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

Identificació de l'expedient

Resolució procediment sancionador núm. PS 39/2021, referent al Servei Català de la Salut.

Antecedents

1. En data 14/07/2020, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit pel qual un Delegat de Protecció de Dades (DPD) d'un hospital participant en un estudi promogut i finançat pel Servei Català de la Salut (en endavant, CatSalut), posava en coneixement d'aquesta Autoritat uns fets que podrien contravenir la normativa de protecció de Dades. En concret, el DPD exposava que l'hospital en el qual exercia les seves funcions, inicialment havia acceptat participar en l'estudi anomenat *"Avaluació de l'estat immunitari del personal sanitari a Catalunya davant el virus SARS-COV2: informació per a les estratègies i preses de decisions del sistema sanitari català"*; i, exposava que en el marc d'aquest estudi s'havia detectat una bretxa de seguretat en la plataforma que el CatSalut feia servir per aquest estudi, en concret indicava que *"s'ha observat que a la plataforma si poses el NIF al cercador al que es té accés com a usuari de l'enquesta de l'estudi, es veu absolutament totes les dades que té el RCA* [Registre Central de persones assegurades] *(adreça, número afiliació, CAP, tipus de cobertura ….). Si ens anem inventant NIFs podem accedir a les dades de qualsevol persona"*.

Junt amb aquest escrit s'aportava diversa documentació, entre d'altra, el document intitulat *"AVALUACIÓ DE L'ESTAT IMMUNITARI DEL PERSONAL SANITARI A CATALUNYA EN FRONT AL VIRUS SARS-CoV2 Comunicació de dades de professionals"*, de 29/06/2020, que detallava el disseny de l'estudi i els protocols a seguir en la recollida d'informació. Entre d'altres, i pel que fa a la relació amb les persones que podrien participar amb l'estudi, s'indica el següent:

"(...) s'enviarà un correu electrònic a cada professional, indicant la possibilitat d'adherir-se a aquest estudi. Dins el text d'aquest correu, s'informarà de l'adreça a la que els professionals poden accedir per tal de poder omplir una breu enquesta i donar el seu consentiment explícit a la participació en aquest estudi (...)".

2. Tot i que el DPD havia posat en coneixement de l'Autoritat aquests fets utilitzant el formulari de notificació de violació de seguretat, es va considerar que, atesa la naturalesa dels fets descrits, aquesta notificació havia de ser considerada com una denúncia, de la qual cosa es va informar al DPD de l'hospital.

3. En consonància amb l'anterior, l'Autoritat va obrir una fase d'informació prèvia (núm. IP 216/2020), 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.

4. En aquesta fase d'informació, en data 24/07/2020 es va requerir el DPD denunciant per tal que informés en quines circumstàncies concretes -mitjançant l'aplicatiu al qual accedia el personal sanitari que havia decidit participar en l'estudi esmentat- es podien visualitzar les dades que constaven a l'RCA de qualsevol persona quin NIF s'introduís al cercador del citat aplicatiu.

5. En data 26/07/2020 el DPD de l'hospital va donar resposta a aquest requeriment en els següents termes:

"Podem transcriure el que van detectar els nostres serveis d'informació:
«El problema de seguretat doncs sí, és cert. He posat el NIF de la meva dona al cercador al que es té accés com a usuari d'aquesta enquesta i veig absolutament totes les dades que té el RCA (adreça, número afiliació, CAP, tipus de cobertura...). Si ens anem inventant NIFs podem accedir a les dades de qualsevol persona».
Com d'altre treballador del centre sanitari en primer moment:
«Se han cedido a terceros sin mi consentimiento explícito datos personales: como nombre y apellidos, NIF, CIP, sé que es así porque te identifica con el NIF y automáticamente carga el CIP, (…)
El programa tiene un bug de seguridad y he podido ver las variables del mismo, no he trasteado más, pero no está adecuadamente protegido, envío foto»".

6. En data 31/07/2020 es va requerir el CatSalut -com a responsable del tractament de l'RCA, i com a promotor de l'estudi citat- perquè informés sobre en quines circumstàncies les persones treballadores dels centres hospitalaris que havien decidit participar en l'estudi d'investigació, podien accedir a dades de terceres persones contingudes en l'RCA; i en concret, si aquest accés permetia visualitzar: a) les dades de qualsevol persona inscrita en aquest registre; o, b) les dades de les persones treballadores dels centres que participaven a l'estudi.

7. Mitjançant escrit de 03/08/2020 el CatSalut va sol·licitar una ampliació del termini per donar resposta el requeriment, la qual li fou concedida en data 05/08/2020.

8. Mitjançant escrit de 31/08/2020 el CatSalut va sol·licitar una nova ampliació del termini per donar resposta al requeriment, la qual li fou denegada en data 16/09/2020. El mateix dia s'advertí a l'entitat que en cas de no donar resposta al requeriment, es podia incórrer en una infracció de la normativa de protecció de dades.

9. En data 23/09/2020 el CatSalut va donar resposta al requeriment, exposant el següent:

- *"El sistema esta previst de manera que per accedir a l'enquesta es necessita un Link personalitzat que envia l'aplicació a traves d'un Token únic, amb aquest Link que només rep la persona interessada* [la persona participant a l'estudi]*, s'accedeix a una pàgina on es*

demana el DNI i es comprova que la relació TOKEN-DNI es compleixi sinó no es pot continuar.
Durant els primers dies dins l'enquesta va haver un bug que et permetia canviar el DNI i posar el d'un altre persona. En el moment que es va conèixer el problema es var solucionar immediatament i ja no es pot modificar res de la persona participant a l'estudi, això concretament es va solucionar el 21/07/2020 que va ser el dia que es va tenir coneixement de la incidència".

- *"No es pot concretar amb exactitud si l'accés a les dades de l'RCA permetia visualitzar les dades de qualsevol registre, les dades de totes les persones que participaven a l'estudi, atès que des del mateix moment que es va tenir coneixement de la 'incidència es va solucionar i en aquests moments no es reproduïble, la qual cosa hores d'ara no es pot fer la comprovació".*

10. En data 21/06/2021, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra el CatSalut per una presumpta infracció prevista a l'article 83.4.a), en relació a l'article 32; 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 l'entitat imputada en data 23/06/2021.

11. A l'acord d'iniciació es concedia a l'entitat imputada un termini de 10 dies hàbils, comptadors a partir de l'endemà de la notificació, per formular al·legacions i proposar la pràctica de proves que considerés convenients per defensar els seus interessos.

Aquest termini s'ha superat amb escreix i no s'han formulat al·legacions.

Fets provats

Les persones treballadores de determinats centres sanitaris van rebre un correu mitjançant el qual s'oferia als dits professionals la possibilitat d'adherir-se a l'estudi d'investigació anomenat *"Avaluació de l'estat immunitari del personal sanitari a Catalunya davant el virus SARS-COV2: informació per a les estratègies i preses de decisions del sistema sanitari català"*; promogut pel CatSalut. En aquest correu es facilitava a la persona treballadora un link personalitzat a través d'un Token únic -associat al DNI- al qual s'havien de connectar per omplir l'enquesta i donar el seu consentiment explícit a la participació en l'estudi.

Des de, al menys el 14/07/2020, fins el 21/07/2020, el sistema permetia a la persona usuària de l'enquesta canviar el DNI al cercador de l'aplicatiu i posar el d'una altra persona, de manera que, en cas de fer-ho, es podien visualitzar les dades d'aquesta tercera persona contingudes al Registre Central de persones Assegurades (com ara, domicili, núm. CIP, etc), del qual és responsable del tractament el CatSalut.

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

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. 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 confidencialitat, segons el qual 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".*

Per la seva banda, l'article 32 de l'RGPD, referent a la seguretat de les dades, estableix 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.*
> *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".

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 fer referència al 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, més concretament, el seu article 16 relatiu a l'autorització i control dels accessos:

"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. *"Control de acceso"* de l'Annex II ("Mesures de Seguretat") de l'ENS, determina el següent:

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.
(…)
En todo control de acceso se requerirá lo siguiente:
a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].
c) Que la utilización de los recursos esté protegida [op.acc.2].
d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
f) Que la identidad de la entidad quede suficientemente autenticada [op.acc.5].
g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del

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

> *sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.*
>
> *Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).*

I, concretament, l'epígraf 4.2.2 *"Requisitos de acceso"*, determina el següent:

dimensiones	*I C A T*		
nivel	*bajo*	*medio*	*alto*
	aplica	=	=

> *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.*
> *b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.*
> *c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración."*

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit a l'apartat de fets provats, relatiu a la manca d'implementació d'un control d'accés adequat, el que és constitutiu de la infracció prevista a l'article 83.4.a) de l'RGPD, de l'RGPD, que tipifica com a tal la vulneració de *"las obligaciones del responsable y del encargado (...)"*, en aquest cas aquelles vinculades amb la seguretat 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:

> *"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 cas que aquí es ocupa no escau requerir el CatSalut perquè adopti cap mesura correctora per corregir els efectes de la infracció, ja que en el si de la informació prèvia que precedí a aquest procediment sancionador (antecedent 9è), l'entitat va informar a aquesta Autoritat que *"en el moment que es va conèixer el problema es va solucionar immediatament i ja no es pot modificar res de la persona participant a l'estudi, això concretament es va solucionar el 21/07/2020 que va ser el dia que es va tenir coneixement de la incidència"*.

Per tot això, resolc:

1. Amonestar el Servei 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 4t.

2. Notificar aquesta resolució al Servei 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

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

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,