

## Identificació de l'expedient

Resolució d'arxivament de la informació prèvia núm. IP 635/2023, referent a la Fundació Hospital Sant Joan de Déu de Martorell.

## Antecedents

1. En data 05/12/2023, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit de denúncia contra la Fundació Hospital Sant Joan de Déu de Martorell (FHSJDM), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la persona denunciant exposava que, per accedir al recinte de l'Hospital Sant Joan de Déu de Martorell, personal de seguretat d'una empresa subcontractada per la FHSJDM fa un control d'accés en què es demana a les persones que volen visitar usuaris ingressats que s'identifiquin i que informin sobre el nom i cognoms de la persona que volen visitar. Respecte d'això, indicava que el personal que realitza aquest control disposa d'un llistat on consta la informació següent: nom i cognom, número d'historial clínic i/o número de DNI de tots els pacients ingressats. La denunciant també indicava que, quan el personal de seguretat s'absenta del seu lloc de treball, aquest tapa l'esmentat llistat amb un full en blanc i el deixa damunt d'una taula "que és de lliure accés per tothom".

En darrer terme, indicava que l'esmentat control d'accés es va implementar amb motiu de la incidència de la COVID-19.

L'escrit de denúncia s'acompanya d'una reclamació que va presentar davant la FHSJDM en data 25/10/2023, per mitjà de la qual denunciava els mateixos fets.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 635/2023), 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), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador.
3. En data 15/01/2024, en el si d'aquesta fase d'informació prèvia, l'Àrea d'Inspecció de l'Autoritat va fer una sèrie de comprovacions a través d'internet sobre els fets objecte de denúncia. Així, va constatar que, per mitjà del web de la FHSJDM, i en concret a l'apartat "normativa visites", es podia accedir a una infografia que estableix normes per a les visites a pacients, i que preveu que les persones acompanyants s'han d'acreditar a l'entrada de l'hospital.
4. També en el si d'aquesta fase d'informació prèvia, en data 16/01/2024 es va requerir l'entitat denunciada perquè, entre d'altres qüestions: identifiqués l'empresa encarregada del control d'accés a l'Hospital i aportés el contracte d'encarregat del tractament; identifiqués les mesures de seguretat i tècniques implementades en relació amb el llistat que utilitza el personal de seguretat; i assenyalés la finalitat del tractament de dades personals denunciat.

5. En data 29/01/2024, la FHSJDM va respondre el requeriment d'informació amb un escrit en què exposava el següent:
- L'empresa encarregada dels controls d'accessos a la FHSJDM és IMAN SEGURIDAD SA. S'adjunta el contracte de serveis, així com l'acord específic d'encarregat del tractament formalitzat amb aquesta empresa, on es descriuen aspectes rellevants en matèria de protecció de dades i privacitat.
  - Durant els controls d'accessos, el personal auxiliar pregunta al visitant el seu nom i cognoms i li demana els dos cognoms del pacient ingressat. Després de consultar el llistat, comunica al visitant el número d'habitació del pacient.
  - Les dades que consten al llistat que utilitza el personal que realitza els controls d'accessos són, únicament, el número d'habitació i els cognoms del pacient.
  - Per tal de garantir la màxima seguretat i confidencialitat de les dades, aquest personal auxiliar ha de seguir un protocol rigorós. En cap moment deixa el llistat, que inclou dades dels pacients, "a la vista". En cas d'absència temporal, l'auxiliar s'enduu el llistat o el guarda en un lloc segur –com ara un armari tancat amb clau. Així, s'assegura que les dades romanen protegides en tot moment i evita qualsevol accés no autoritzat, o exposició accidental.
  - El protocol de l'hospital "Actuació davant la nova normalitat en la pandèmia COVID-19", establert el maig de 2020, detalla els procediments per a la gestió segura de l'accés durant la pandèmia. Aquest protocol preveu un control previ a l'entrada i que els acompanyants dels pacients presentin acreditació per entrar. Aquest document, juntament amb la "Normativa de visites a pacients" i el "Pla d'acció per rebrot del Covid-19", evidencia el compromís de l'hospital amb la seguretat i la protecció en el context de la pandèmia, així com la necessitat de controlar els accessos sota un criteri de proporcionalitat.
  - La finalitat del tractament de dades personals efectuat a través del control d'accés queda directament relacionada amb les mesures implementades a causa de la incidència de la COVID-19. Aquesta acció es justifica i s'acredita amb el Protocol de Nova Normalitat (adjunt), que detalla les mesures necessàries per garantir la seguretat i salut tant dels pacients com del personal, en el context de la pandèmia. Aquest protocol subratlla la importància del control d'accés com a mesura preventiva essencial per limitar la propagació del virus dins de les instal·lacions de l'hospital.
  - El control d'accés en un hospital té com a objectiu principal garantir la seguretat dels pacients, del personal i de les instal·lacions arran de la COVID-19 i de la seguretat en termes generals. La base legal per a aquest tractament és l'interès públic (art. 6.1.e RGPD), que es basa en la necessitat de garantir la seguretat i integritat de les persones i les instal·lacions, així com les obligacions legals del sector sanitari i de la salut, com per exemple la normativa relativa a la prevenció de riscos laborals o de la lluita contra la COVID-19.
  - Els noms i cognoms són dades bàsiques per identificar els individus i permeten un control efectiu sense recórrer a dades més excessives i/o sensibles. Així, evitem el risc d'errors associats amb el tractament alternatiu de dades, com ara l'ús exclusiu de

números d'habitació, que poden canviar i portar a confusions o situacions de risc per a la seguretat dels pacients i el personal.

L'entitat denunciada adjuntava a l'escrit documentació diversa.

5.1 Contracte de serveis de vigilància i protecció formalitzat entre FHSJDM i IMAN SEGURIDAD, SA.

5.2 Contracte d'encarregat del tractament signat entre FHSJDM i IMAN SEGURIDAD, SA. La clàusula tercera d'aquest contracte regula el deure de confidencialitat i secret professional, en relació amb totes les dades personals a les quals el personal de l'empresa proveïdora del servei pugui accedir com a conseqüència de la prestació de serveis. Així mateix, la clàusula cinquena disposa les mesures de seguretat que ha d'implementar l'encarregat del tractament per preservar la seguretat de la informació.

5.3 Protocol de nova normalitat, que regula el pla d'actuació en relació amb els usuaris que accedeixen a l'hospital.

5.4 Normativa de visites per a familiars o acompanyants de pacients sense COVID-19, que preveu que, en el moment d'ingressar al centre sanitari l'acompanyant s'ha d'acreditar al personal que fa els controls d'accessos.

5.5 Pla d'acció per rebrot de la pandèmia COVID-19.

## Fonaments de dret

1. D'acord amb el que preveuen els articles 90.1 de l'LPAC i 2 del Decret 278/1993, en relació amb l'article 5 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i l'article 15 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, és competent per dictar aquesta resolució la directora de l'Autoritat Catalana de Protecció de Dades.

2. A partir del relat d'antecedents, cal analitzar els fets denunciats objecte d'aquesta resolució d'arxivament.

2.1. Sobre la licitud del tractament de les dades personals dels pacients ingressats i de les persones acompanyants

En primer lloc, la persona denunciant exposava que el personal de seguretat de la FHSJDM demanava a les persones que accedien a l'hospital que s'identifiquessin (nom i cognoms) i que indiquessin a quin pacient ingressat volien visitar. Respecte d'això, indicava que, un cop la persona visitant facilitava aquesta informació, el personal de seguretat li indicava el número d'habitació del pacient, a partir de la consulta d'un llistat físic. D'acord amb les afirmacions de la persona denunciant, l'esmentat llistat contindria la informació següent: noms, cognoms, número d'historial clínic i/o DNI dels pacients ingressats.

Al seu torn, la FHSJDM va exposar que el tractament de dades personals denunciat es duu a terme per controlar la incidència de la COVID-19 als centres sanitaris i, també, per preservar la seguretat i salut pública en termes generals. Vinculat amb l'anterior, també

feia referència a l'obligació de complir la normativa de prevenció de riscos laborals, per preservar la integritat de les persones i instal·lacions, així com d'altres obligacions legals en matèria sanitària. També indicava que, contràriament al que sosté la persona denunciant, el llistat que empra el personal de l'empresa IMAN SEGURIDAD SA només conté els cognoms del pacient ingressat i el número d'habitació.

En aquest punt, escau indicar que, el tractament de la dada personal referida al número d'historial clínic d'un pacient, amb la finalitat d'efectuar un control d'accés a les instal·lacions d'un centre sanitari, certament podria constituir una actuació contrària al principi de minimització de dades personals, en els termes recollits per l'article 5.1.c RGPD ("los datos personales serán: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»"). Tanmateix, en aquest cas, a banda de les afirmacions de la denunciant, no es disposa de cap indici o prova documental, que permeti constatar que, efectivament, el personal que realitza els controls d'accessos tracta dades personals excessives en l'exercici de les seves funcions. Al seu torn, la FHSJDM ha negat aquest extrem, i ha especificat que la informació que conté aquest document és únicament els números d'habitacions i els cognoms dels pacients ingressats. En conseqüència, aquesta Autoritat no té cap element per qüestionar la veracitat de les afirmacions de l'entitat imputada, referides a la informació que conté el llistat que empra el personal de l'empresa IMAN SEGURIDAD S.A.

Pel que aquí interessa, el centre sanitari gestionat per la FHSJDM acull i presta atenció sanitària (urgències, hospitalització i atenció primària, entre d'altra) a persones que, en ocasions, a causa del seu estat de salut, poden presentar vulnerabilitat. Aquesta circumstància, entre d'altres, justifica que s'adoptin mesures destinades a protegir-les.

Quant al marc normatiu d'aplicació, escau assenyalar que l'RGPD disposa que qualsevol tractament de dades personals ha de ser lícit, lleial i transparent en relació amb la persona interessada (article 5.1.a). En aquest sentit, estableix un sistema de legitimació del tractament de dades que es fonamenta en la necessitat que hi concorri alguna de les bases jurídiques establertes al seu article 6.1. Entre d'altres supòsits, legitima el tractament "necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento" (6.1.c), o bé "para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" (6.1.e), i cal que una norma amb rang de llei l'habiliti, d'acord amb l'article 6.3 de l'RGPD i l'article 8 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

Dit això, el fet que les persones que accedeixen a un hospital hagin de comunicar el seu nom i cognoms al personal que controla l'accés –o, fins i tot, exhibir el seu DNI–, així com indicar a quin pacient volen visitar, no sembla que pugui excedir les expectatives de privacitat de les persones acompanyants d'una persona usuària dels serveis de l'hospital. De fet, la finalitat del document nacional d'identitat és principalment policial i administrativa (art. 9 i ss de la Llei orgànica 1/1992, de 21 de febrer, de seguretat ciutadana, i Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques), i són moltes les institucions que requereixen que les persones que accedeixen a les seves immediacions s'identifiquin, per raons de seguretat.

El fet que el personal de seguretat de l'empresa Iman SA custodii dades personals de pacients – en concret, els cognoms i el número d'habitació on es troben ingressats - tampoc no constitueix una infracció de la normativa de protecció de dades, atès que

actua per compte de la FHSJDM i, per tant, el tractament denunciat no constitueix cap comunicació de dades personals il·lícita a tercers. En aquest sentit, l'article 33 de l'LOPDGDD estableix que "el acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos (...)."

Per altra banda, escau assenyalar que l'FHSJDM ha de vetllar per la seguretat i salut dels seus pacients i dels acompanyants, així com del seu personal. Així ho estableix l'article 14.2 la Llei 31/1995, de 8 de novembre, de prevenció de riscos laborals (PRL), quan disposa el següent (la negreta és de l'Autoritat):

"En compliment del deure de protecció, l'empresari haurà de garantir la seguretat i la salut dels treballadors al seu servei en tots els aspectes relacionats amb la feina. A aquests efectes, en el marc de les seves responsabilitats, l'empresari realitzarà la prevenció dels riscos laborals **mitjançant la integració de l'activitat preventiva** a l'empresa i l'adopció de les mesures que siguin necessàries per a la protecció de la seguretat i la salut dels treballadors, amb les especialitats que es recullen en els articles següents en matèria de pla de prevenció de riscos laborals, avaluació de riscos, informació, consulta i participació i formació dels treballadors, actuació en casos d'emergència i de risc greu i imminent, vigilància de la salut, i mitjançant la constitució d'una organització i dels mitjans necessaris en els termes establerts en el capítol IV d'aquesta llei.

L'empresari desenvoluparà una acció permanent de seguiment de l'activitat preventiva amb la finalitat de perfeccionar de manera continuada les activitats d'identificació, avaluació i control dels riscos que no s'hagin pogut evitar i els nivells de protecció existents, i disposarà el que sigui necessari per a l'adaptació de les mesures de prevenció assenyalades en el paràgraf anterior a les modificacions que puguin experimentar les circumstàncies que incideixin en la realització de la feina."

Al seu torn, la regulació del dret a la protecció de la salut, prevista a l'article 43 de la Constitució espanyola, també ha estat desenvolupada per diferents normatives, entre les quals la regulació bàsica en l'àmbit estatal, per mitjà de la Llei 14/1986, de 25 d'abril, general de sanitat. Aquesta norma preveu a l'article 11 l'obligació de la ciutadania de complir les prescripcions generals de naturalesa sanitària comunes a tota la població, així com les específiques determinades pels serveis sanitaris.

També la Llei 15/1990, de 9 de juliol, d'ordenació sanitària de Catalunya, manté el màxim respecte a la dignitat de la persona i a la llibertat individual, i declara que l'organització sanitària catalana ha de permetre garantir la salut com a dret inalienable de la població.

En aquest punt escau assenyalar que, per mitjà de l'Ordre SND/726/2023, de 4 de juliol, es va publicar l'Acord del Consell de Ministres de 4 de juliol de 2023, pel qual es va declarar la finalització de la situació de crisi sanitària ocasionada per la COVID-19. Tanmateix, en aquest cas, l'entitat denunciada ha justificat la necessitat de controlar els accessos a l'hospital a causa de la incidència de la covid, però també per raons de seguretat i salut pública, en general. Respecte d'això, tot seguit s'analitza la proporcionalitat d'aquesta mesura.

En efecte, d'acord amb jurisprudència reiterada (per totes, STC 66/1995), l'anàlisi del compliment del principi de proporcionalitat d'una determinada mesura, que limita el dret a

la protecció de dades personals, requereix superar el que s'anomena test de proporcionalitat:

- a) Ha de ser idònia. És a dir, ha de ser apta per assolir el resultat pretès.
- b) Ha de ser necessària. Per això, cal valorar si hi ha altres opcions menys intrusives o més moderades per assolir la finalitat perseguida.
- c) Cal dur a terme una anàlisi de la proporcionalitat en sentit estricte. En concret, s'ha de valorar si de la mesura que s'adopti se'n deriven més beneficis per l'interès general, que perjudicis sobre altres béns jurídics o valors en conflicte.

D'entrada, des del punt de vista de la idoneïtat de la mesura, és evident que la identificació de les persones que accedeixen a un hospital permet al personal de seguretat d'un hospital conèixer en tot moment qui hi ha a les seves instal·lacions. Aquesta informació pot ser del tot rellevant per tal d'identificar les persones que acompanyen un pacient; controlar els aforaments; fer seguiment d'eventuals incidències; identificar l'acompanyant d'un pacient en cas de restricció de visites; entre d'altres.

La mesura també es pot considerar necessària atès que, si bé actualment ja no ens trobem en un context de pandèmia sanitària, el control d'accessos representa un mecanisme idoni per contribuir a preservar la salut pública i la seguretat.

Finalment, la mesura també es pot considerar justificada des del punt de vista de la proporcionalitat, en sentit estricte, si se n'analitzen els costos i els beneficis. En efecte, la intrusió que comporta accedir a informació identificativa –tant d'un acompanyant com d'un pacient– no és significativa i reporta un benefici important, quant al control de la seguretat i de la sanitat. Tot això tenint en compte, a més, l'autonomia i la capacitat organitzativa dels centres sanitaris quant a les seves instal·lacions.

Per tot això, es considera que el tractament de dades personals denunciat, referit als cognoms i número d'habitació dels pacients ingressats, que es duu a terme en el control d'accés de l'hospital, està emparat per l'article 6.1.c i e de l'RGPD, en connexió amb la normativa sanitària i de prevenció de riscos laborals.

## 2.2. Sobre l'eventual manca de mesures de seguretat

Tot seguit, la persona denunciant indicava que el personal que fa els controls d'accessos no adopta les mesures de seguretat adequades per protegir les dades personals dels pacients, de manera que, sovint, el llistat que conté la identificació dels pacients i el número d'habitació queda a l'abast de qualsevol persona.

En resposta a aquesta afirmació, la FHSJDM ha aportat el contracte d'encarregat del tractament celebrat amb l'empresa que presta el servei de seguretat (Iman SA) i ha afirmat que, per garantir la màxima seguretat i confidencialitat de les dades, el personal que efectua aquests controls en cap moment deixa el llistat a la vista. Reforça la idea anterior el fet que, en cas d'absència temporal, "l'auxiliar s'enduu el llistat o el guarda en un lloc segur", com ara un armari tancat amb clau.

Des d'un enfocament basat en la prevenció del risc, l'article 25 de l'RGPD estableix que les dades personals s'han de protegir des del disseny i per defecte. I, al seu torn, l'article



32 de l'RGPD disposa que tant el responsable com l'encarregat del tractament han d'aplicar mesures tècniques i organitzatives adequades per garantir un nivell de seguretat adequat al risc.

Doncs bé, l'entitat denunciada ha remarcat que el personal que controla els accessos segueix un protocol rigorós respecte de les dades personals que consten en l'esmentat llistat (antecedent 5è). També ha acreditat que disposa d'un acord d'encàrrec del tractament, que preveu les mesures de seguretat que Iman SA adopta en la prestació del servei contractat. Així, la FHSJDM ha destacat que el llistat roman protegit en tot moment enfront d'eventuals accessos no autoritzats.

En aquest punt, a banda de les afirmacions de la persona denunciant, no es disposa de cap altre indicatiu que permeti sostenir que aquest llistat ha romàs accessible per terceres persones.

Cal tenir en consideració que el procediment administratiu sancionador és especialment garant, per raó de les conseqüències que se'n poden derivar. Per això, per incoar-lo cal que hi hagi prou elements probatoris o indicis racionals que permetin imputar la comissió d'una infracció a l'entitat denunciada. Elements que no concorren en el cas que s'examina. A més, també resulten d'aplicació, amb alguna matisació però sense excepcions, els principis inspiradors de l'ordre penal. Així, resulta clara la plena virtualitat dels principis de presumpció d'innocència i *in dubio pro reo* en l'àmbit de la potestat sancionadora, que desplaça a qui acusa la càrrega de provar els fets i la seva autoria. En aquest sentit, l'article 53.2.b de l'LPAC reconeix el dret "a la presumpció de no-existència de responsabilitat administrativa mentre no es demostri el contrari."

D'acord amb l'exposat, amb base al dret a la presumpció de no existència de responsabilitat administrativa mentre no es demostri el contrari, escau arxivar aquestes actuacions.

3. L'article 10.2 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, preveu que "(...) no es formularà plec de càrrecs i s'ordenarà el sobreseïment de l'expedient i l'arxiu de les actuacions quan de les diligències i de les proves practicades, en resulti acreditada la inexistència d'infracció o responsabilitat. Aquesta resolució es notificarà als interessats". I l'article 20.1 del mateix decret determina que escau el sobreseïment: "c) Quan no s'ha acreditat l'existència de responsabilitat, o bé s'ha produït l'extinció d'aquesta."

De conformitat amb tot el que s'ha exposat en el fonament de dret 2n, i atès que durant les actuacions dutes a terme en el marc de la informació prèvia no s'ha acreditat cap fet que pugui ser constitutiu d'alguna de les infraccions previstes a la legislació sobre protecció de dades, escau acordar-ne l'arxivament.

## Resolució

Per tant, resolc:

1. Arxivar les actuacions d'informació prèvia número IP 635/2023, relatives a la Fundació Hospital Sant Joan de Déu de Martorell, ja que no s'ha constatat que s'hagi produït cap

actuació que pugui ser constitutiva d'alguna de les infraccions previstes a la legislació sobre protecció de dades.

2. Notificar aquesta resolució a la Fundació Hospital Sant Joan de Déu de Martorell i a la persona denunciant.
3. Ordenar que la resolució es publiqui al web de l'Autoritat ([apdcat.gencat.cat](http://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 les persones interessades poden 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 la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Igualment, les persones interessades poden interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora