Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 54/2021, referent al Departament de Salut de la Generalitat de Catalunya.

Antecedents

1. En data 30/06/2021 va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava denúncia contra el Departament de Salut, amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la persona denunciant exposava que havia detectat determinades vulnerabilitats de seguretat en el lloc web que el Departament de Salut ha posat a disposició de la ciutadania per demanar cita de vacunació (https://vacunacovid.catsalut.gencat.cat), ja que *"permet accedir de forma molt fàcil per part de tercers no autoritzats a dades de vacunació, targeta sanitària, mòbil, correu, nom complet, cita per la vacunació, etc. Per fer-ho només cal disposar del número de DNI (o targeta sanitària) de la víctima. No cal cap altre pas extra per verificar l'autenticitat, ni rebre cap SMS de verificació (a part de l'inicial)"*.

La persona denunciant detallava en el seu escrit la manera en què es podia accedir a informació de terceres persones, i literalment indicava els següents passos a seguir:

"1.(...)
2.(...)
3.(...)
4.(...).
5.(...)
6.(...)
7.(...)

En definitiva, la persona denunciant exposava que un cop l'usuari es validava al lloc web https://vacunacovid.catsalut.gencat.cat, fent determinades crides a la API (aplication programming interface) de la web a través de la consola del navegador, es podia accedir a dades de terceres persones.

Junt amb el seu escrit, la persona denunciant aportava impressions de pantalla en les que documentava cadascun dels passos que havia seguit per poder accedir a informació de terceres persones. En la documentació aportada s'havien anonimitzat les dades d'aquestes terceres persones.

A aquesta denúncia se li assignà el núm. IP 264/2021.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

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.

3. En data 05/07/2021, es va rebre a l'Autoritat una notificació del Departament de Salut d'una violació de seguretat de dades personals, d'acord amb el que preveu l'article 33 de l'RGPD, consistent en un possible ciberatac a la *"plataforma K2 de vacunacions",* arran d'haver-se detectat un volum inusual de consulta a dita plataforma.

4. En la fase d'informació prèvia iniciada arran la denúncia, en data 09/07/2021 es va requerir el Departament de Salut perquè donés compliment al següent:

- Informés sobre la vulnerabilitat detectada per la persona denunciant (antecedent 1r), les circumstàncies que l'haurien propiciat i si ja havia estat esmenada.
- Indiqués si, amb caràcter previ a la posada en marxa de la plataforma https://vacunacovid.catsalut.gencat.cat, s'havia elaborat un anàlisi de riscos pel que fa al tractament de dades personals a través d'aquest canal. En cas afirmatiu, n'aportés una còpia.

5. En data 22/07/2021 va entrar a l'Autoritat un escrit del Departament de Salut mitjançant el qual complementava la notificació de la violació de seguretat que havia fet en data 05/07/2021.

En el citat escrit el Departament de Salut descrivia la bretxa de seguretat com *"l'atac consisteix en realitzar peticions seqüencials de DNI, aprofitant una mancança en la validació de les peticions, saltant-se la cua d'espera i peticionant directament el node".*

6. El mateix dia 22/07/2021, el Departament de Salut va respondre el requeriment d'informació de 09/07/2021 (antecedent 4t), a través d'escrit en què exposava el següent:

- Que *"la vulnerabilitat que es descriu en l'expedient es va identificar el dia 1 de juliol arran de l'incident de seguretat notificat en l'expedient NVS 67/2021 produït contra la web (https://vacunacovid.catsalut.gencat.cat)"*, la qual consisteix en *"el retorn d'informació vinculada a una persona validant només el CIP o DNI. La informació que retornava en un primer moment es: DNI, CIP, nom i cognoms, telèfon mòbil, adreça electrònica, dia i hora de la cita, lloc de vacunació, tipus de vacuna*".
- Que "*s'han adoptat les següents mesures de contenció, mitigació i millores*:
  - *Ampliar el codi de verificació de 6 xifres numèriques a 6 xifres alfa numèriques*
  - *Moure la validació del codi del Frontal al node.*
  - *Aplicació de mesures de baneig de IP per número de peticions per minut (màxim de 500 peticions des de Espanya i 50 per minut des de estranger)*

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- *Bloqueig per un indicador de compromís identificat en el User Agent de la petició atacant.*
- *Bloqueig de les IP atacants conegudes*
- *Xifrat de la resposta*
- *Contacte amb el servei d'abuse dels proveïdors de les IP atacants*
- *Restringir la informació que retorna l'aplicació en fer-ne una petició, deixant només la informació respecte a la cita (data, hora i lloc de la vacunació i tipus de vacuna)".*

- Que "*els casos individuals eren de difícil detecció però les peticions massives activaven el sistema de control i seguiment".*
- Que "*respecte a l'anàlisi de riscos, degut d'una banda a la urgència d'iniciar el procés de vacunació i per una altra banda, la necessitat d'incorporar el màxim volum de població al procés de vacunació en el menor temps possible es varen realitzar proves de seguretat per no es va fer un anàlisis de riscos amb profunditat".*

7. En data 14/07/2021, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un altre escrit de denúncia contra el Departament de Salut, amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, l'entitat denunciant exposava que en un mitjà de comunicació digital (https://www.(...)) s'havia publicat una notícia en la que s'indicava que *"la página web de autocita para recibir la vacuna contra el coronavirus de la Generalitat de Catalunya, ha expuesto datos personales de los ciudadanos que han hecho uso de esta plataforma a terceros no autorizados".*

A aquesta denuncia se li assignà el núm. IP 283/2021

8. En data 22/09/2021 es va requerir el Departament de Salut perquè donés compliment al següent:

- Informés si el problema de seguretat del qual es feia ressò la noticia indicada era el mateix al qual es referia la vulnerabilitat de seguretat a la qual el Departament de Salut havia fet referència en el seu ofici data 22/07/2021, de resposta al requeriment que aquesta Autoritat li havia dirigit en el marc de la informació prèvia iniciada arran la denúncia núm. IP 264/2021. I, en cas que no fos així donés resposta al següent:
- Informés detalladament sobre el problema de seguretat al qual s'estaria referint la noticia, les circumstàncies que l'haurien propiciat i si ja ha estat esmenat.

9. En data 08/10/2021, el Departament de Salut va contestar aquest segon requeriment per mitjà d'escrit a través del qual manifestava el següent:

- Que el problema de seguretat del qual es feia ressò la notícia indicada és el mateix al qual es referia la vulnerabilitat de seguretat detectada en el marc de la informació prèvia iniciada arran la denúncia núm. IP 264/2021, en la mesura que coincideixen les dates de publicació i

que la mateixa noticia inclou el contingut literal del comunicat de premsa efectuat pel Departament de Salut en el sentit que s'havia comunicat a l'Autoritat la bretxa de seguretat a través de la corresponent notificació de violació de seguretat que va donar lloc a l'expedient NVS 67/2021.

10. En data 27/10/2021, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra el Departament de Salut per dues presumptes infraccions: una infracció prevista a l'article 83.5.a), en relació amb l'article 5.1.f); i, una altra infracció prevista a l'article 83.4.a), en relació amb l'article 35; 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 27/10/2021.

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. Aquest termini es va superar amb escreix sense que el Departament de Salut formulés al·legacions.

11. En data 21/12/2021, la instructora d'aquest procediment va formular una proposta de resolució, en què proposava la modificació de la qualificació jurídica dels fets imputats que s'havia efectuat a l'acord d'iniciació i això de conformitat amb el previst a l'article 89.3 de l'LPAC. La instructora, un cop valorada detingudament la documentació incorporada a les actuacions, estimà que els dos fets imputats constituïen, cadascun d'ells, una vulneració de la seguretat de les dades. A la vista de l'anterior, en la proposta de resolució la instructora proposava que la directora de l'Autoritat Catalana de Protecció de Dades amonestés el Departament de Salut com a responsable de la infracció prevista a l'article 83.4.a) en relació amb l'article 32 de l'RGPD.

Aquesta proposta de resolució es va notificar en data 21/12/2021 i es concedia un termini de 10 dies per formular al·legacions.

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

Fets provats

1. Des d'una data indeterminada, però en tot cas fins el dia 30/06/2021, els sistemes d'informació del Departament de Salut permetien que, un cop l'usuari es validava al lloc web https://vacunacovid.catsalut.gencat.cat (web que el Departament havia posat a disposició de la ciutadania per tal de demanar cita de vacunació), fent crides a l'API de la web, aquest pogués accedir a dades d'altres usuaris del sistema de salut (com ara, el DNI, el CIP, nom i cognoms, telèfon mòbil, adreça electrònica, dia i hora de la cita, lloc de vacunació i tipus de vacuna).

2. En relació amb el tractament de dades vinculat a la posada en marxa del lloc web https://vacunacovid.catsalut.gencat.cat, el Departament de Salut no va realitzar una anàlisi de riscos per determinar les mesures tècniques i organitzatives apropiades per garantir la seguretat de les dades.

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. En relació amb els fets descrits als punts 1r i 2n de l'apartat de fets provats, relatius a la seguretat de les dades, cal acudir a l'article 32 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.*
> 2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
> (...)"

Com s'ha dit, respecte les conductes descrites als punts 1 i 2 de l'apartat de fets provats, es considera que en el si d'aquest procediment ha quedat provat que el Departament de Salut ha vulnerat les mesures de seguretat que es detallen a continuació de forma separada, amb cita dels preceptes que les regulen:

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

2.1.- En relació amb el fet provat 1r:

D'acord amb el que disposa la disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), cal mencionar el que estableix el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica, i concretament el seu apartat 4.2.2 *"Requisitos de acceso"* de l'Annex II ("*Mesures de Seguretat*"):

> *"Los requisitos de acceso se atenderán a lo que a continuación se indica:*
> *a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes".*

2.2.- En relació amb el fet provat 2n:

En aquest punt cal fer expressa referència a allò que preveu l'apartat 2n de l'article 32 de l'RGPD ja transcrit, que obliga al responsable del tractament a dur a terme una anàlisi de riscos d'aquells tractaments que prevegi fer, a fi i efecte de determinar les mesures de seguretat que cal implementar.

De conformitat amb el que s'ha exposat, el fets recollits als punts 1r i 2n de l'apartat de fets provats constitueixen la infracció prevista 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.

Aquestes conductes s'han 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."*

3. 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 (...)".*

En virtut d'aquesta facultat, i pel que fa al fet provat 2n, escau requerir el Departament de Salut perquè al més aviat possible i en tot cas en el termini màxim de 1 mes a comptar des de l'endemà de la notificació d'aquesta resolució, acrediti a aquesta Autoritat haver dut a terme una anàlisi de riscos de conformitat amb l'article 32 de l'RGPD, per tal de determinar les mesures tècniques i organitzatives apropiades per garantir la seguretat de les dades tractades a través de la plataforma https://vacunacovid.catsalut.gencat.cat.

Pel que fa al fet provat 1r, no escau requerir l'adopció de cap mesura correctora, ja que el Departament de Salut va acreditar a aquesta Autoritat, en el marc de la NVS 67/2021, haver pres les mesures adequades per solucionar l'incident de seguretat detectat en la plataforma https://vacunacovid.catsalut.gencat.cat.

Per tot això, resolc:

1. Amonestar el Departament de Salut com a responsable de la infracció prevista a l'article 83.4.a) en relació amb l'article 32, ambdós de l'RGPD.

2. Requerir el Departament de Salut perquè acrediti davant aquesta Autoritat haver dut a terme l'actuació assenyalada al fonament de dret 3r, en el termini indicat.

3. Notificar aquesta resolució al Departament de Salut.

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

5. 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.