Identificació de l'expedient

Resolució del procediment sancionador núm. núm. PS 3/2023, referent a l'Agència Catalana del Consum.

Antecedents

1. En data 27/10/2021 va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit pel qual una persona formulava una denúncia contra l'Agència Catalana del Consum, organisme autònom adscrit al Departament d'Empresa i Treball de la Generalitat, amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la persona denunciant exposava que el web de l'Agència Catalana del Consum (en endavant, Agència), i especialment el formulari per presentar reclamacions *"estava sota una connexió insegura"*. Manifestava que, per tal motiu, s'havia adreçat al delegat de protecció de dades de l'Agència, qui li hauria contestat que *"no faran res per solucionar-ho fins el gener de 2022"*. A l'efecte d'acreditar la seva denúncia, aportava dos correus electrònics:

- Un correu que la persona denunciant va enviar en data 30/09/2021 a l'adreça *"Bústia LOPD"* de l'Agència (lopd.acc@gencat.cat) amb l'assumpte *"inseguretat en formularis amb dades personals"*, en el qual posava de manifest, tant el que considerava una connexió insegura del seu web corporatiu - fent al·lusió a la manca d'un certificat segur-, com a eventuals *"problemes de filtració de dades personals quan s'estiguin omplint formularis",* derivats de la manca d'un certificat segur.

- Un correu de resposta de l'Agència, enviat en data 27/10/2021 des de l'adreça lopd.acc@gencat.cat a la persona aquí denunciant, en el qual s'assenyalava el següent:

  "(...) Actualment s'està fent la migració del portal consum.gencat.cat el que comportarà que els formularis de reclamacions també quedaran sota el protocol segur https. La previsió és que aquesta migració quedarà completada el proper mes de Gener. En qualsevol cas, cal tenir en compte que les dades dels formularis s'envien al nostre gestor d'expedients mitjançant un servei web. Aquest servei web, que recull les dades dels formularis i les fa arribar al gestor d'expedients, sí que es troba sota protocol segur (...)"

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 434/2021), 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 04/11/2022 l'Àrea d'Inspecció de l'Autoritat va fer una sèrie de comprovacions a través d'Internet sobre els fets objecte de denúncia. Així, es va constatar que el formulari que figurava al web de l'Agència, per a la formulació de

reclamacions o denúncies davant aquesta entitat, disposava d'un certificat d'autenticació del lloc web (amb una connexió xifrada). Del resultat obtingut es va aixecar la corresponent diligència de constància.

4. En data 11/11/2022 es va requerir l'Agència perquè informés sobre diverses qüestions relatives als fets denunciats.

5. En data 20/12/2022, l'Agència va respondre el requeriment esmentat a través d'escrit en què exposava el següent:

- Sobre si en la data dels fets denunciats (27/10/2021), el web de l'Agència Catalana de Consum no disposava d'un certificat d'autenticació del seu lloc web corporatiu (certificat SSL/TLS o altre), i no tenia implementat el protocol https o altre protocol de transferència d'arxius amb connexions xifrades; i si en l'actualitat ja en disposava d'un:

  "El 27/10/2021 el lloc web principal (consum.gencat.cat) no estava protegit per certificat https.
  En l'actualitat sí es disposa de certificat CDS consum.gencat.cat (dades a sota), migrant tot el sistema (lloc web i formularis que en pengen) a data 17/11/2021.
  A continuació reproduïm la informació de la captura de pantalla de posada en producció del sistema xifrat a data novembre 2021. Si s'escau podem enviar informació addicional en relació al certificat així com l'intercanvi de correus amb proveïdor de l'aplicació durant el procés de validació de la posada en marxa.
  Dades del certificat generat al 2021, amb validesa d'1 any. (...)

  Nom: consum.gencat.cat
  (...)
  Aplicació-
  Servei-
  Departament: EMT
  Tipus: SSL
  Autoritat: Sectigo

  El certificat va ser renovat el passat mes d'octubre d'aquest any 2022. El Certificat està qualificat sota CA Sectigo (les dades del certificat que es mostren a continuació són les que es poden veure i comprovar a la pàgina web de l'Agència).
  Dades del certificat vigent. (...)

- Sobre si durant el període de temps en què l'Agència no disposava d'un certificat d'autenticació del seu lloc web, l'enviament i l'enregistrament de les dades personals que s'efectuava a través dels formularis web (en tot cas, dels formularis adreçats a enviar una reclamació), s'efectuava en el marc d'un certificat d'autenticació del lloc web (amb una connexió xifrada) i en el seu cas, de quin certificat es tractava, i si corresponia a un certificat qualificat:

  "Tot i que abans de novembre de 2021, la web GECO consum.gencat.cat no era segura (HTTP), les crides al sistema destí (SIC) per enviar les dades dels formularis web (entre ells els de reclamació) sempre s'han fet per protocol segur (HTTPS). El servei invocat és el següent:
  https://empresa.extranet.gencat.cat/sicweb/AppJava/services/SicWebNvSOAP

A continuació facilitem les dades del certificat de servei invocat pels formularis. Hi ha constància de l'històric d'aquest certificat des de 2015, actualment renovat i amb CA Sectigo fins 2023 (captura a sota):
Nom: empresa.extranet.gencat.cat
(...)
Aplicació-
Servei-
DepartamentEMC
TipusSSL
AutoritatCatCert

(...)"

- Pel que fa als formularis web, sobre si durant el període de temps en què l'Agència no disposava d'un certificat d'autenticació del lloc web, quan un usuari enviava dades personals (formulava una consulta, una reclamació, una queixa o una denúncia, entre d'altres), després d'haver-hi enviat les dades, en la resposta del servei web corresponent a l'enviament figuraven dades personals:

  "La resposta del servei invocat pels formularis web no conté dades personals, només conté un número d'expedient. Com evidència d'aquest punt, adjuntem el següent enllaç a través del qual podreu accedir al fitxer xml / descriptor del servei web que invoquen els formularis: (...)''

L'Agència acompanyava el seu escrit de documentació diversa.

6. En data 13/01/2023, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'Agència Catalana del Consum per una presumpta infracció prevista a l'article 83.4.a), en relació amb l'article 32.1, ambdós 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 dita Agència en data 13/01/2023.

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

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

Fets provats

El lloc web principal de l'Agència Catalana del Consum, consum.gencat.cat, durant un període de temps indeterminat, però en tot cas fins el 28/10/2021 segons ha reconegut l'entitat, no disposava d'un certificat d'autenticació del seu lloc web corporatiu (certificat SSL/TLS o altre), i no tenia implementat el protocol HTTPS ni altre protocol de transferència d'arxius amb connexions xifrades, tret de l'enviament i l'enregistrament de dades que s'efectuava a través dels formularis web, el qual s'efectuava en el marc d'un certificat d'autenticació del lloc web (amb una connexió xifrada).

L'Agència ha acreditat disposar d'un certificat CDS emès en data 28/10/2021 (renovat el 03/10/2022), i ha manifestat que en data 17/11/2021 va fer efectiva la migració de les seves pàgines web a HTTPS.

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. D'acord amb l'article 64.2.f) de l'LPAC i de conformitat amb el que s'indica a l'acord d'iniciació d'aquest procediment, escau dictar aquesta resolució sense una proposta de resolució prèvia, atès que l'Agència no ha formulat al·legacions a l'acord d'iniciació. Aquest acord contenia un pronunciament precís sobre la responsabilitat imputada.

3. En relació amb la conducta descrita a l'apartat de fets provats, cal acudir en primer lloc a l'article 32.1 de l'RGPD, relatiu a la seguretat del tractament, el qual determina el següent:

> *"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."*

D'acord amb l'article 156.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, *"l'Esquema Nacional de Seguretat té per objecte establir la política de seguretat en la utilització de mitjans electrònics en l'àmbit de la present Llei, i està constituït pels principis bàsics i requisits mínims que garanteixin adequadament la seguretat de la informació tractada"*.

El Reial decret 3/2010, de 8 de gener, pel qual es regulava inicialment, i en tot cas en el moment dels fets imputats, l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica (a partir del previst a l'art. 42 de la Llei 11/2007, de 22 de juny, ja derogada), contenia al seu Annex II les mesures de seguretat que calia implementar per tal d'aconseguir el compliment dels principis bàsics i requisits mínims establerts a l'ENS. Entre aquestes mesures de seguretat, l'apartat 5 contenia les *mesures de protecció (mp)*, i el subapartat 5.8.2, intitulat "*Protecció de serveis i aplicacions web [mp.s.2]",* establia l'obligatorietat d'emprar certificats d'autenticació del lloc web en tots els casos, és a dir, tant

si calia establir un nivell baix en les mesures de seguretat, com un nivell alt, com segueix (el subratllat és nostre):

> *"Els subsistemes dedicats a la publicació d'informació han de ser protegits contra les amenaces que els són pròpies.*
> *a) Quan la informació tingui algun tipus de control d'accés, s'ha de garantir la impossibilitat d'accedir a la informació obviant l'autenticació, en particular prenent mesures en els aspectes següents:*
> *1r S'ha d'evitar que el servidor ofereixi accés als documents per vies alternatives al protocol determinat.*
> *2n S'han de prevenir atacs de manipulació d'URL.*
> *3r S'han de prevenir atacs de manipulació de fragments d'informació que s'emmagatzema en el disc dur del visitant d'una pàgina web a través del seu navegador, a petició del servidor de la pàgina, conegut en terminologia anglesa com a «cookies».*
> *4t S'han de prevenir atacs d'injecció de codi.*
> *b) S'han de prevenir intents d'escalat de privilegis.*
> *c) S'han de prevenir atacs de «cros site scripting».*
> *d) S'han de prevenir atacs de manipulació de programes o dispositius que realitzen una acció en representació d'altres, coneguts en terminologia anglesa com a «proxies», i sistemes especials d'emmagatzematge d'alta velocitat, coneguts en terminologia anglesa com a «caches».*
>
> *Nivell BAIX*
>
> *S'empraran "certificats d'autenticació del lloc web" de conformitat amb la normativa europea (...).*
>
> *Nivell ALT*
>
> *S'empraran "certificats qualificats d'autenticació del lloc web".*

Durant la tramitació d'aquest procediment ha quedat degudament acreditat el fet descrit a l'apartat de fets provats, a partir de la denúncia i dels correus adjunts presentats per la persona denunciant, però, especialment, del reconeixement en la fase precedent per part de l'Agència Catalana de Consum sobre la manca d'implementació d'un protocol HTTPS en el web principal durant el temps assenyalat, la qual cosa suposa un incompliment de l'obligació prevista a l'apartat 5.8.2 de l'ENS llavors vigent.

Això hauria fet el dit web més vulnerable als atacs informàtics, com ara, atacs de tipus *man-in-the-middle* ("atac d'intermediari"), en que l'atacant actua com a intrús entre els parts que s'estan comunicant. Així, podria haver-se donat el cas que una persona introduís dades en un formulari del web de l'Agència, a l'efecte de presentar una reclamació, i que ho hagués fet en una web que semblés idèntica a la que aquesta persona estigués visitant, però que en realitat es tractés d'una web falsa, que no correspongués al web oficial de l'Agència Catalana del Consum.

Val a dir que el Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS actualment vigent, igualment preveu al seu apartat 5.8.2 que els sistemes que presten serveis web han

de ser protegits front les mateixes amenaces contemplades a l'apartat 5.8.2 de l'anterior ENS.

Aquest fet imputat, i ara provat, és constitutiu d'infracció, segons el previst a l'article 83.4.a) de l'RGPD, que tipifica com a tal la vulneració de: *"a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"*

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

> *"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."*

Atès que en la fase precedent l'Agència va acreditar, en relació amb el seu lloc web principal, disposar d'un certificat CDS emès en data 28/10/2021 (renovat el 03/10/2022), i va manifestar que en data 17/11/2021 havia fet efectiva la migració de les seves pàgines web a HTTPS, es considera innecessari requerir l'adopció de mesures correctores.

Per tot això, resolc:

1. Amonestar l'Agència Catalana del Consum 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 4t.

2. Notificar aquesta resolució a l'Agència Catalana del Consum.

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,