Identificació de l'expedient

Resolució del procediment sancionador núm. PS 20/2022, referent a l'Institut Català de la Salut (Hospital de Viladecans)

Antecedents

1. En data 11/06/2021, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava denúncia contra l'Hospital de Viladecans, depenent de l'Institut Català de Salut (ICS), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals. La persona denunciant exposava el següent:

1.1 Que l'Hospital de Viladecans havia fet públiques diverses URLS on introduint només el DNI, sense cap altre comprovació, es podien obtenir dades personals dels pacients. Concretament, el nom, adreça, CIP, data de naixement, telèfon i correu electrònic.

1.2 Que per tal d'acreditar l'anterior manifestació, aportava les següents URLS en les que fent clic a l'opció 'lupa', s'obtenien les dades personals esmentades:

https://ciutadania.metrosud.cat/ciutadania/FRM/frm_canvi_identificatiu.aspx
https://ciutadania.metrosud.cat/ciutadania/FRM/frm_canvi_data.aspx
https://ciutadania.metrosud.cat/ciutadania/

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 252/2021), 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 prèvia, en data 14/06/2021, 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 accedint al web de l'Hospital de Viladecans (http://www.viladecanshospital.cat/ca/default.aspx), apartat 'Unitat d'atenció a la ciutadania > Fem-ho fàcil' en les opcions 'Reclamacions queixes i suggeriments' i 'Canvi de Dades identificatives', introduint el DNI de la persona denunciant i fent clic a l'opció 'lupa', s'obtenien les dades personals següents:

Pel que fa a la primera opció: nom, cognoms, número de CIP i telèfon.

Pel que fa a la segona opció: nom, cognoms, número de CIP, telèfon, adreça del domicili, i data de naixement.

També es va comprovar que en el mateix apartat 'Unitat d'atenció a la ciutadania > Fem-ho fàcil', en les opcions 'Informació visites i proves pendents / canvi de data' i 'Consulta llista d'espera quirúrgica', seguint el mateix procés d'accés, es podia obtenir el número de CIP de la persona denunciant.

Seguidament, es va aixecar diligència de constància per part de la instructora i es va conservar còpia automatitzada de les dades personals a les quals s'havia tingut accés mitjançant la introducció del DNI de la persona denunciant.

4. En la mateixa data, 14/06/2021,es va requerir a l'entitat denunciada perquè confirmés que mitjançant introducció de DNI de qualsevol pacient a les rutes especificades en el punt anterior, es podien obtenir, en funció de l'opció seleccionada ("Reclamacions, queixes i suggeriments", "canvi de dades identificatives", "Sol·licitud d'informes de consultes externes", "sol·licitud documentació clínica / altres informes de proves (no imatges)", "sol·licitud còpia d'imatge", "informació visites i proves pendents / canvi de data", "consulta llista d'espera quirúrgica", "canvi de dades identificatives", "sol·licitud canvi de facultatiu especialista", "per qualsevol altre tipus de consulta") les següents dades personals:

- Nom, cognoms, número de CIP i telèfon;
- Nom, cognoms, número de CIP, telèfon, adreça del domicili, i data de naixement; o
- Número de CIP

També es va requerir a l'entitat que indiqués en relació a quins pacients es podien obtenir aquestes dades i si es podien visualitzar altres dades clíniques o de salut vinculades al pacient.

5. En data 06/07/2021 i dins del marc d'aquesta fase d'informació prèvia, l'Àrea d'Inspecció de l'Autoritat va tornar a accedir a Internet per a efectuar noves comprovacions sobre els fets objecte de denúncia. Així, es va constatar que accedint a la pàgina web de l'Hospital de Viladecans, apartat 'Unitat d'atenció a la ciutadania > Fem-ho fàcil' apareixia un missatge que deia 'Aplicació temporalment fora de servei. Disculpeu les molèsties' i, per tant, les dades ja no eren accessibles.

6. En data 19/07/2021, l'Institut Català de la Salut (Hospital de Viladecans) va donar compliment al requeriment d'informació a través d'escrit en què exposava el següent:

- Que per error tècnic, en la web de l'Hospital de Viladecans es va publicar un entorn de proves on mitjançant introducció del DNI del pacient, es recuperava la 'informació de filiació' que, segons manifestava, consistia en el nom, número de CIP, adreça del domicili, telèfon i adreça de correu electrònic; i que en cap cas eren dades obertes dels pacients de l'hospital ni de qualsevol pacient atès a l'organització, sinó només dels pacients 'actius' de l'Hospital de Viladecans.
- Que no es podia visualitzar cap dada relacionada amb la informació clínica i assistencial del pacient.
- Que en el moment de detecció de l'error tècnic es va procedir a la despublicació de les pàgines web de manera que no es pugues accedir des de l'exterior, és a dir, Internet.
- Així mateix, va manifestar que en el moment de presentació de resposta al requeriment (19/07/2021), ja no es podia accedir a cap de les URL denunciades.

7. En data 20/04/2022, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'ICS per una presumpta infracció prevista en l'article 83.4.a) en relació amb l'article 32; 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). Així mateix, va nomenar persona instructora de l'expedient a la senyora (...),

funcionaria de l'Autoritat Catalana de Protecció de Dades. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 22/04/2022.

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.

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

Fets provats

La pàgina web de l'Hospital de Viladecans (http://www.viladecanshospital.cat/ca/default.aspx) permetia accedir a les dades personals dels pacients, seguint la ruta '*Unitat d'atenció a la ciutadania* > *Fem-ho fàcil',* seleccionant una de les quatre opcions que s'especificaran a continuació, i tan sols introduint el DNI i fent clic a l'opció '*lupa'*, sense requerir de cap altra dada addicional, ni contrasenya, ni mesura d'autenticació addicional.

Opcions:
- Opció '*Reclamacions queixes i suggeriments'*: el nom, cognoms, número de CIP i telèfon.
- Opció *'Canvi de Dades identificatives'*: el nom, cognoms, número de CIP, telèfon, adreça del domicili, i data de naixement.
- Opció '*Informació visites i proves pendents / canvi de data'* i opció *'Consulta llista d'espera quirúrgica'*: el número de CIP

Aquesta situació es va mantenir per un període de temps indeterminat que, com a mínim, compren des del dia 14/06/2021, data en la que l'Àrea d'Inspecció de l'Autoritat va efectuar comprovacions a través d'Internet i va confirmar l'accessibilitat a les dades personals d'un pacient mitjançant introducció del seu DNI com a únic requeriment d'accés; i fins una data indeterminada però en tot cas anterior al dia 6/07/2021, data en què l'Àrea d'Inspecció va efectuar noves comprovacions i va constatar que ja no es podia accedir a la ruta esmentada en el primer paràgraf d'aquest apartat.

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'entitat imputada no ha formulat al·legacions a l'acord d'iniciació.

Aquest acord contenia un pronunciament precís sobre la responsabilitat imputada.

3. Pel que fa al fet descrit en l'apartat de fets provats, relatiu a la seguretat de les dades, cal acudir a l'article 32 de l'RGPD, que disposa:

"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 persones físicas, el responsable y el encargado del tratamiento aplicaran medidas técnicas y organizativas apropiades 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.*
3. *La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*
4. *El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".*

Així mateix, 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, 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, en el seu article 16:

"Artículo 16. ***Autorización y control de los accesos.***

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas."

L'apartat 4.2.5 *"Mecanismo de autenticación"* de l'Annex II ("Mesures de Seguretat") de l'ENS, determina el següent:

"Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseña o claves concertadas.

- "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens)

- "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

(…)

Nivel BAJO
a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
c) Se atenderá a la seguridad de las credenciales de forma que:
1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
(...)"

També l'article 9.4 de la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent a la salut i autonomia del pacient, i a la documentació clínica, determina que *"els centres sanitaris han de prendre les mesures tècniques i organitzatives adequades per a protegir les dades personals recollides i evitar-ne la destrucció o la pèrdua accidental, i també l'accés, l'alteració, la comunicació o qualsevol altre processament que no siguin autoritzat".*

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit en l'apartat de fets provats, reconegut, a més, per la pròpia entitat denunciada en les seves al·legacions en fase d'informació prèvia (IP 252/2021), quan admet haver comés '*un error tècnic*' al publicar '*un entorn de proves on introduint el DNI d'un pacient es recuperava informació de filiació (noms, CIP, adreça, telèfon i adreça de correu electrònic).'*

Aquest fet és constitutiu de la infracció prevista l'article 83.4.a) l'RGPD, que tipifica la vulneració de *"las obligaciones del responsable y del encargado a tenor de los articulos 8, 11, 25 a 39, 42 y 43"* entre els quals hi ha l'obligació descrita a l'article 32 referida a la seguretat del tractament.

Al seu torn, aquesta conducta 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. 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 el present cas, no escau requerir l'ICS l'adopció de mesures correctores per tal de corregir els efectes de les infraccions, ja que es tracta d'un fet ja consumat i, a més, l'ICS, en el moment de detecció de l'error, va procedir a la despublicació de les pàgines web. Així mateix, va manifestar que en el moment de presentació de resposta al requeriment d'aquesta Autoritat (19/07/2021), ja no es podia accedir a cap de les URL denunciades.

Per tot això, resolc:

1. Amonestar l'Institut Català de la Salut com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32, 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 4.

2. Notificar aquesta resolució a l'Institut Català de la Salut.

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,