar que els fets es tornin a produir.

Resolució

Per tot això, resolc:

1. Declarar que l'Ajuntament de Girona ha comès una infracció prevista a l'article 83.5.*a* en relació amb l'article 5.1.*f*, ambdós de l'RGPD.

No cal requerir mesures per corregir els efectes de la infracció, de conformitat amb el que s'ha exposat al fonament de dret 5.

2. Notificar aquesta resolució a l'Ajuntament de Girona.

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 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, amb caràcter potestatiu l'entitat imputada pot interposar un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar a partir de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de la Llei 39/2015. També es pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius de Barcelona, en el termini de dos mesos a comptar a partir 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