Identificació de l'expedient

Resolució del procediment sancionador núm. PS 4/2024, referent a la Fundació de Recerca Clínic Barcelona-Institut d'Investigacions Biomèdiques August Pi i Sunyer.

Antecedents

1. En data 05/03/2023 l'Hospital Clínic de Barcelona (HCB) va detectar haver patit un atac amb programari de segrest (*ransomware*) a la plataforma corporativa de virtualització de l'hospital, que afectava els sistemes d'informació del propi HCB i també els de les entitats vinculades - la Fundació de Recerca Clínic Barcelona-Institut d'Investigacions Biomèdiques August Pi i Sunyer (FRCB-IDIBAPS), el Consorci d'Atenció Primària de Salut Barcelona Esquerra (CAPSBE) i Barnaclínic S.A - que s'hi allotjaven.

El mateix dia 05/03/2023, l'HCB va notificar el ciberatac patit a l'Agència de Ciberseguretat de Catalunya, (Catalonia-CERT), com a centre de resposta d'incidents de ciberseguretat, i se'n va fer difusió als mitjans de comunicació. L'endemà dia 06/03/2023, l'HCB va notificar a l'Autoritat Catalana de Protecció de Dades (APDCAT) la violació de la seguretat de les dades que havia patit (...).

(...) Així doncs, l'encriptació de dades va implicar la indisponibilitat (impossibilitat d'accés) dels sistemes d'informació que suporten la gran majoria de processos de l'HCB i de la Fundació. Això va suposar una interrupció del normal funcionament de l'entitat, en tant que els seus sistemes d'informació allotjats a la plataforma atacada van quedar també encriptats.

A més, l'atacant va aconseguir exfiltrar (robar) prop de 4 TB de dades relatives a persones treballadores i a milers de pacients que estaven emmagatzemades als entorns virtuals atacats (...); l'exfiltració afectava també els tractaments de dades de les entitats vinculades, que posteriorment es van publicar al web fosc (*dark web*). Entre d'altra informació, les dades personals compromeses incloïen la relativa a estudis clínics, així com dades relatives a persones treballadores.

2. En compliment dels poders atribuïts a l'Autoritat Catalana de Protecció de Dades, per l'article 58.1 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 dades (RGPD) i l'article 19 de la Llei 32/2010, d'1 d'octubre de l'Autoritat Catalana de Protecció de Dades, i d'acord amb les competències atribuïdes, l'APDCAT va obrir un expedient informatiu contra l'HCB (IP 213/2023) i les entitats vinculades, entre aquestes, la FRCB-IDIBAPS (IP núm. 216/2023) amb la finalitat d'esbrinar les circumstàncies dels fets. En concret, per esbrinar si l'HCB i les entitats, en la seva condició de responsables o d'encarregades del tractament, abans de patir l'atac tenien implementades les mesures de seguretat (tècniques i organitzatives) apropiades per garantir un nivell de seguretat adequat al risc del tractament de les dades que duien a terme a la plataforma corporativa atacada, tenint en compte el seu volum i la categoria de dades objecte de tractament i, consegüentment, la conveniència d'iniciar o no un procediment sancionador.

En el marc d'aquesta informació prèvia, es van incorporar a l'expedient les actuacions dutes a terme en la instrucció de la violació de la seguretat de les dades (NVS), així com tota la informació recopilada de les publicacions i comunicats de premsa sobre l'incident.

3. Així mateix, en el marc de la IP 216/2023, en data 27/04/2023 es va requerir la Fundació que:

3.1 Aportés còpia del document de política de seguretat aprovat pel centre.

3.2 Identifiqués la categoria del sistema d'informació afectat per l'atac, d'acord amb la categorització establerta a l'Esquema Nacional de Seguretat (ENS). També, que informés sobre el procediment d'avaluació que va conduir a aquesta conclusió, on constessin els nivells màxims relatius a les diferents dimensions de seguretat.

3.3 Indiqués les mesures tècniques i organitzatives que resulten aplicables/exigibles per garantir un nivell de seguretat adequat al risc que comporta el tractament de les dades afectades per l'atac (per protegir les dades i minimitzar-ne els riscos derivats), que ha d'incloure, en tot cas, les que corresponguin d'acord amb l'annex II de l'ENS. També, les que derivin de l'anàlisi de riscos preceptiva i de les avaluacions d'impacte que corresponguin.

3.4 Indiqués el grau de maduresa d'implementació de les mesures que s'haguessin identificat en la resposta al punt anterior. Així mateix, se sol·licitava còpia del pla de millora.

3.5 Aportés còpia del procediment de gestió d'incidents de ciberseguretat i del Pla de continuïtat, amb indicació de les proves de restauració que s'haguessin dut a terme durant els dos anys anteriors a l'incident (quan es van dur a terme, qui les va realitzar i en què van consistir).

3.6 Aportés còpia de l'anàlisi forense sobre l'incident de ciberseguretat, que recollís entre d'altres, els aspectes següents:

(i) Abast d'afectació (servidors i bases de dades compromeses).

(ii) Mètode d'infiltració del codi maliciós (com es va perpetrar l'atac).

(iii) Com es va propagar el codi maliciós.

(iv) Quan i de quina manera es va tenir coneixement de l'atac.

(v) Mesures adoptades com a reacció davant l'atac. Si es va seguir un protocol específic, identifiqués quin.

4. En data 02/06/2023, la Fundació, va respondre el requeriment amb un escrit en què, en primer terme, exposava el següent:

- "Que, la informació requerida està relacionada amb l'atac amb programari de segrest que ha afectat als sistemes d'informació de l'Hospital Clínic de Barcelona (en endavant "HCB") i de les entitats que hi estem vinculades, entre aquestes la FRCB-IDIBAPS."

- "Que la FRCB-IDIBAPS no disposa d'un sistema d'informació propi i comparteix el sistema d'informació de l'HCB, gestionat per la Direcció de Sistemes d'Informació de l'HCB (en endavant, la "DSI")."

- "Que, en conseqüència, vaig traslladar a la DSI el requeriment rebut i ha estat necessari esperar a la investigació forense i a la recopilació d'informació per part de la DSI per poder donar resposta al requeriment d'aquesta Autoritat."

  A continuació, la FRCB-IDIBAPS, donava resposta a cadascuna de les peticions efectuades per l'APDCAT, en el sentit següent:

  (...)

- A l'últim, en resposta al punt 3.6, referent a l'anàlisi forense sobre l'incident patit, la FRCB-IDIBAPS manifestava que "ens remetem a l'aportat per l'HCB a aquesta Autoritat", i en aquest sentit afegia que "l'Agència de Ciberseguretat de Catalunya, ha considerat que aquest document és extremadament sensible i no es pot distribuir fora de la DSI".

5. En data 31/07/2023, l'Autoritat va efectuar un segon requeriment d'informació a la FRCB-IDIBAPS, en què es demanava que aportés còpia de l'acord o contracte que regulés els tractaments de dades que duia a terme l'HCB per a la prestació dels serveis encomanats, a què es feia referència en l'escrit de resposta al primer requeriment, en els termes establerts a l'article 28 de l'RGPD.

6. En data 01/08/2023, la FRCB-IDIBAPS va complir aquest requeriment per mitjà d'un escrit, amb el qual acompanya còpia de "l'acord multilateral d'encarregat de tractament" sol·licitat, en concret, "l'Acord multilateral de prestació de serveis entre entitats amb accés a dades personals" de data 06/04/2022, signat entre l'HCB, la FRCB-IDIBAPS i altres entitats del Campus Clínic".

7. En data 18/01/2024, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer per tres presumptes infraccions: una infracció prevista a l'article 83.4.*a,* en relació amb l'article 32.1; una altra infracció prevista a l'article 83.4.*a,* en relació amb l'article 32.2; i una tercera infracció prevista a l'article 83.4.*a,* en relació amb l'article 28; 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 dades (RGPD). Aquest acord d'iniciació es va notificar a l'entitat imputada en data 22/01/2024.

En la mateixa data, la directora de l'Autoritat va acordar iniciar un procediment sancionador contra l'Hospital Clínic de Barcelona (PS núm. 1/2024), contra el Consorci d'Atenció Primària de Salut Barcelona Esquerra (PS núm. 2/2024) i contra Barnaclínic S.A (PS núm. 3/2024).

8. 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.

9. En data 26/01/2024 la Fundació va sol·licitar l'ampliació del termini atorgat per formular al·legacions, a l'empara de l'article 32 LPAC.

10. En data 29/01/2024 l'Autoritat va acordar ampliar el termini per presentar al·legacions per cinc dies més.

11. En data 12/02/2024, la FRCB-IDIBAPS va formular al·legacions a l'acord d'iniciació, que s'aborden als apartats 5è i 6è dels fonaments de dret i va sol·licitar l'acumulació dels procediments sancionadors núm. PS 2/2024, 3/2024 i 4/2024.

Adjunt al seu escrit d'al·legacions, aportava la informació següent:

11.1 Extractes d'actes del Comitè de Protecció de Dades, de dates 05/03/2019, 29/11/2019, 08/11/2022, 05/03/2019 i 15/03/2023.

11.2 Certificat conforme el Consorci Hospital Clínic de Barcelona és una entitat adherida al codi tipus, expedit per la Unió Catalana d'Hospitals.

11.3 Correus electrònics intercanviats entre la DSI i la Direcció de Persones de l'HCB els anys 2021 i 2022, sobre (...).

11.4 Evidències (...) i mesures actuals de seguretat.

11.5 Mesures de detecció i prevenció implementades abans de l'incident.

11.6 Informe de context previ a l'incident de *ransomware* de la Secretaria de Telecomunicacions i Transformació Digital del Departament de la Presidència.

11.7 Pla de conscienciació i formació en ciberseguretat 2022-2023 de l'HCB.

11.8 Informe sobre l'impacte assistencial del ciberatac patit per l'Hospital Clínic elaborat pel Director Assistencial de l'HCB.

11.9 Relat (...).

11.10 Informe de conclusions realitzat per l'Agència de Ciberseguretat.

11.11 Auditories en ciberseguretat.

11.12 Mesures aplicades després de l'atac.

11.13 Avaluacions d'impacte en protecció de dades (AIPDs).

11.14 Metodologia interna d'AIPDs.

12. En data 21/02/2024 l'Autoritat va descartar l'acumulació de procediments sol·licitada, amb base als motius que s'exposen al fonament de dret 5è.

13. Atenent a les al·legacions i documentació aportada per l'entitat, s'incorporen a l'expedient els informes emesos des de l'Àrea de Tecnologia i Seguretat de la Informació d'aquesta Autoritat en data 12/04/2024 i 29/04/2024, en el marc del procediment

sancionador núm. 1/2024 contra l'HCB. Aquests informes analitzen tota la documentació que va aportar l'HCB per defensar la pertinença de les mesures tècniques i organitzatives que tenia implementades, en el moment del ciberatac. Així mateix, també s'incorpora a l'expedient el Document número 18 de l'Agència de Ciberseguretat de Catalunya, aportat al PS núm. 1/2024.

Pel que fa a les anàlisis de l'Àrea de Tecnologia i Seguretat de la Informació d'aquesta Autoritat, destaca la conclusió de l'Informe de data 12/04/2024 que, en termes literals, estableix el següent:

> "(...) En definitiva, d'acord amb l'estat de la tècnica en el moment en què els sistemes d'informació de l'HCB van ser ciberatacats, i en atenció als tractaments de dades personals que l'entitat duia a terme, escau concloure que les mesures tècniques i organitzatives implementades no eren adequades per garantir el nivell de seguretat que els riscos associats a la informació allotjada en els servidors atacat exigia. I, vinculat amb l'anterior, escau fer notar que, difícilment l'HCB podia implementar mesures adequades als riscos existents tenint en compte que no ha ni aportat evidències d'haver-los documentat adequadament."

14. En data 24/05/2024, la persona instructora d'aquest procediment va formular una proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades declarés que la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer havia incorregut, en primer lloc, en una infracció prevista a l'article 83.4.*a* en relació amb l'article 32.1; en segon lloc, en una infracció prevista a l'article 83.4.*a* en relació amb l'article 32.2; i, en tercer lloc, en una infracció prevista a l'article 83.4.*a* en relació amb l'article 28, tots ells de l'RGPD.

Aquesta proposta de resolució es va notificar en data 03/06/2024 i es concedia un termini de 10 dies per formular al·legacions.

15. En data 04/06/2024 la FRCB-IDIBAPS va sol·licitar l'ampliació del termini atorgat per formular al·legacions, a l'empara de l'article 32 de l'LPAC.

16. En data 07/06/2024 l'Autoritat va acordar l'ampliació sol·licitada.

17. En data 25/06/2024 l'entitat imputada va presentar un escrit d'al·legacions a la proposta de resolució, que s'aborden al fonament de dret 5è d'aquesta resolució.

Fets provats

1. La FRCB-IDIBAPS té allotjades les seves dades als sistemes d'informació de l'HCB, el qual li presta serveis informàtics i d'allotjament d'informació, en condició d'encarregat del tractament.

La FRCB-IDIBAPS, en la seva condició de responsable del tractament, amb anterioritat al ciberatac, no va determinar quines eren les mesures necessàries per protegir les seves dades. Prova d'això és que, les mesures de seguretat que va implementar l'HCB en compliment del contracte d'encarregat del tractament van resultar ser insuficients, ja que d'acord amb la documentació aportada, ni tant sols complien les mesures (...).

D'acord amb la normativa de protecció de dades, el responsable del tractament ha d'actuar amb diligència en relació amb els encàrrecs de tractament de dades personals que efectuï a terceres persones, com és el cas, i ser especialment diligent quant a la protecció de categories especials de dades personals.

En concret, la FRCB-IDIBAPS com a responsable del tractament no va vetllar per la implementació de les mesures de seguretat, de prevenció, detecció i contenció que s'indiquen a continuació. Així, ha quedat provat que, malgrat ser unes mesures essencials per una prevenció mínima envers els ciberatacs, l'entorn de l'HCB, en l'execució del contracte d'encarregat del tractament:

- No tenia implementat (....) ni un (...).
- No tenia degudament implementat un sistema (...).
- No tenia degudament implementades mesures de (...).
- No s'ha acreditat que s'haguessin dut a terme programes de (...).
- No disposava de (...).

D'acord amb la normativa de protecció de dades, el responsable del tractament ha d'actuar amb diligència en relació amb els encàrrecs de tractament de dades personals que efectuï a terceres persones, com és el cas, i ser especialment diligent quant a la protecció de categories especials de dades personals.

2. L'entitat FRCB – IDIBAPS no va realitzar la corresponent anàlisi de riscos, per definir les mesures de seguretat aplicables al tractament de les dades que van ser objecte del ciberatac.

En aquest sentit, s'havien de dur a terme dues anàlisi de riscos. D'una banda, l'HCB – com a encarregat del tractament – havia de realitzar la pertinent anàlisi de riscos, en el context de l'encàrrec efectuat. I, d'altra banda, el responsable del tractament (la FRCB-IDIBAPS) havia d'efectuar la seva anàlisi de riscos, respecte les dades que tractava, per tal de determinar les condicions de l'encàrrec i complir amb les seves obligacions com a responsable.

3. L'entitat FRCB – IDIBAPS i l'HCB disposaven d'un "acord multilateral de prestació de serveis entre entitats amb accés a dades personals", de data 06/04/2022. Una vegada analitzat el seu contingut es desprèn que no disposa dels elements necessaris bàsics d'un contracte d'encarregat del tractament d'acord amb l'establert a l'article 28 de l'RGPD. En aquest sentit, cal tenir en compte que en l'acord aportat per l'entitat, no es regula la relació entre el responsable del tractament, la FRCB-IDIBAPS, i l'encarregat del tractament, l'HCB, per a la prestació de serveis informàtics i allotjament d'informació, ni s'identifiquen els tractaments de dades que ha de dur a terme l'encarregat del tractament, és a dir, l'HCB, per compte de la FRCB-IDIBAPS, per a la prestació de l'esmentat servei.

En definitiva, la FRCB-IDIBAPS, no hauria articulat ni els mecanismes formals adequats, ni tampoc els materials (revisió sistemàtica de les condicions dels tractaments objecte d'encàrrec) mínims necessaris per tal d'assegurar un adequat tractament i la seguretat de la seva informació. Mecanismes que haurien hagut

d'incloure les exigències de seguretat corresponents i les garanties per a l'adequat compliment i satisfacció d'aquestes exigències, en funció de les dades que eren objecte de tractament.

La qualificació jurídica d'aquests fets provats, no ha quedat desvirtuada per les al·legacions que ha presentat la FRCB-IDIBAPS, tant a l'acord d'iniciació com a la proposta de resolució d'aquest procediment, tal com s'analitzarà amb detall als fonaments de dret 5è i 6è d'aquesta resolució.

Fonaments de dret

1. Competència

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. Marc normatiu aplicable

- Reglament (UE) 2016/679 del Parlament europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).
- Esquema Nacional de Seguretat, aprovat pel Reial decret 3/2010, de 8 de gener (ENS 2010).

3. Contextualització del ciberatac

Tal com s'assenyalava a la proposta de resolució, abans d'entrar a valorar l'escrit d'al·legacions que ha presentat la FRCB-IDIBAPS al llarg d'aquet procediment, escau fer una referència a les circumstàncies en què va tenir lloc el ciberatac als sistemes d'informació de l'HCB, així com a l'exigència legalment requerida en termes de seguretat de la informació l'any 2023.

Els documents aportats per la FRCB-IDIBAPS, així com la informació incorporada en aquest procediment sancionador, permet constatar que, (...).

(...) Aquest atac va comprometre dades personals en relació amb les quals la FRCB-IDIBAPS n'era la responsable del tractament i l'HCB l'encarregat. (...)

En efecte, l'incident esmentat va afectar la confidencialitat d'un volum ingent de dades personals de treballadors; dades identificatives i de salut de pacients; i dades d'entitats col·laboradores i proveïdors, entre d'altra informació. Aquest fet és especialment rellevant tenint en compte el nombre de terceres persones afectades, i la sensibilitat de la informació compromesa. En efecte, l'article 9 de l'RGPD estableix que les categories especials de dades personals – com ho són, les dades de salut – són mereixedores d'una especial protecció davant eventuals riscos i amenaces.

Una vegada establert l'anterior, per definir i implementar les mesures tècniques i organitzatives apropiades calia que, prèviament, la FRCB-IDIBAPS hagués identificat les amenaces i els riscos existents en relació amb els diferents tractaments de dades personals que duia a terme. Així, en funció dels resultats d'aquesta anàlisi, hagués pogut concretar la implementació de les mesures necessàries en cada supòsit, per preservar la seguretat de la informació i, en darrera instància, els drets i llibertats dels titulars de les dades. Aquesta és una obligació que deriva de l'article 32 RGPD, però també del principi de responsabilitat proactiva, d'acord amb el qual el responsable del tractament ha de poder demostrar que els tractaments de dades que duu a terme són conformes al Reglament (art. 5.2 RGPD). En termes pràctics, cal que les persones implicades en el tractament de dades personals tinguin una actitud conscient, diligent i proactiva quant a la seguretat de la informació.

Tanmateix, tal com s'exposarà amb més detall als apartats 5.4 i 6.2 d'aquesta resolució, la FRCB-IDIBAPS, en la seva condició de responsable del tractament, no ha acreditat haver analitzat els riscos que s'associaven al tractament de les diferents tipologies de dades personals, pel que difícilment podia definir i implementar mesures tècniques i organitzatives adequades, en relació amb les amenaces existents.

Per altra banda, la cronologia dels fets exposats evidencia que les mesures que l'HCB va implementar, com a encarregat del tractament per compte de la Fundació, no van poder detectar ni l'atac ni la intrusió de l'atacant als seus sistemes d'informació fins al cap de (...) i que, pel que fa a les mesures de prevenció, aquestes no van resultar suficients per evitar la materialització de l'atac. En aquest punt, escau avançar que, malgrat que l'obligació d'adoptar mesures de seguretat constitueixi una obligació de mitjans – i no de resultats – el cert és que l'article 32.1 RGPD exigeix que aquestes mesures siguin tècnicament adequades i que s'implementin amb una diligència raonable.

Pel que fa a la implementació de mesures de seguretat, al llarg d'aquest procediment sancionador s'han fet nombroses referències a l'ENS 2010 malgrat que l'ENS 2022 (aprovat pel Reial Decret 311/2022, de 3 de maig) – que estableix majors exigències en termes tecnològics – ja havia entrat en vigor. De fet, es pren com a referència l'ENS 2010, atès que la disposició transitòria única de l'ENS 2022, preveu un termini de 24 mesos perquè els sistemes d'informació del seu àmbit d'aplicació – com ho són els de l'HCB – s'adeqüin plenament al nou esquema nacional de seguretat.

Establert l'anterior, cal fer avinent que l'ENS 2010 estableix un llistat de mesures necessàries per protegir els sistemes, les dades, les comunicacions, i els servies electrònics. En aquest sentit, com més alt sigui el nivell de risc al qual s'afronta un sistema d'informació ("categoria del sistema") més gran serà l'exigència d'implementar les mesures que preveu el mateix ENS. Per tant, en funció de la "categorització" del sistema d'informació (bàsica, mitjana o alta) hi ha mesures que poden esdevenir d'implementació obligatòria atesos els beneficis globals que aporten quant a la gestió o securització d'un sistema d'informació concret. En canvi, d'altres poden ser obligatòries només pel que fa a aspectes o dimensions de seguretat concretes. En qualsevol cas, per determinar amb precisió l'exigència requerida en termes de seguretat, cal determinar el nivell del risc corresponent a les diferents dimensions de seguretat de les informacions que discorrien pel sistema de l'HCB, així com al nivell de risc associat a la pèrdua de disponibilitat dels serveis que s'ofereixen a partir de la plataforma esmentada.

Al fil de l'anterior, tenint en compte, entre d'altres factors, la sensibilitat de les dades que emmagatzemava la plataforma corporativa de l'HCB, que va ser atacada; la repercussió d'un eventual incident de seguretat per als drets i llibertats de les persones afectades; l'impacte organitzatiu d'una fallada de seguretat i les amenaces i riscos associats als tractaments de

dades personals, les mesures exigibles correspondrien a les previstes en relació amb una categorització mitjana, d'acord amb l'ENS 2010. Reforça aquest punt el fet que l'informe "Perfil Compliment Específic per Salut", elaborat pel Centre Criptològic Nacional i publicat l'any 2024 – i, per tant després del ciberatac- estableix que la situació desitjable, quant a la seguretat de la informació, és que les organitzacions sanitàries assumeixin el compromís d'elevar les seves mesures de seguretat per damunt de les exigències associades a la categorització mitjana. En qualsevol cas, la FRCB-IDIBAPS no ha qüestionat que el mínim exigible fos la categorització mitjana d'acord amb l'ENS, d'acord amb la qual s'ha basat aquesta resolució.

Arribats en aquest punt, escau tenir present que l'ENS 2010 concreta una obligació més genèrica, que és la prevista a l'article 32 de l'RGPD. En termes literals aquest precepte disposa el següent:

> "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.
> (…)"

D'aquest article s'infereix que l'obligació d'adoptar mesures tècniques i organitzatives té una vocació dinàmica i que exigeix que es respecti el principi de proporcionalitat. És a dir, per una banda, cal que els responsables i encarregats del tractament adoptin en cada moment les mesures suficients per protegir les dades que tracten. I, per altra banda, cal que la implementació d'aquestes mesures respecti el principi de proporcionalitat i s'adeqüin a l'estat de la tècnica.

D'acord amb les Directrius 4/2019, relatives a l'article 25 RGPD, del Comitè Europeu de Protecció de Dades (CEPD) es defineix el concepte "estat de la tècnica" en el context de l'article 25 RGPD, de la manera següent (la negreta és de l'Autoritat):

> "**El «estado de la técnica» es un concepto dinámico que no puede definirse de manera estática en un momento determinado, sino que debe evaluarse de manera continua en el contexto del progreso tecnológico.** Frente a los avances tecnológicos, un responsable del tratamiento podría considerar que una medida que proporcionaba un nivel adecuado de protección ya no lo hace. Por consiguiente, desatender la obligación de mantenerse al día de los cambios tecnológicos podría dar lugar al incumplimiento del artículo 25.

El criterio del «estado de la técnica» no solo se aplica a las medidas tecnológicas, sino también a las de carácter organizativo. La falta de medidas organizativas adecuadas puede reducir o incluso restar toda efectividad a la tecnología elegida. Ejemplos de medidas organizativas pueden ser la adopción de políticas internas, la formación de reciclaje tecnológico, la seguridad y protección de datos, y las políticas de gobernanza y gestión de la seguridad de TI.
Los marcos, normas, certificados, códigos de conducta, etcétera, existentes y reconocidos en distintos ámbitos, pueden servir para indicar el «estado de la técnica» actual en un ámbito de uso concreto. Cuando tales normas ya existan y confieran un elevado nivel de protección al interesado de modo que se cumplan —o se excedan— los requisitos legales, **los responsables del tratamiento deberán tenerlas en cuenta en la concepción y aplicación de las medidas de protección de datos."**

En efecte, l'estat de la tècnica exigeix que es revisin les mesures de seguretat que són adequades en cada moment i, per això, es poden prendre de referència codis de conducta i marcs normatius existents i reconeguts – com ho és l'Esquema Nacional de Seguretat-.

Doncs bé, els fonaments de dret 5è i 6è d'aquesta resolució desenvoluparan amb més detall els motius pels quals escau concloure que la FRCB-IDIBAPS no havia realitzat l'anàlisi de riscos, respecte els tractaments dels què n'era responsable; no havia definit les mesures tècniques i organitzatives per protegir la informació esmentada; i no havia celebrat un contracte d'encarregat del tractament que recollís els extrems previstos per la normativa de protecció de dades personals.

En darrer terme, escau assenyalar que les referències a l'ENS responen a una doble consideració: a) d'una banda, a l'obligatorietat d'implementar-les, que es deriva del marc normatiu aplicable; i b) d'altra banda, la seva configuració com a paràmetre de referència envers les mesures tècniques i organitzatives necessàries a implementar en els sistemes d'informació.

4. Consideracions prèvies sobre l'actuació de l'HCB i la FRCB-IDIBAPS arran del ciberatac.

L'HCB i les Entitats vinculades presten serveis de salut referents a Catalunya i al món, amb una clara voluntat d'excel·lència en les seves principals àrees d'acció. En aquest sentit, cal reconèixer que les seves tasques ordinàries requereixen activitats de tractament de dades personals especialment complexes i extenses, tenint en compte entre d'altres aspectes, el volum de dades personals compromeses; les persones implicades; la sensibilitat de la informació i els diferents àmbits de treball.

En aquest punt, escau fer notar que el ciberatac va tenir lloc en un moment de recuperació dels efectes ocasionats per la Covid-19 i que, en el context de la pandèmia sanitària, els esforços de la FRCB-IDIBAPS es van centrar en el desenvolupament de la vacuna (...) i, per tant, en investigar exhaustivament la malaltia. En aquestes circumstàncies, l'Autoritat no pot desconèixer els esforços ingents del personal de la Fundació, centrats en la investigació de la Covid-19, i en donar suport a l'HCB.

Doncs bé, tal com s'exposarà amb més detall al fonament de dret 5è, l'Autoritat valora molt positivament les diferents mesures tècniques i organitzatives que es van adoptar, després del ciberatac, per tal de reforçar la seguretat dels sistemes d'informació, així com la celeritat amb què es van implementar. Entre d'altres actuacions destaca: (...).

Vinculat amb l'anterior, escau fer notar que aquestes noves mesures de seguretat les van implementar l'HCB i la FRCB-IDIBAPS, en les seves respectives condicions d'encarregat i de responsable del tractament de les dades personals, respecte la informació que es

trobava allotjada a la plataforma que va ser atacada. En aquest punt, cal indicar que la plataforma atacada també contenia dades personals en relació amb les quals l'HCB n'era el responsable del tractament. Tanmateix, aquesta resolució només se centrarà en valorar la responsabilitat de la Fundació en la seva condició de responsable del tractament, si bé caldrà avaluar l'actuació duta a terme per part de l'HCB, en la seva condició d'encarregat del tractament, per compte de la FRCB-IDIBAPS.

Feta l'anterior precisió, escau avançar que, la Fundació tenia l'obligació de complir amb els deures derivats de la seva condició de responsable del tractament, que exigia diligència en la supervisió del compliment de les obligacions per part de l'encarregat del tractament – l'HCB -.

Establert l'anterior, cal fer notar que, actualment, en termes de seguretat, les dades personals que són responsabilitat de la FRCB-IDIBAPS es troben en un escenari més favorable, davant eventuals intents d'intromissió il·lícita als sistemes d'informació de l'HCB. En efecte, d'acord amb la documentació aportada al llarg d'aquest procediment sancionador, es constata que, des del moment del ciberatac fins a la data d'aquesta resolució, s'han implementat mesures que en milloren la protecció.

Tanmateix, les actuacions esmentades no desvirtuen els fets que aquí s'imputen, referits a les omissions de la FRCB-IDIBAPS com a responsable del tractament, pel que fa a la manca de realització d'anàlisi de riscos, la manca d'identificació de mesures tècniques i organitzatives apropiades, i la manca de formalització d'un contracte d'encarregat del tractament, que recollís tots els extrems previstos per l'RGPD i l'LOPDGDD.

5. Anàlisi de les al·legacions

La Fundació ha formulat al·legacions tant a l'acord d'iniciació com a la proposta de resolució. Les primeres ja es van analitzar en la proposta de resolució, però tot i això es considera procedent tractar-les aquí, atès que en l'escrit d'al·legacions que ha presentat l'entitat en data 25/06/2024 es fa una remissió global al contingut de l'escrit presentat en data 12/02/2024 davant l'Autoritat (antecedent 11è). Així, tot seguit s'analitzen el conjunt d'al·legacions formulades per la FRCB-IDIBAPS.

5.1 Sobre l'acumulació dels procediments

Tal com s'exposa a l'antecedent 11è la Fundació va sol·licitar l'acumulació dels procediments sancionadors núm. 2/2024, 3/2024 i 4/2024, a l'empara de l'article 57 LPAC, incoats respectivament contra el Consorci d'Atenció Primària Barcelona Esquerra (CAPSBE), Barnaclínic S.A i aquesta Fundació.

Doncs bé, tal com s'assenyalava a la proposta de resolució, en data 21/02/2024, l'Autoritat va descartar l'acumulació dels procediments pretesa, per mitjà d'un ofici notificat a la FRCB-IDIBAPS, els arguments del qual donem per reproduïts, per mitjà del qual es concloïa que:

> "si bé els fets origen de l'expedient sancionador són els mateixos, la posició subjectiva de cadascuna de les entitats objecte dels corresponents procediments, la singularitat de cadascuna d'elles en quan a les dades personals i el tractament de les mateixes, i les actuacions individualment realitzades per cadascuna d'elles, justifiquen rebutjar l'acumulació instada, en no concórrer els requisits d'identitat substancial i íntima connexió, tal com s'ha indicat i, d'altra banda, perquè l'exercici del seu dret de defensa en el procediment sancionador, en base a l'avaluació del principi de culpabilitat i les circumstàncies concurrents en cada cas, es garanteix d'igual o millor manera amb la tramitació separada de cadascun dels procediments."

En qualsevol cas, escau fer avinent que, el fet de rebutjar l'acumulació sol·licitada en cap cas ha produït indefensió a la Fundació, ni ha afectat negativament als seus drets processals, tenint en compte que ha presentat, igualment, les al·legacions que ha considerat escaients i ha aportat la documentació que ha considerat pertinent.

En aquest sentit, el seu dret de defensa no ha patit cap reducció i, ans al contrari, la tramitació separada permet singularitzar la condició de responsable del tractament i d'encarregat del tractament envers la responsabilitat assumida, sense perjudici que l'entitat imputada ha reproduït substancialment els arguments plantejats per part de l'HCB.

En aquest punt, s'ha d'indicar que la FRCB-IDIBAPS no ha reiterat posteriorment la seva petició d'acumulació, ni ha al·legat cap vulneració dels seus drets en la tramitació posterior realitzada, el que porta a confirmar els arguments que varen conduir a l'acumulació.

5.2 Sobre el contingut del contracte d'encarregat del tractament

Respecte d'aquesta imputació, l'entitat no ha presentat noves al·legacions a la proposta de resolució. Tanmateix, sí que en va presentar davant l'acord d'iniciació, en els termes que tot seguit s'exposen.

En primer terme, la FRCB-IDIBAPS defensava haver celebrat un contracte d'encàrrec amb l'HCB, d'acord amb les previsions de la normativa de protecció de dades personals. En concret, en virtut de l'"acord multilateral de prestació de serveis entre entitats amb accés a dades personals" de data 06/04/2022 (Acord multilateral) i argumentava que en ell "es regulen totes les obligacions a què es refereixen els apartats 3 i 4 de l'article 28 de l'RGPD".

Quant al contingut d'aquest Acord multilateral la Fundació puntualitzava que, tot i que es va optar per una redacció genèrica de les clàusules, perquè fossin perdurables en el temps, aquest document regula els elements bàsics d'un contracte d'encarregat del tractament. En aquest sentit, l'entitat exposava que, la primera clàusula de l'Acord multilateral, relativa a l'objecte del contracte, defineix el rol que assumeixen les parts, "en funció de si aquestes es troben en una situació de prestar el servei o bé de demanar-lo, entenent que la part que assisteix a l'altra actuarà com a encarregat del tractament i que qui sol·liciti el servei actuarà com a responsable."

Vinculat amb l'anterior, la Fundació especificava que "tenint en compte que l'HCB proveeix dels equipaments i recursos a la resta d'Entitats vinculades, l'HCB actua com a encarregat per compte de cadascuna d'aquestes, considerades com a responsables del tractament de les dades de les seves respectives entitats."

Tot seguit, indicava que, pel que fa a la manca d'identificació dels tractaments de dades que l'encarregat ha de dur a terme, per a la prestació de serveis informàtics i allotjament d'informació, l'Acord multilateral "estableix les condicions o termes generals que han de regir en tots els serveis que s'encomanin a l'encarregat del tractament, sobre la base del llistat d'obligacions que aquest han d'assumir d'acord amb els apartats 3 i 4 de l'RGPD" i afegia que "en els expositius de l'Acord multilateral s'indica que les entitats comparteixen seu, equipaments i recursos que, en major o menor mesura queda reflectida la participació de l'HCB en els òrgans de govern de la resta d'entitats i que, a conseqüència d'aquesta vinculació, pel desenvolupament de les seves activitats i per la prestació de serveis, les parts han d'accedir a recursos de les altres." Per l'exposat, la FRCB-IDIBAPS considerava que del contingut de l'Acord es desprèn clarament que les Entitats vinculades i l'HCB comparteixen la mateixa infraestructura tecnològica on "indiscutiblement" resulta necessària la prestació de serveis informàtics i allotjament d'informació.

En darrer terme, la Fundació argumentava que, amb anterioritat al ciberatac, disposava de diferents mecanismes que li permetien supervisar les condicions del tractament que duia a terme l'HCB. Respecte d'aquests, assenyalava els següents: que l'HCB i les Entitats vinculades participaven en un Comitè de Protecció de Dades que celebrava reunions periòdicament per tractar aspectes de protecció de dades i de seguretat; o que el Consorci Hospital Clínic de Barcelona es troba adherit al Codi tipus de la Unió Catalana d'Hospitals.

Doncs bé, el primer que cal assenyalar és que l'Acord multilateral es va celebrar entre set entitats – d'entre les quals, la FRCB – IDIBAPS i l'Hospital Clínic de Barcelona –, amb anterioritat al ciberatac, i que l'objecte del tractament és el que es transcriu tot seguit:

> "La Part que actuï com a Encarregat del Tractament guardarà secret sobre les dades de caràcter personal dels quals tingui coneixement per raó de les prestacions objecte d'aquest Acord. Tot el personal de l'entitat Encarregada del Tractament que accedeixi i/o tracti dades de caràcter personal està subjecta al secret professional i deure de confidencialitat, obligació que continua un cop finalitzada la relació entre les Parts. Mitjançant el present Acord, l'Encarregat del Tractament es compromet a portar a terme les activitats de tractament que siguin necessàries per al desenvolupament de les seves activitats en el marc d'aquesta Aliança.
> A efectes del present document, cada Part tindrà la condició de Responsable del Tractament o d'Encarregat del Tractament en funció de si es troba en una situació de prestar el servei o de demanar-lo, respectivament. Per tant, les referències realitzades en aquest document a Responsable o Encarregat s'entendran aplicables a cada Part en funció del rol que els hi apliqui en cada tractament de dades en concret."

Al seu torn, la clàusula segona de l'Acord multilateral, referida a la identificació de la informació afectada pel tractament de dades, estableix el següent: "dades de les Parts per tal que aquestes desenvolupin les seves activitats estatutàries."

Doncs bé, l'RGPD exigeix que el contracte d'encàrrec del tractament sigui un acte jurídic que estableixi i defineixi la posició de l'encarregat del tractament, en relació amb el responsable del tractament. En aquests termes, cal que el contracte d'encarregat reguli, com a mínim, les qüestions següents: l'objecte de l'encàrrec, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i les categories de persones interessades, així com les obligacions i els drets del responsable. En termes literals, l'article 28.3 RGPD estableix el següent:

> "El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. (...)"

Establert l'anterior, tot seguit s'exposen els motius pels quals cal concloure que la Fundació no disposava d'un contracte d'encarregat del tractament que recollís els extrems transcrits.

D'entrada, escau evidenciar que l'Acord multilateral no identifica quin rol assumeixen cadascuna de les 7 parts signants d'aquest. En relació amb aquest extrem, l'esmentat Acord deixa oberta la possibilitat que una part signant pugui ésser responsable del tractament o bé encarregada, en funció "del rol que els hi apliqui en cada tractament de dades en concret". Aquesta redacció imprecisa i genèrica impedeix sostenir que, d'acord amb els termes

d'aquest contracte, l'HCB assumís la condició d'encarregat per compte de cadascuna de les entitats signants, sens perjudici que de facto actués com a tal. En conseqüència, no es pot afirmar que l'objecte de l'encàrrec s'hagués definit de manera clara, tenint present que no s'especificava qui assumia la condició d'encarregat, en relació amb un tractament de dades concret.

En aquest sentit, l'esmentat Acord tampoc documenta de manera precisa les instruccions respecte l'encàrrec realitzat. Tal com estableix la Guia sobre l'encarregat del tractament en el Reglament general de protecció de dades (RGPD), elaborada per aquesta Autoritat "cal identificar de forma clara i concreta quins són els tractaments de dades que ha de dur a terme l'encarregat del tractament, atenent al tipus de servei prestat i a la manera de prestar-lo. (...)."

D'igual manera, cal posar en relleu que l'Acord multilateral no estableix les categories de dades personals que són objecte d'encàrrec, ni la categoria d'interessats afectats pel tractament. Novament, s'identifica la informació afectada de manera imprecisa ("dades de les Parts") sense concretar si les dades afectades pel tractament són categories especials de dades personals o dades personals identificatives. I, vinculat amb l'anterior, l'Acord tampoc preveu cap clàusula que defineixi la naturalesa i la finalitat del tractament o tractaments de dades, (*p.ex:* finalitat d'investigació; finalitat d'atenció sanitària, entre d'altres).

L'omissió de la informació que s'ha relacionat és especialment greu atès que les dades que es van veure compromeses pel ciberatac eren de tipologia molt diversa i eren responsabilitat de diferents entitats. En aquests termes, cal evidenciar que les entitats responsables del tractament haurien hagut de definir les dades personals que eren objecte d'encàrrec (p.ex: dades dels seus treballadors, informació personal de pacients, etcètera). Doncs, calia especificar les condicions amb què s'havia de tractar cada tipologia de dades; les categories de persones interessades; les mesures organitzatives i tècniques que l'HCB com a encarregat havia d'implementar; la finalitat de cada tractament; entre d'altres.

En aquest punt, escau puntualitzar que, el fet que fossin set les parts que van formalitzar l'Acord també exigia ser especialment curós i diligent en la definició de les obligacions i deures que assumien cadascuna d'elles, en relació amb els tractaments de dades que encarregaven a una tercera part. Tanmateix, tal com s'ha argumentat, els termes genèrics amb què es va redactar l'Acord, impedeixen sostenir que es concretessin les obligacions que va assumir l'HCB per compte de la FRCB-IDIBAPS.

A més, pel que fa a les al·legacions presentades relatives a l'existència de mecanismes que permetessin fer un seguiment sobre l'encàrrec, es tracta d'afirmacions genèriques que, tal com s'exposa posteriorment, no s'han acompanyat de cap instrument probatori suficient del que es constati que, la generalitat dels termes del conveni multilateral havia estat concretada i s'havia donat compliment a les previsions del RGPD, per salvar les imprecisions o manca de concreció de l'Acord.

Per altra banda, cal evidenciar que l'avaluació d'impacte en matèria de protecció de dades personals (AIPD), en projectes científics amb finalitats de recerca, que ha aportat la FRCB-IDIBAPS, identificava les següents amenaces (la negreta és de l'Autoritat):

- "Derivat de la complexitat del tema avaluat i la diversitat de projectes pot comportar que no **s'identifiqui de forma clara els rols que poden assumir les entitats del Grup Clínic".**

En aquest cas, per mitigar el risc d'aquesta amenaça, l'AIPD proposava implementar les mesures següents:

"Valorar de forma detallada abans de l'inici de qualsevol projecte de recerca, quin rol en matèria de protecció de dades assumeix cadascuna de les entitats intervinents en el projecte i, **formalitzar l'acord oportú en funció del resultat d'aquesta anàlisi**.
1. Si l'HCB i el promotor actuen com a responsables separats, cal signar el Data Transfer Agreement (DTA)
2. Si hi ha una corresponsabilitat, formalitzar un acord de corresponsabilitat amb el promotor.

- **Inexistència de contracte d'encarregat de tractament en aquells casos en que l'Entitat assumeix aquest rol en desenvolupament d'un projecte de recerca"**

Respecte d'aquesta amenaça, es proposava implementar la mesura correctora següent:

"Formalitzar els contractes d'encarregat de tractament en aquells casos en què l'HCB assumeix aquest rol en un projecte de recerca."

Aquestes amenaces, detectades en una AIPD respecte d'un tractament de dades concret, que afectava l'HCB i les Entitats vinculades, evidencien que l'Acord multilateral, celebrat entre les diferents parts, no definia de manera concreta el rol que assumia cadascuna d'elles, i palesava la necessitat de formalitzar nous acords i contractes d'encàrrec del tractament. Respecte d'aquest extrem, tampoc consta que les mesures correctores esmentades a l'AIPD fossin implementades degudament per la FRCB-IDIBAPS ja que, tal com s'ha avançat, no ha aportat cap altre document, a banda de l'Acord, que reguli l'encàrrec dels diferents tractaments de dades personals.

En aquestes circumstàncies, el fet d'acollir-se a un redactat genèric perquè l'Acord multilateral fos perdurable en el temps no pot ésser un argument que en validi el seu contingut. D'una banda, perquè les clàusules genèriques han resultat ser poc precises i, d'altra banda, perquè l'Acord no recull tots els extrems exigits per l'article 28.3 RGPD.

En aquest punt, escau portar a col·lació les Directrius 07/2020 sobre els conceptes de "responsable del tractament i "encarregat del tractament" en el RGPD, adoptades el 0707/2021 que, disposen el següent (la negreta és de l'Autoritat):

> "La obligación, recogida en el artículo 28, apartado 1, del RGPD, de recurrir únicamente a un encargado "que ofrezca garantías suficientes" **es una obligación continua**; es decir, no finaliza en el momento en que el responsable y el encargado formalizan el contrato u otro acto jurídico: **el responsable del tratamiento debe verificar**, con una periodicidad adecuada, las garantías del encargado, incluso cuando sea adecuado, mediante auditorias e inspecciones. (...)
>
> Por lo general, el contrato entre las partes debe redactarse a la luz de la actividad de tratamiento de datos concreta. Por ejemplo, no hay necesidad de imponer unas medidas de protección y unos procedimientos particularmente rigurosos a un encargado al que se haya encomendado una actividad de tratamiento que únicamente entrañe pequeños riesgos: aunque todos los encargados del tratamiento deben cumplir los requisitos estipulados en el Reglamento, las medidas y los procedimientos deben ajustarse a la situación concreta. En cualquier caso, el contrato debe cubrir todos los elementos indicados en el artículo 28, apartado 3. (…)

Por lo que respecta al contenido **obligatorio** del contrato u acto jurídico, el CEPD interpreta el artículo 28, apartado 3, en el sentido de que prescribe la inclusión de lo siguiente:

- El objeto del tratamiento (por ejemplo, las grabaciones realizadas por sistemas de videovigilancia de las personas que entran y salen de unas instalaciones de alta seguridad). Aunque el objeto del tratamiento es un concepto amplio, **debe formularse de un modo suficientemente detallado como para que quede claro cuál es el principal objetivo del tratamiento.**

- La duración del tratamiento: deben especificarse el **período de tiempo exacto o los criterios empleados para determinarlo**. Por ejemplo, podría hacer referencia a la duración del acuerdo de tratamiento.

- La naturaleza del tratamiento, es decir, **el tipo de operaciones realizadas** como parte del tratamiento (por ejemplo, grabación en vídeo, grabación sonora, archivo de imágenes, etc.); y la **finalidad** del tratamiento (por ejemplo, detectar una entrada ilegal). Esta descripción debe ser lo más exhaustiva posible, en función de la actividad de tratamiento concreta, para que las partes ajenas al contrato (por ejemplo, las autoridades de control) puedan comprender el contenido y los riesgos del tratamiento encomendados al encargado.

- El tipo de datos personales: este elemento debe **especificarse con el mayor grado de detalle posible** (por ejemplo, imágenes de vídeo de personas cuando entran y salen de las instalaciones). No bastaría meramente con indicar que se trata de datos personales con arreglo al artículo 4, apartado 1, del RGPD o de categorías especiales de datos personales con arreglo al artículo 9. En el caso de las categorías especiales de datos, el contrato o acto jurídico debe especificar al menos los tipos de datos de que se trata; por ejemplo, información sobre la historia clínica o información sobre la afiliación o no del interesado a una organización sindical.

- Las categorías de interesados: esto también debe especificarse con bastante grado de detalle (por ejemplo, visitantes, empleados, servicios de reparto, etc.)

- Las obligaciones y derechos del responsable: los derechos del responsable del tratamiento se abordan de un modo más exhaustivo en las secciones siguientes (por ejemplo, el derecho del responsable a llevar a cabo inspecciones y auditorías). Por lo que respecta a las obligaciones del responsable, algunos ejemplos son la obligación de proporcionar al encargado los datos mencionados en el contrato; la obligación de proporcionar al encargado instrucciones relativas al tratamiento de datos y documentarlas: la obligación de garantizar, antes del tratamiento y durante este, el cumplimiento de las obligaciones impuestas al encargado en el RGPD; y la obligación de supervisar el tratamiento, incluida la realización de auditorías e inspecciones del encargado."

D'acord amb l'exposat, escau concloure que l'Acord multilateral celebrat entre l'HCB i les Entitats vinculades no regulava el contracte d'encarregat, en els termes exigits per l'article 28 RGPD, ni donava compliment, en la seva execució, al manament legal imposat, atenent a la tipologia de dades compromesa.

Com afegitó, escau descartar que la participació de la FRCB – IDIBAPS al Comitè de Protecció de Dades o l'adhesió al Codi Tipus constitueixin mecanismes suficients per assegurar un adequat tractament de les dades personals, en el marc de l'encàrrec del

tractament. Respecte d'això, tal com ja s'ha avançat, l'entitat no ha aportat cap evidència en la què es demostri que vetllés pel compliment de les exigències requerides en termes de seguretat. De fet, aporta dues actes d'aquest Comitè, en relació amb reunions celebrades amb posterioritat al ciberatac, i només la còpia de dues actes d'una sessió de data 05/03/2019 i d'una sessió de data 29/11/2019. En darrer terme, respecte la sessió del dia 08/11/2022, només s'aporta còpia de l'ordre del dia de la reunió.

En relació amb aquesta informació, escau subratllar que, de la documentació aportada es constata que, en cap punt de l'ordre del dia de les reunions esmentades, celebrades amb anterioritat al ciberatac, s'inclou la necessitat de fer un seguiment sobre l'execució de l'Acord multilateral, ni es concreta el seu contingut genèric.

En definitiva, al marge de que l'acord multilateral incomplia clarament les previsions normativament exigibles per un encàrrec del tractament, tampoc s'ha acreditat que actuacions materials posteriors esmenessin aquestes mancances.

Per tot l'exposat, s'estima que les al·legacions de la FRCB-IDIBAPS no poden reeixir als efectes d'eximir-lo de responsabilitat.

5.3 Sobre la inexistència de mesures tècniques i organitzatives

L'escrit que la FRCB-IDIBAPS ha presentat davant el contingut de la Proposta de resolució posa de manifest que, en el moment del ciberatac, existien mesures adequades en termes de seguretat i que aquesta Autoritat hauria equiparat de manera errònia l'obligació de l'article 32.1 RGPD a una "obligació de resultat" i no de mitjans.

Doncs bé, cal assenyalar que, precisament la proposta de resolució (pàgines 9, 37 i 42) feia constar explícitament que "l'obligació d'adoptar mesures de seguretat es configura com una obligació de mitjans, i no de resultats", afirmació que s'ha vist recolzada pels arguments exposats al llarg d'aquest procediment. Pel que, en cap cas, es comparteix l'al·legat de la FRCB-IDIBAPS que pretén sostenir que l'Autoritat ha defensat que l'article 32.1 RGPD recull una obligació de resultats. De fet, aquí no s'imputa que s'hagués materialitzat un ciberatac, sinó que l'objecte de la qüestió és l'omissió de les obligacions que la Fundació havia d'acomplir com a responsable del tractament de dades.

Vinculat amb l'anterior, cal fer notar que l'article 32 RGPD també comporta que el responsable del tractament hagi d'actuar diligentment en el procés d'identificació, verificació, avaluació i valoració de l'eficàcia de les mesures tècniques i organitzatives que s'implementin. Aquestes actuacions, que s'han de dur a terme de manera regular, tenen per finalitat garantir la seguretat del tractament, tenint en compte que, tal com s'ha avançat a l'apartat 3r d'aquesta resolució, els riscos i la probabilitat d'aquests són variables en el temps.

Tanmateix, respecte d'aquestes qüestions, la FRCB-IDIBAPS no ha aportat cap evidència que acrediti haver facilitat instruccions concretes a l'HCB, respecte mesures tècniques i organitzatives exigibles en atenció als riscos; ni ha aportat cap altra informació que denoti un seguiment o avaluació de les mesures que l'HCB va implementar. Aquest seguiment era del tot necessari tenint en compte l'evolució de la tècnica, i que els riscos associats al tractament són canviants. Respecte d'aquestes qüestions, escau afegir que, la Fundació no havia efectuat una anàlisi dels riscos als què s'exposaven les dades de les què n'era responsable, pel que difícilment podia valorar si les mesures implementades eren apropiades.

Aquestes exigències deriven també del principi de responsabilitat proactiva (article 5.2 RGPD) que exigeix que el responsable del tractament dugui a terme totes les actuacions

escaients per tal de vetllar per a la protecció de les dades personals, així com ser especialment diligent tant en l'elecció, com en la supervisió, de les persones a qui encarrega tractaments de dades personals.

En aquest punt, escau assenyalar que la FRCB-IDIBAPS també al·lega que "l'APDCAT no aconsegueix aportar les proves necessàries per constatar l'ocurrència de les infraccions imputades, corresponent per llei a l'Autoritat la càrrega de provar la comissió d'aquestes infraccions."

Doncs bé, en resposta, escau invocar la Sentència del Tribunal de Justícia de la Unió Europea, de data 14/12/2023 (assumpte C-340/21) que, en termes literals estableix el següent:

> "Del tenor de los artículos 5, apartado 2, 24, apartado 1, y 32, apartado 1, del RGPD se desprende inequívocamente que **la carga de la prueba de que los datos personales se tratan de modo que se garantiza una seguridad adecuada, en el sentido de los artículos 5, apartado 1, letra f), y 32 de dicho Reglamento, incumbe al responsable del tratamiento en cuestión** [véanse, por analogía, las sentencias de 4 de mayo de 2023, Bundesrepublik Deutschland (Buzón electrónico judicial), C-60/22, EU: C:2023:373, apartados 52 y 53, y de 4 de julio de 2023, Meta Platforms y otros (Condiciones generales del servicio de una red social), C-252/21, EU:C:2023:537, apartado 95]."

En efecte, no hi ha dubte que el responsable del tractament ha de poder demostrar que els tractaments de dades personals que duu a terme o que encarrega a tercers, són conformes l'RGPD, d'acord amb el principi de responsabilitat proactiva.

Dit això, tot seguit es donarà resposta a cada una de les al·legacions presentades, des d'una perspectiva tècnica, i s'incidirà especialment en aquelles qüestions que la FRCB-IDIBAPS ha volgut ressaltar a l'escrit presentat a la proposta de resolució. Tot això, tenint també en compte el contingut dels informes emesos des de l'Àrea de Tecnologia i Seguretat de la Informació d'aquesta Autoritat – reproduïts en la part jurídicament rellevant -.

5.3.1 (...)

(...)

5.3.2 (...)
(...)

5.3.3 (...)

(...)

5.3.4 (...)

(...)

5.3.5 (...)
(...)

5.3.6 (...)

(...)

5.4 Sobre la manca de realització d'anàlisi de riscos

En l'escrit d'al·legacions de data 25/06/2024 la FRCB-IDIBAPS afirma que ha aportat "exemples d'avaluacions d'impacte en protecció de dades, on s'analitza l'impacte que determinades activitats de tractament poden tenir pels drets i llibertats de les persones" i que va facilitar "un conjunt d'evidències relatives a anàlisis de riscos des d'una aproximació tècnica, que sembla ser que no s'han valorat per part de l'Autoritat". Tot seguit, l'entitat assenyala que "el Pla director de Seguretat incloïa una anàlisi de riscos de seguretat sobre la base del marc de referència ISO 27:002, que va servir per a definir el pla d'acció i l'estratègia futura de l'HCB per a mitigar els riscos que presentaven els tractaments de dades que s'havien identificat" i afegia que "la realització d'auditories va contribuir a l'avaluació permanent de l'estat de la seguretat dels actius de l'HCB i de la FRCB-IDIBAPS, en tant que es van realitzar anàlisis de riscos i vulnerabilitats en matèria de seguretat, tenint present en tot moment els tractaments de dades que es realitzaven a l'HCB".

Doncs bé, tal com s'assenyalava a la proposta de resolució d'aquesta Autoritat, el primer que cal fer és diferenciar l'obligació d'efectuar una anàlisi de riscos respecte un determinat tractament, de l'obligació de dur a terme una avaluació d'impacte en matèria de protecció de dades personal (AIPD).

L'article 32.2 de l'RGPD exigeix que els responsables i encarregats del tractament facin una anàlisi del risc associat als tractaments que duen a terme, que ha de tenir en compte, entre d'altres factors: la tipologia del tractament; la naturalesa de les dades; el nombre de persones afectades i la quantitat o varietat de tractaments que realitza una mateixa organització. En aquest sentit, qualsevol organització que disposi de plataformes corporatives per al tractament de dades personals i actuï com a encarregada, i també els responsables del tractament de dades personals, cal que duguin a terme les anàlisi de riscos pertinents. En efecte, l'esmentada anàlisi és un document que pot aportar informació suficient per tal que el responsable del tractament decideixi si és necessari dur a terme una AIPD.

En canvi, l'AIPD s'ha d'efectuar quan una tipologia de tractament pugui comportar un risc alt per als drets i llibertats de les persones titulars de les dades. L'article 35.3 de l'RGPD concreta que, cal fer una AIPD quan s'avaluïn de manera sistemàtica i exhaustiva aspectes personals de persones físiques amb base a un tractament automatitzat; quan es tractin dades personals a gran escala; o quan s'observi sistemàticament a gran escala una zona d'accés públic.

Per tant, l'anàlisi de riscos ha de contenir una aproximació tècnica per d'identificar els actius més valuosos d'un sistema i les amenaces que poden afectar-los així com l'impacte que suposaria pels drets i interessos afectats. Aquests riscos existents poden ésser diferents en funció dels tractaments de dades personals que el responsable dugui a terme. D'una banda, perquè les persones implicades en el tractament poden no coincidir i, d'altra banda, perquè unes dades poden requerir ser especialment protegides enfront determinats riscos.

Establerta la diferència entre ambdós instruments, escau palesar que l'obligació d'efectuar l'esmentada anàlisi de riscos ho és tant pels responsables del tractament, com pels encarregats del tractament. Això és així atès que cadascun d'ells pot identificar riscos diferents respecte les dades que tracten, en funció dels seus rols i de les persones implicades i afectades. En aquest sentit, l'HCB – com a encarregat del tractament – havia de

realitzar la pertinent anàlisi de riscos, en el context de l'encàrrec efectuat i, en canvi, la responsable del tractament (la FRCB-IDIBAPS) havia d'efectuar el seu anàlisi de riscos respecte les dades que tractava, amb vistes a determinar els mitjans de l'encàrrec. Aquesta exigència ja la preveia l'ENS 2010 per a sistemes de categoria mitjana – i, fins i tot per a sistemes de categoria bàsica [op.pl.1]-. En aquest punt, escau fer notar que, la plataforma que va ser atacada contenia dades identificatives i de salut de pacients, vinculades a tractaments assistencials, així com d'investigació clínica, dades personals d treballadors, i dades personals de tercers col·laboradors interns i externs, i proveïdors.

La rellevància d'efectuar aquesta anàlisi de riscos és encara més evident si es té en compte que, a l'AIPD aportada per la FRCB-IDIBAPS s'hi descriuen fins a 32 riscos associats a un tractament de dades molt concret, en projectes científics amb finalitats de recerca.

En aquest punt, escau destacar que el considerant 75è de l'RGPD estableix el següent (la negreta és de l'Autoritat):

> "Los riesgos para los derechos y libertades de las personas físicas, **de gravedad y probabilidad variables**, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; **o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".**

En efecte, per poder gestionar correctament el risc, calia que la FRCB-IDIBAPS identifiqués i caracteritzés de manera precisa les finalitats de les operacions dels tractaments de dades personals que duia a terme i que va encarregar a l'HCB.

Així, un cop identificada la finalitat dels diferents tractaments, l'entitat havia de descriure'ls correctament per tal de conèixer l'abast de les amenaces existents per als drets i llibertats, en cada una de les etapes del seu tractament. Concretament, les descripcions de tractament inclouen: el flux de les dades personals, el cicle de vida d'aquestes, els rols de les persones que havien d'accedir a la informació en cada etapa, les característiques de les tecnologies a emprar, l'extensió o volum d'informació, la periodicitat de recollida i supressió de dades, etcètera. Aquesta informació constitueix la caracterització d'un tractament, que el diferencia d'altres.

Per tant l'anàlisi del risc que preveu l'RGPD exigia conèixer l'abast de cadascun del tractament de dades dels què la FRCB-IDIBAPS n'era responsable i veure les potencials amenaces existents en el marc de la plataforma de l'HCB. En aquest punt, resultava cabdal

valorar la probabilitat de la materialització del risc i el nivell global d'amenaça pel que fa als drets i llibertats afectats. En aquest sentit, el considerant 76è de l'RGPD estableix el següent (la negreta és de l'Autoritat):

> "La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del **tratamiento de datos.** El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones del tratamiento de datos suponen un riesgo o si el riesgo es alto."

Respecte d'aquest punt, la Fundació pretén considerar acomplerta aquesta obligació a partir del document núm. 5 "Pla director de seguretat" de l'any 2018 que assenyala fins a deu riscos associats als sistemes d'informació de l'HCB. Tanmateix, aquest document analitza la situació de l'HCB respecte del compliment de la ISO 2700:2013, sense tenir en compte les exigències de l'RGPD quant a l'anàlisi dels riscos en matèria de protecció de dades personals. De fet, no conté cap referència als potencials drets fonamentals i llibertats que es podien veure potencialment afectats davant una intrusió als sistemes de l'HCB ni descriu els tractaments de dades personals que es duien a terme per compte de la FRCB-IDIBAPS.

En aquest context, és evident que la filtració de les dades de salut pot tenir un impacte diferent als drets fonamentals de les persones que en són titulars, en comparació amb la filtració de dades identificatives de treballadors. Així mateix, l'exposició a diferents amenaces i riscos també es diferent en funció dels usuaris habilitats per accedir a la informació, del context en què tracten les dades, etcètera. Per tant, calia analitzar el risc tenint en compte les característiques de les operacions de tractament.

Obligació que és exigible tant a la Fundació, com a les entitats encarregades del tractament que, en el seu cas, han de realitzar una anàlisi de riscos tenint en compte el context en què es duu a terme l'encàrrec.

D'acord amb l'exposat fins aquí, escau concloure que les AIPD's aportades per la FRCB-IDIBAPS – que fan referència a tractaments específics que duia a terme l'HCB – no poden servir, en cap cas, per entendre satisfeta l'obligació d'efectuar l'anàlisi de riscos prevista a l'article 32.2 RGPD, en connexió amb l'article 28 LOPDGDD. D'una banda, perquè l'RGPD ha diferenciat les AIPD dels anàlisis de riscos i, d'altra banda, perquè el responsable del tractament no pot pretendre la satisfacció de l'obligació de realitzar l'anàlisi de riscos, a partir de documents elaborats per un encarregat del tractament, en el context de l'encàrrec en qüestió i respecte d'un tractament de dades molt concret.

En conseqüència, escau concloure que les al·legacions i documentació que ha presentat la FRCB-IDIBAPS no desvirtuen la imputació referida a la manca de realització d'una anàlisi de riscos prèvia a la identificació de les mesures de seguretat exigibles, en relació amb les dades personals de les quals n'era responsable del tractament.

De la mateixa manera, la Fundació tampoc ha acreditat haver dut a terme cap activitat de supervisió, tal com la pròpia entitat ha reconegut que era de la seva responsabilitat. Doncs, no s'ha provat cap actuació concreta per part de la FRCB-IDIBAPS en relació amb l'encàrrec del tractament encomanat a l'HCB, ni tampoc constitueix evidència suficient el mer fet de formar part del comitè de protecció de dades.

5.5 Sobre l'incompliment dels principis aplicables a l'exercici de la potestat sancionadora

L'escrit d'al·legacions que la Fundació va presentar a l'acord d'iniciació del procediment, al qual es remet en l'escrit presentat en data 25/06/2024, adduïa que totes les parts del

procediment sancionador han de respectar els principis de la potestat administrativa sancionadora, previstos als articles 25 a 31 de la Llei 40/2015, d'1 d'octubre, del règim jurídic del sector públic, i insistia en la necessitat de sobreseure aquest procediment.

5.5.1 Sobre el principi de tipicitat

L'article 27 de la Llei 40/2015, sobre el principi de tipicitat, estableix que només constitueixen infraccions administratives les vulneracions de l'ordenament jurídic previstes com a tals infraccions per una llei, i afegeix que les normes que defineixen infraccions i sancions no són susceptibles d'aplicació analògica.

Respecte d'aquesta qüestió, escau recordar la Sentència de l'Audiència Nacional de 17/10/2007 (recurs núm. 23/2006) que recull l'argumentació jurídica següent: "concurre la tipicidad cuya infracción se denuncia en el escrito de demanda, pues hay predeterminación normativa que desempeña la función de garantía mediante la cual se tiene una predicción razonable de la conducta ilícita y de las consecuencias jurídicas que lleva aparejada la comisión de dicha conducta, dicho de otra forma, **la tipicidad es suficiente si consta en la norma una predeterminación inteligible de la infracción, de la sanción y de la correlación entre una y otra."**

Doncs bé, contràriament al que pretén la FRCB-IDIBAPS, les conductes referides a la manca d'adopció de mesures tècniques i organitzatives; la manca de realització d'una anàlisi de riscos; i la formalització d'un contracte d'encarregat del tractament, sense el contingut previst a l'article 28 de l'RGPD, constitueixen conductes tipificades d'acord amb l'article 83.4.*a* de l'RGPD. En aquestes circumstàncies, per tot l'exposat en aquesta resolució, s'aprecia identitat entre els seus components fàctics i els elements descrits per l'esmentat precepte, en connexió amb els articles 28 i 32 de l'RGPD. Per tant, l'homogeneïtat entre els fets comesos i els elements normatius que el descriuen i que fonamenten el contingut material dels il·lícits impedeix sostenir que mantenir les imputacions vulneri el principi de tipicitat.

Dit d'una altra manera, l'RGPD constitueix una norma comunitària intel·ligible, directament aplicable als estats membres, que recull la tipificació de les tres infraccions que aquí s'imputen, en consonància amb els fets que han resultat provats.

En darrer terme, l'entitat defensava la seva innocència i argumenta que l'Autoritat no té elements probatoris suficients per afirmar que des de la FRCB-IDIBAPS s'han comès les infraccions esmentades. Respecte d'això, invoca la sentència del Tribunal Suprem, de 6 de juliol de 1990 (RJ 1990/6589) d'acord amb la qual: "l'activitat sancionadora de l'Administració ha de respectar el principi de la presumpció d'innocència, recollit a l'article 24.2 de la Constitució, ja no només com un mer principi teòric de dret aplicable en l'àmbit de la jurisdicció penal a través de l'axioma in dubio pro reo relacionat amb la valoració benigna de les proves en cas d'incertesa, sinó com un ampli dret fonamental de la persona (...)".

Pel que aquí interessa, aquesta Autoritat no qüestiona el dret a la presumpció d'innocència recollit a l'article 24 de la Constitució espanyola i a l'article 53.2.*b* de l'LPAC. Nogensmenys, existeix la presumpció de "no existència de responsabilitat administrativa" mentre no es demostri el contrari. I, d'acord amb la documentació que l'entitat imputada ha aportat al llarg d'aquest procediment, hi ha proves documentals suficients que recolzen les imputacions que s'efectuen en aquest procediment, i que cal atribuir a la Fundació. Proves que no han estat desvirtuades per l'entitat.

5.5.2 Sobre el principi de proporcionalitat

La FRCB-IDIBAPS assenyalava la importància de tenir present el principi de proporcionalitat, quan una administració pública valora la imposició d'una sanció. En aquest sentit, recorda l'argumentació seguida per l'Audiència Nacional (Sala del Contenciós Administratiu, Secció 1a) de 21/11/2017 (recurs núm. 208/2014) que sostè que el marge d'apreciació que s'atorga a l'Administració en la imposició de sancions, s'ha de desenvolupar ponderant les circumstàncies concurrents en cada supòsit.

Quant a les circumstàncies fàctiques del cas, que la FRCB-IDIBAPS considera que han d'incidir en el judici de proporcionalitat, s'esmenten, d'una banda, l'afectació de la situació de pandèmia sanitària als serveis de salut i, d'altra banda, l'estat de la tècnica en el moment de l'incident.

En primer terme, la Fundació assenyalava que els fets que aquí s'imputen van ocórrer en un context caracteritzat per una lenta recuperació dels efectes ocasionats per la Covid-19, en què el principal afectat va ser el sector sanitari i els hospitals "sobretot els de naturalesa pública" atesa la limitació dels seus recursos – tant materials, com humans i econòmics – per fer front a totes les necessitats sorgides arran de la pandèmia.

Al fil de l'anterior, l'entitat subratllava el seu paper crucial en la recerca de la Covid-19. (...) Entre d'altres qüestions, l'entitat indicava que els seus recursos es van mobilitzar de manera decisiva per donar suport a l'HCB durant la crisi sanitària i que la seva dedicació es va focalitzar en dur a terme una investigació exhaustiva sobre la Covid-19. Aquestes actuacions considerava que eren suficients per demostrar la capacitat d'adaptabilitat i de resposta de la institució davant aquest tipus de desafiament, que els va situar com un "puntal essencial" en la lluita de la pandèmia".

Per l'exposat, considerava desproporcionada la conclusió d'aquesta Autoritat, respecte la manca de mesures de seguretat en relació amb les dades personals tractades, tenint en compte el context de dificultat anteriorment descrit.

Doncs bé, el primer que cal dir és que l'RGPD preveu un sistema normatiu complet destinat a preservar la protecció de dades de caràcter personal, en tots els nivells. D'aquesta manera, les previsions referides al seu règim sancionador resulten d'aplicació de manera immediata i directa, amb la finalitat última de garantir el dret fonamental a la protecció de dades personals.

Al fil de l'anterior, el legislador europeu ha reglamentat i recollit el principi de proporcionalitat a l'article 83 de l'RGPD. En qualsevol cas, en el sistema normatiu que preveu aquest reglament el que és determinant no és la sanció econòmica o la declaració d'una infracció, sinó els poders correctius de les autoritats de control previstos a l'article 58.2 de l'RGPD, amb la finalitat de fer complir aquesta norma; reduir el grau d'incompliment; i que les infraccions no resultin més rendibles que els incompliments. Dit això, es parteix de la premissa que les sancions i mesures que imposi l'Autoritat han de ser efectives, proporcionades i dissuasives per aconseguir la finalitat que persegueix l'RGPD i que, per assolir-ho, cal tenir present les circumstàncies de cada cas concret.

Respecte de les manifestacions de la FRCB-IDIBAPS, aquesta Autoritat és coneixedora de la importància de la investigació en un context de crisi sanitària, i dels recursos que es van

haver de destinar per al desenvolupament de les vacunes contra la Covid-19. Tanmateix, l'excepcionalitat d'aquestes circumstàncies no eximeix els responsables del tractament de continuar garantint el dret fonamental a la protecció de dades personals.

De fet, cal tenir ben present que la manca d'identificació de les mesures tècniques i organitzatives que aquí s'imputa no és una obligació nova, exigible arran de la Covid-19, sinó que, ja abans de la situació de crisi sanitària, la Fundació havia de protegir la informació de la què n'és responsable, d'acord amb l'ENS 2010 i amb l'RGPD, i assegurar-se que l'encarregat del tractament (l'HCB) implementava les mesures de seguretat necessàries. En aquests termes, el fet que el ciberatac tingués lloc en un context caracteritzat per la "lenta recuperació" dels efectes ocasionats per la Covid-19, no eximia a la FRCB-IDIBAPS de la seva responsabilitat respecte dels fets imputats, que venia des de lluny (any 2010). En aquest sentit, l'al·legació relativa al principi de proporcionalitat decau en sí mateixa, si atenem al temps transcorregut des de l'obligatorietat d'implementar les mesures de l'ENS 2010, sense que es donés compliment a aquest.

Així mateix, l'entitat imputada insisteix en la necessitat d'interpretar l'estat de la tècnica en consonància amb el principi de proporcionalitat. Tot seguit, assenyala que, en el moment de produir-se el ciberatac, a Catalunya no hi havia cap hospital públic que "constés certificat respecte de l'Esquema Nacional de Seguretat" i afegia que, les mesures que tenien implementades abans de l'incident s'emmarquen en el llistat de recomanacions que va emetre l'Agència de la Unió Europea per a la Ciberseguretat, al juliol de l'any 2023. Aquestes recomanacions es refereixen, entre d'altres, al següent: (...).

Tot seguit, la FRCB-IDIBAPS també assenyalava que cal fer referència a les seves actuacions – com a supervisor de l'HCB – però també a la conducta d'aquest, "en tant que encarregat del compliment del mandat donat per l'anterior". En concret, destaca la seva assistència a la sessió extraordinària del Comitè de Protecció de Dades, "de la qual cosa es desprèn la seva diligència en la supervisió de la gestió de l'incident efectuada per l'HCB". L'entitat també justifica haver actuat amb diligència quan va informar "ràpidament a l'Agència en el moment de produir-se l'incident, així com en contestar en temps i forma totes les peticions d'informació relacionades".

Vinculat amb l'anterior, la Fundació assenyalava que l'afectació del ciberatac a l'activitat normal de l'HCB i de les Entitats Vinculades "va ser curta" i que aquestes van posar tots els seus esforços en minimitzar l'impacte de l'incident. Aquests fets, segons la FRCB-IDIBAPS denoten que es va adoptar una conducta diligent i que es van assolir bons resultats, malgrat la complexitat i sofisticació de l'atac. Els resultats obtinguts no s'haguessin pogut obtenir "si no hagués estat per la implementació de la multitud de mesures que s'han detallat" i conclou que el judici de proporcionalitat només pot portar a la conclusió que, tant l'HCB com les Entitats vinculades, van implementar les mesures que, conforme el principi de proporcionalitat, els hi eren exigibles.

La FRCB-IDIBAPS també dedicava un apartat de les seves al·legacions al principi de proporcionalitat "en la regulació actual en matèria de protecció de dades". Respecte d'aquesta qüestió, assenyalava que aquest principi ha de ser valorat d'acord amb els principis rectors que regeixen el Sistema Nacional de Ciberseguretat, plasmats al Codi de bon govern de la ciberseguretat. D'acord amb aquest Codi, el primer principi recollit és precisament el referit a la proporcionalitat, de manera que les previsions que s'hi contenen s'han d'aplicar sempre "tenint en compte la complexitat i recursos amb què compta cada entitat." I, respecte d'això, la Fundació també assenyalava que la proporcionalitat s'ha de

posar en relació amb l'estat de la tècnica del moment (STS núm. 188/2022). En aquest sentit, indica que l'article 32 RGPD estableix que les mesures tècniques i organitzatives apropiades han de tenir en compte l'estat de la tècnica i els costos d'aplicació. Així, defensa que, és precisament el conjunt d'aquests elements "el que determina si les mesures de seguretat són apropiades", és a dir, si les mesures tècniques i organitzatives implementades contribueixen a l'objectiu perseguit dins dels paràmetres de raonabilitat, proporcionalitat i eficàcia, tal com s'estableix a l'Ordre PCI/487/2019, de 26 d'abril, per la que es publica l'Estratègia Nacional de Ciberseguretat 2019, aprovada pel Consell de Seguretat Nacional.

En darrer terme, la Fundació insistia amb què una eventual sanció sobre la base d'una bretxa de seguretat, degut a un esdeveniment fortuït, suposaria configurar l'obligació d'implementar mesures tècniques i de seguretat, com una obligació de resultats. Aquest fet, segons assenyala, suposaria invalidar "tot l'esforç i inversió tecnològica i organitzativa realitzats i desincentivar la presa de mesures de prevenció i seguretat (...)". A l'anterior, la Fundació afegia que "no es pot obviar la influència del nivell de sofisticació de les tècniques intrusives emprades pel tercer no autoritzat, trobant-se en aquesta la causa de la bretxa de seguretat quan les mesures implementades són les adequades" i argumenta que, tant l'HCB com les Entitats vinculades "es trobaven en una situació considerablement més madura en relació amb les exigències en matèria de ciberseguretat que la majoria de els organitzacions de la mateixa naturalesa i sector". Vinculat amb l'anterior, l'entitat indicava que en el cas d'altres incidents molt similars, no hi ha hagut conseqüències més enllà de l'incident de seguretat.

Doncs bé, no es pot desconèixer que el principi de proporcionalitat requereix, en tot cas, ponderar les circumstàncies que concorren en cada cas, per tal d'assolir la necessària i deguda proporcionalitat entre els fets imputats i la responsabilitat exigida. Aquest principi normatiu redueix l'àmbit discrecional de les administracions – també d'aquesta Autoritat – i exigeix l'adequació de les sancions als fets comesos.

Al fil de l'anterior, aquesta resolució s'efectua després d'haver valorat les circumstàncies dels fets provats; el context en què es van ocasionar; les al·legacions i proves documentals aportades per la FRCB-IDIBAPS; la conducta de l'entitat imputada; la naturalesa dels perjudicis ocasionats; així com el marc normatiu aplicable en aquell moment, entre d'altres. Circumstàncies que impedeixen sostenir que aquest pronunciament s'efectua sense haver tingut en compte l'esmentat principi.

Així mateix, escau palesar que aquest procediment no s'inicia pel fet que la plataforma de l'HCB hagi estat víctima d'una violació de seguretat; sinó que els fets que aquí s'imputen són la manca d'identificació de mesures tècniques i organitzatives exigibles, d'acord amb el marc normatiu referit al llarg d'aquesta resolució; la manca de realització d'una anàlisi de riscos; i la manca de formalització d'un contracte d'encarregat del tractament, en els termes de l'article 28 RGPD.

En aquest punt, cal recordar que algunes de les mesures de seguretat no implementades eren les corresponents a qualsevol sistema de seguretat, amb independència del nivell baix, mitjà o alt el que acredita la rellevància de l'incompliment, en termes de proporcionalitat no tan sols pel temps transcorregut, sinó per l'entitat dels incompliments.

Finalment, cal dir que l'obligació d'adoptar mesures de seguretat es configura com una obligació de mitjans, i no de resultats. Per aquesta raó, en d'altres supòsits, en què una entitat ha notificat una violació de seguretat davant l'Autoritat, les circumstàncies del cas

poden haver justificat descartar l'inici d'un procediment sancionador. Seria el supòsit, per exemple, dels casos en què les entitats, tot i haver adoptat les mesures tècniques i organitzatives exigibles d'acord amb l'RGPD i l'ENS, han estat víctimes d'un ciberatac. Aquest raonament s'efectua de conformitat amb la línia jurisprudencial del Tribunal de Justícia de la Unió Europea (vid. Assumpte C-340/21, de 14/12/2023, ECLI:EU:C:2023:986) que, sobre la interpretació dels articles 24 i 32 de l'RGPD, estableix el següent:

> "(...) del tenor de los artículos 24 y 32 del RGPD se desprende que estas disposiciones se limitan a obligar al responsable del tratamiento a adoptar medidas técnicas y organizativas destinadas a evitar, en la medida de lo posible, cualquier violación de la seguridad de los datos personales. El carácter apropiado de tales medidas debe evaluarse en cada caso concreto, examinando si el responsable ha adoptado esas medidas teniendo en cuenta los diferentes criterios establecidos en los mencionados artículos y las necesidades de protección de datos específicamente inherentes al tratamiento de que se trate y a los riesgos que conlleva.
>
> Por consiguiente, los artículos 24 y 32 del RGPD no pueden entenderse en el sentido de que una comunicación no autorizada de datos personales o un acceso no autorizado a dichos datos por parte de un tercero basten para concluir que las medidas adoptadas por el responsable del tratamiento no eran apropiadas, en el sentido de esas disposiciones, sin siquiera permitir a este último aportar la prueba en contrario."

Tanmateix, aquest no és el cas que aquí ens ocupa atès que la FRCB-IDIBAPS, ja abans del ciberatac del mes de març de 2023, no havia vetllat per la implementació deguda de les mesures exigibles d'acord amb l'RGPD i l'ENS 2010, i tampoc no havia formalitzat un contracte d'encarregat del tractament amb l'HCB, en els termes de l'article 28 de l'RGPD, ni havia realitzat la pertinent anàlisi de riscos.

En resum, l'obligació de complir amb les previsions de l'ENS deriva de l'any 2010 i, pel que fa al fet d'una inadequada gestió de la política de seguretat, tant des del punt de vista de la implementació com des del punt de vista de la supervisió, amb incompliments exigibles a qualsevol sistema de seguretat baix, mitjà o alt, fa que la proporcionalitat a l'hora d'aplicar el règim sancionador resulti justificada.

5.5.3 Sobre el principi de culpabilitat

Tot seguit, la Fundació adduïa que el principi de culpabilitat impedeix sancionar-la atès que, sostenir el contrari, suposaria exigir un grau de diligència inassumible, que no seria proporcionat "tenint en compte la naturalesa d'entitat pública de la FRCB-IDIBAPS i les circumstàncies post-pandèmiques a les quals hem fet referència". Així mateix, l'entitat també cita diferents sentències en base a les quals, l'apreciació del principi de culpabilitat està condicionat a l'existència de dol, culpa o fins i tot una ignorància inexcusable. Per reforçar aquesta argumentació, també aporta el pronunciament recent del Tribunal de Justícia de la Unió Europea, en l'assumpte C-683/21, de 5 de desembre de 2023, el qual conclou que només es pot imposar una multa administrativa a un responsable del tractament de dades "per una infracció de l'RGPD si la infracció s'ha comès de manera culpable, és a dir, de forma intencionada o negligent. Aquesta circumstància concorre, segons el TJUE, quan el responsable del tractament no podia ignorar el caràcter infractor de la seva conducta, tingués o no consciència de la infracció (apartat 81)."

D'acord amb aquest posicionament, la FRCB-IDIBAPS assenyala que ignorava el caràcter infractor de la seva conducta i reforça aquesta circumstància en el fet que "és una entitat adherida al Codi Tipus de la Unió Catalana d'Hospitals". En relació amb això, s'indica que, el fet de comptar amb una certificació emesa per una associació pública catalana, "és una clara mostra que no se li pot atribuir responsabilitat per les presumptes deficiències posades de manifest per l'APDCAT".

Doncs bé, en relació amb el principi de culpabilitat, escau assenyalar que aquesta Autoritat ha recordat en diverses resolucions la doctrina jurisprudencial aplicable, tant del Tribunal Suprem, com del Tribunal Constitucional. En efecte, la potestat sancionadora de l'Administració, atès que és una manifestació de l'"ius puniendi" de l'Estat, es regeix pels principis del dret penal – com ho és, el principi de culpabilitat – incompatible amb un règim de responsabilitat objectiva, sense culpa. En aquest sentit, en les sentències de dates 15/04/2016 i 24/11/2011, entre d'altres, el Tribunal Suprem es remet a la doctrina del Tribunal Constitucional i cita textualment l'argumentació següent:

> "No cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, doctrina que se reafirma en la sentencia 164/2005, de 20 de junio de 2005, en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad, aun a título de mera negligencia."

D'acord amb aquesta doctrina, per atribuir la responsabilitat per infraccions comeses al seu autor, cal que hi concorri l'element de culpa, dins del que tenen cabuda les accions o omissions comeses per "mera negligència".

Doncs bé, en consonància amb la jurisprudència esmentada, escau assenyalar que la negligència no exigeix un clar ànim d'infringir, sinó que radica precisament en el descuit o en la manca d'atenció exigible a l'entitat, en relació amb el compliment de les seves obligacions en matèria de protecció de dades personals. En aquest punt, convé posar en relleu que el deure de diligència és màxim quan les activitats que el responsable duu a terme afecten drets fonamentals, com ho és el dret a la protecció de dades personals.

Així mateix, el Tribunal Suprem en la seva sentència de 25/01/2006, dictada també en l'àmbit de protecció de dades, al·ludia a la diligència exigible i establia que la intencionalitat no constitueix un requisit necessari perquè una conducta sigui considerada culpable. El que cal és que en la conducta que s'imputa hi concorri l'element de la culpabilitat, i per poder apreciar l'existència de culpabilitat n'hi ha prou que els fets infractors portin causa d'una conducta negligent o atribuïble a la simple inobservança.

En aquest cas, s'han exposat diferents situacions que denoten la inobservança de la FRCB-IDIBAPS respecte les obligacions que tenia, com a responsable del tractament de les dades que es trobaven allotjades a la plataforma de l'HCB.

En aquests termes, la responsabilitat de la Fundació pel que fa a la manca de seguretat de la plataforma de l'HCB, deriva de la "*culpa in vigilando*" atès que també era exigible que – en la seva condició de responsable del tractament – supervisés les actuacions de l'HCB o ordenés la implementació de les mesures oportunes. També es podria considerar que va incórrer en "*culpa in eligendo*" atès que va escollir un encarregat del tractament que no va donar o implementar les garanties suficients, en termes de seguretat, per a la protecció de les dades personals de les què n'era responsable.

Per altra banda, escau fer notar que, la Fundació – en la seva condició de responsable del tractament – també va eludir la seva obligació d'efectuar una anàlisi de riscos, i de formalitzar un contracte d'encarregat del tractament amb l'HCB, que recollís en termes precisos els extrems previstos per la normativa de protecció de dades personals, o concretar els termes genèrics de l'acord subscrit, per donar compliment als requeriments materials legalment exigibles.

Totes aquestes omissions denoten la inobservança respecte el compliment de l'RGPD i l'LOPDGDD, i són suficients per acreditar l'element de culpabilitat necessari, en els termes que ho exigeix la jurisprudència que s'ha transcrit.

Per tot el que s'ha exposat, aquesta Autoritat no comparteix que la Fundació actués de manera diligent en la definició de les mesures tècniques i organitzatives, com a responsable del tractament de les dades personals que duia a terme l'HCB, per mitjà de la plataforma corporativa atacada; tampoc comparteix que l'entitat efectués cap anàlisi de riscos respecte les dades de les què n'era el responsable; ni que definís de manera concreta un contracte d'encarregat del tractament, en els termes previstos a l'article 28 de l'RGPD. En conseqüència, es considera que les imputacions efectuades no contravenen el principi de culpabilitat.

5.5.4 Sobre els principis de confiança legítima i bona fe de les administracions públiques

L'article 3.1.*e* de la Llei 40/2015 estableix que les administracions públiques han de servir amb objectivitat els interessos generals i han de respectar amb la seva actuació els principis de "bona fe, confiança legítima i lleialtat institucional".

D'acord amb aquest precepte, i amb nombrosa jurisprudència que l'interpreta, la Fundació argumenta que quan l'Agència de Ciberseguretat de Catalunya va elaborar l'informe "Context previ incident de *ransomware* a l'Hospital Clínic", en les setmanes immediatament posteriors a l'incident, es va crear una confiança legítima en l'HCB i en la Fundació de què les mesures tècniques i organitzatives implementades eren suficients i que l'incident no comportaria represàlies com la que suposa la iniciació d'un procediment sancionador per part d'aquesta Autoritat.

En relació amb l'anterior, l'entitat afegeix que, d'acord amb les conclusions de l'esmentat Informe, es va crear la confiança que l'actuació de les entitats vinculades era ajustada a dret i per això considera que, les imputacions que s'efectuen en aquest procediment, contradiuen les conclusions d'aquest informe, fet que implica "una situació jurídica completament inesperada i desfavorable per a les entitats". A més, assenyala que el fet que aquests actes no fossin dictats pel mateix organisme de l'Administració "no és un requisit exigit per la jurisprudència perquè pugui apreciar-se la vulneració dels principis esmentats" i recorda quines són les funcions de l'Agència de Ciberseguretat de Catalunya, regulades a l'article 2 de la Llei 15/2017, de 25 de juliol.

En darrer terme, la FRCB-IDIBAPS sosté que "en haver-se elaborat aquest informe durant el primer trimestre de l'any 2023 i haver-se iniciat el procediment sancionador gairebé un any després, resulta evident el trencament de la confiança que havia dipositat en l'HCB i en les Entitats vinculades en l'adequació de les mesures preses, que es veu posteriorment frustrada en veure's front una possible sanció per la presumpta inadequació de les mateixes."

En resposta a les qüestions que planteja la FRCB-IDIBAPS, escau precisar que l'Informe "Context previ incident de *ransomware*" al qual fa referència, en cap cas conclou que les mesures implementades per l'entitat, en termes de ciberseguretat, s'haguessin implementat en els termes exigits per l'RGPD i l'ENS 2010. De fet, aquest informe, que no està datat, i que s'hauria elaborat les "setmanes immediatament posteriors a l'incident" seria coincident temporalment amb l'informe resultant de la gestió de l'incident, de data 31/03/2023, elaborat per l'Agència de Ciberseguretat de Catalunya. Aquest darrer informe palesa les vulnerabilitats dels sistemes de l'HCB que van permetre a l'atacant materialitzar l'atac, i descriu un pla – que inclou escenaris a curt, mitjà i llarg termini – per tal que l'entitat implementi mesures necessàries per millorar la seguretat de la seva informació, així com "altres recomanacions per prevenir futurs casos com el succeït.".

Aquests dos informes, elaborats per l'Agència de Ciberseguretat de Catalunya, que denoten vulnerabilitats en els sistemes d'informació de l'HCB i proposen diferents mesures per millorar-ne la seguretat, impedeixen sostenir que s'havia creat una confiança legítima entre l'HCB i les Entitats vinculades, d'acord amb la qual la seva actuació havia estat ajustada a l'RGPD. Respecte d'aquesta circumstància, escau fer notar que, malgrat que l'entitat argumenti que, precisament, en base a aquesta confiança va assumir que actuava conforme a dret, el cert és que la Fundació coneixia la fase d'informació prèvia que va derivar amb l'inici d'aquest procediment.

Per altra banda, el fet que l'acord d'iniciació del procediment sancionador es notifiqués a la FRCB-IDIBAPS al mes de gener de 2024, no és un element que permeti sostenir el pretès "trencament de la confiança". Doncs, des del moment en què l'Autoritat va tenir coneixença de l'abast del ciberatac, va iniciar una investigació per tal de valorar les circumstàncies del cas i la pertinença d'iniciar un expedient sancionador. Aquest fet era del tot conegut per l'entitat imputada i, per aquest motiu, no es pot sostenir la vulneració de l'article 3.1.*e* de la Llei 40/2015.

En resum, ni es produeix una vulneració de la bona fe, ni menys encara de la confiança legítima. Ans al contrari, atenent a l'especial consideració de les dades de salut, s'ha de traslladar la confiança legítima per part de les entitats responsables de què adoptin els mínims estàndards de seguretat legalment exigibles per protegir-les.

De conformitat amb el que s'ha exposat, s'estima que aquesta al·legació no pot reeixir.

5.6 Altres qüestions

5.6.1 Sobre l'estat de la tècnica

Al tercer punt del seu escrit d'al·legacions a la proposta de resolució, la Fundació insisteix en l'excepcionalitat del context postpandèmic en el marc del qual es va produir l'incident; en l'escassetat de dotació pressupostària als centres sanitaris; la complexitat de l'incident, i l'eficaç recuperació després de l'atac. Respecte d'aquestes qüestions, l'entitat considera que la proposta n'omet la seva rellevància, sense valorar-les amb el deteniment que mereixerien.

Doncs bé, tal com s'argumenta a l'apartat 5.5.2 d'aquesta resolució, sobre el principi de proporcionalitat, escau assenyalar que la FRCB-IDIBAPS ha omès obligacions que venien de lluny. Cal tenir en compte que l'exigència de vetllar per la implementació de mesures tècniques i organitzatives apropiades; la realització d'una anàlisi de riscos; i la formalització del corresponent contracte d'encarregat del tractament, conforme l'RGPD i l'LOPDGDD, no són obligacions noves exigibles arran de la Covid-19, sinó que, ja abans de la situació de

crisi sanitària, calia d'haver adoptat una major seguretat per als sistemes d'informació de l'HCB i, en darrer terme, per als drets i llibertats dels titulars de les dades personals. Respecte d'aquest punt, tampoc es pot compartir que existís una dificultat tècnica o econòmica insalvable per adoptar determinades mesures tècniques i organitzatives, si tenim en compte que aquestes es van implementar immediatament després de l'atac.

De la mateixa manera, l'anàlisi del risc associat als tractaments de dades personals tampoc és una obligació exigible arran de la pandèmia sanitària, sinó que ja estava prevista a l'RGPD. En aquests termes, l'excepcionalitat del context postpandèmic, l'escassetat de dotació pressupostaria o la complexitat del ciberatac sofert no constitueixen factors eximents de la responsabilitat de la FRCB-IDIBAPS.

Pel que fa a l'estat de la tècnica, l'entitat insisteix amb què en el moment de produir-se l'incident no hi havia cap hospital públic a Catalunya que constés certificat de l'ENS, i que és "precisament el conjunt de circumstàncies relatives al context i a l'estat de la tècnica existent el que s'ha de tenir en compte a l'hora de valorar la suficiència de les mesures, i no el potencial resultat patit arrel d'un ciberatac."

En resposta a aquesta qüestió, cal assenyalar que l'Autoritat no imputa al responsable del tractament – la Fundació - la manca de certificació de l'ENS per part de l'HCB. De fet, aquesta és una circumstància que únicament l'ha plantejat la FRCB-IDIBAPS. En aquest sentit, tal com s'exposava a la proposta de resolució – i es reitera en aquesta resolució – les referències a l'ENS 2010 responen a una doble consideració: d'una banda, a l'obligatorietat d'implementar determinades mesures i, d'altra banda, a la seva configuració com a paràmetre de referència envers la seguretat exigible, d'acord amb l'estat de la tècnica.

En darrer terme, la FRCB-IDIBAPS assenyala que si l'Autoritat està "valorant l'adequació de les mesures a partir del seu grau d'eficàcia davant d'un ciberatac", aleshores estaria exigint una obligació de resultats. Tanmateix, tal com s'ha reiterat en aquesta resolució, aquesta Autoritat no imputa la vulneració del principi de confidencialitat (art. 5 RGPD) de les dades personals afectades arran del ciberatac o d'altres eventuals infraccions, com a conseqüència d'aquest. Contràriament a això, s'imputen actuacions que, inclús abans de que es materialitzés el ciberatac, constituïen infraccions de la normativa de protecció de dades personals.

Per l'exposat, les nombroses referències a l'ENS així com el reconeixement, per part del mateix HCB, de la necessitat d'implementar diferents mesures tècniques i organitzatives (...) denoten que, d'acord amb l'estat de la tècnica, era exigible una major seguretat, per garantir la protecció de les dades personals.

5.6.2 Sobre la presumpta indefensió causada per la proposta de resolució

En darrer terme, la FRCB-IDIBAPS addueix que la proposta de resolució reverteix certes mancances que constitueixen vulneracions d'alguns dels principis bàsics de l'actuació administrativa i, en conseqüència, són causants d'indefensió en el present supòsit. En concret, que la proposta manca de recursos doctrinals i jurisprudencials. Aquest fet, segons argumenta l'entitat si bé "no infringeix com a tal el deure de motivació de les resolucions administratives, sí que posa en entredit que la conclusió sigui fruit d'una argumentació ajustada a l'objecte del litigi i que permeti a l'interessat, així com a la resta d'òrgans administratius i judicials i als ciutadans, poder conèixer el fonament de la ratio decidendi de les resolucions (...)".

Respecte d'aquest posicionament, el primer que cal assenyalar és que, contràriament al que pretén la FRCB-IDIBAPS, ja en la proposta de resolució es feia referència al marc normatiu que recull els principis aplicables a l'exercici de la potestat sancionadora, així com a

diferents pronunciaments judicials que els interpreten (vid. entre d'altres: SAN de 17/10/2007 recurs núm. 23/2006, STS de 15/04/2016, STS de 14/11/2011, SAN 21/11/2017 recurs núm. 208/2014, STS 25/01/2006). L'escassetat de recursos jurisprudencial que segons la Fundació li hauria causat indefensió no és tal, tenint en compte que l'Autoritat ha argumentat abastament el seu posicionament jurídic en les 48 pàgines de la seva proposta de resolució, així com també en aquest acte administratiu. En efecte, la Fundació és plenament coneixedora dels arguments que sostenen la decisió d'aquesta Autoritat, ja que tant aquesta resolució com els actes que integren l'expedient administratiu al qual la part interessada ha tingut possibilitat d'accedir des de l'inici d'aquest procediment (art. 53 LPAC), motiven abastament les decisions que s'han adoptat, tant des d'un punt de vista fàctic, com jurídic.

Tot seguit, la Fundació assenyala d'altres elements que "posen en dubte el correcte compliment dels requisits de motivació de les decisions administratives sancionadores i l'existència d'una deguda anàlisi sobre les qüestions plantejades per arribar a la decisió sobre el fons, la qual cosa ens fa concloure que s'ha causat indefensió". En aquest sentit, manifesta que, el fet que la proposta de resolució es basi en l'informe de l'Àrea de Tecnologia i Seguretat de l'Autoritat, al qual la FRCB-IDIBAPS no ha tingut accés, no hauria respectat els drets d'audiència i de bona fe de les administracions públiques. En relació amb l'anterior, l'entitat considera que no és ajustat a dret "recolzar els arguments de l'acusació en un document al qual la part contra qui es dirigeix el procediment sancionador no ha tingut accés i, per tant, no se li ha donat l'oportunitat d'exercir els drets de defensa degudament." Així mateix, l'entitat afegeix que, en cap part de la proposta de resolució, s'hi exposa quina va ser la conclusió o el sentit dels pronunciaments de l'Àrea de Tecnologia i Seguretat de la Informació de l'Autoritat.

Per recolzar la seva argumentació, la Fundació cita la sentència del Tribunal Suprem de 30/06/2011 (recurs núm. 2682/2009) en què s'hi exposa la doctrina del Tribunal Constitucional sobre l'assumpció de la "vigència en l'àmbit administratiu sancionador d'un conjunt de garanties derivades del contingut de l'art. 24 CE, de les que, conforme es va exposar a la STC 7/1998, convé destacar ara el dret de defensa, excloent de la indefensió." Seguidament, aquesta sentència exposa un llistat no exhaustiu de maneres de procedir per l'òrgan administratiu que es consideren causants d'indefensió; entre elles, cita "els drets a ser informat de l'acusació, amb la ineludible conseqüència de la inalterabilitat dels fets imputats (...) que implica que la càrrega de la prova dels fets constituïts de la infracció recaigui sobre l'Administració."

Aquesta darrera al·legació, referida a la pretesa indefensió, en cap cas pot prosperar.

En primer terme, escau palesar que, per mitjà de la proposta de resolució no es fa una mera referència a l'informe de l'Àrea de Tecnologia i Seguretat sinó que, contràriament a això, la proposta incorpora el contingut dels aspectes tècnics de l'informe a la motivació de la proposta. De fet, s'hi incorpora tota la informació necessària per justificar la decisió de l'Autoritat – tant en la proposta de resolució, com també en aquest acte administratiu -. La suficiència de l'explicació de cada raonament, impedeix sostenir que l'entitat desconegui el contingut de l'informe esmentat, el qual s'ha incorporat a la proposta i ha servit per a la seva motivació.

Vinculat amb l'anterior, la FRCB-IDIBAPS addueix que la proposta no recull el sentit dels pronunciaments de l'esmentada Àrea i que tampoc n'inclou la conclusió. Tanmateix, aquestes afirmacions no s'ajusten a la realitat dels fets tenint present que, l'antecedent 11è transcriu en termes literals la conclusió a la què va arribar l'Àrea de Tecnologia i Seguretat de la Informació, i que la resolució conté nombroses remissions literals i referències explícites a l'informe.

Per últim, cal fer avinent que la FRCB-IDIBAPS – com a part interessada en aquest procediment – podia accedir a qualsevol document d'aquest procediment sancionador i que, malgrat això, en cap moment, va exercir l'accés. Així, la proposta fixa de manera motivada els fets que es consideren provats i la seva qualificació jurídica, determina la infracció que constitueixen, i el subjecte que n'és responsable. També estableix la sanció proposada i conté una àmplia argumentació respecte dels fonaments bàsics de la resolució proposada.

Per tot l'exposat, s'estima que aquesta darrera al·legació, referida a una pretesa indefensió, tampoc pot prosperar a l'efecte d'eximir la Fundació de responsabilitat.

6. Qualificació jurídica dels fets provats

6.1 Fet provat 1r

En relació amb el fet descrit al punt primer de l'apartat de fets provats, cal acudir a l'article 32.1 de l'RGPD, referent a la seguretat del tractament, transcrit al fonament de dret 3r d'aquesta resolució.

Tal com s'ha exposat amb anterioritat, del contingut de l'article 32.1 de l'RGPD s'infereix una vocació dinàmica de definir i adoptar mesures tècniques i organitzatives. En aquest sentit, les Directrius 4/2019 del Grup de treball de l'article 29 (actual Comitè Europeu de Protecció de Dades Personals) del 20/10/2020, estableixen el següent (la negreta és de l'Autoritat):

> "(…) Junto con otras medidas de PDDD, el considerando 78 apunta que los responsables del tratamiento tienen la responsabilidad de **evaluar de forma continua si están utilizando medios apropiados de tratamiento en todo momento y si las medidas elegidas neutralizan verdaderamente las vulnerabilidades existentes**. Además, los responsables del tratamiento deben llevar a cabo revisiones periódicas de las medidas de seguridad de la información que rodean y protegen los datos personales, así como el procedimiento para gestionar vulneraciones.
> Elementos esenciales desde el diseño y por defecto con respecto a la integridad y la confidencialidad pueden ser los siguientes:
> (…)
> • Análisis de riesgos: Se evaluarán los riesgos contra la seguridad de los datos personales teniendo en cuenta cómo afectan a los derechos de las personas y se neutralizarán los riesgos identificados. Para su uso en la evaluación de riesgos, se desarrollará y mantendrá un «modelo de amenazas» exhaustivo, sistemático y realista y un análisis de la superficie de ataque del software diseñado para reducir los vectores de ataque y las oportunidades de aprovechar puntos débiles y vulnerabilidades.
> • Seguridad desde el diseño: Se considerarán los requisitos de seguridad lo antes que sea posible en el diseño y desarrollo del sistema y se integrarán y realizarán los ensayos pertinentes de forma continuada.
> • Mantenimiento: Se realizarán revisiones y ensayos periódicos del software, hardware, sistemas y servicios, etcétera, para detectar vulnerabilidades de los sistemas de apoyo al tratamiento.
> (…)
> • Protección en función del riesgo: Todas las categorías de datos personales deberán protegerse con medidas adecuadas con respecto al riesgo de una vulneración de seguridad. Los datos que presenten riesgos especiales deberán mantenerse separados del resto de datos personales en la medida de lo posible.

(…)”

En paral·lel, escau tenir present que, a més l’RGPD exigeix als responsables del tractament que puguin demostrar el compliment de les obligacions que se’n deriven. A tall d’exemple, ja en el considerant 78è de l’RGPD s’hi estableix el següent:

> “La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento.
> **A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.**
> Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. (...)
> Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.”

D’acord amb l’exposat fins aquí, es constata que les mesures de seguretat, que es defineixen prèviament a l’inici d’un tractament de dades personals, exigeixen que es revisin i s’actualitzin, també en el moment de tractar les dades, en funció de l’estat de la tècnica, els costos, els nivells de riscos i amenaces, entre d’altres. També, que el responsable del tractament pugui demostrar les actuacions que ha dut a terme per adequar-se a l’RGPD.

Aquestes exigències obeeixen al fet que les operacions del tractament i els riscos a què estan sotmeses les dades personals poden variar en el temps i poden exigir que per garantir-ne la protecció calgui implementar més seguretat. Tot això, en consonància amb l’obligació que preveu l’article 25 de l’RGPD, de protegir les dades personals des del disseny i per defecte.

En aquest punt, tal com s’ha exposat al fonament de dret precedent d’aquesta resolució, la FRCB-IDIBAPS ha adduït diferents situacions que, al seu parer, demostren que havia identificat mesures tècniques i organitzatives adequades. Tanmateix, pels motius que s’han anat descrivint, escau concloure que l’entitat no ha demostrat que les hagués implementat degudament. Respecte d’això, escau indicar que la infracció de l’article 32.1 de l’RGPD s’efectua entenent la seguretat en termes globals i no només respecte de determinades mesures considerades individualment. En relació amb això, s’assumeix que l’estat de la tècnica permetia adoptar més seguretat i que aquesta no era excessivament costosa tal i com exposa l’entitat. La seguretat, en definitiva, és un concepte integral en la mesura en què ha de comprendre totes les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc.

Reforça la idea anterior el fet que, un cop es va materialitzar l’incident, es van implementar un seguit de mesures que, fins aleshores, no s’havien implementat o definit per diferents motius, com ara “dificultats pràctiques”. A tall d’exemple, tal com ja s’ha avançat al punt 5.3.1 d’aquesta resolució, per contenir i erradicar l’impacte del ciberatac, es va desplegar (...) per a tots els comptes d’usuari de l’HCB. Per aquesta raó, no es pot sostenir que, amb

anterioritat al atac, aquesta mesura constituís un “repte difícil d’assumir”. Així mateix, també es van implementar altres mesures de seguretat com ara (...).

Vinculat amb l’anterior, cal fer notar que la FCRB-IDIBAPS no ha aportat cap evidència documental que permeti constatar que s’havien facilitat instruccions a l’HCB d’acord amb les quals l’instava a adoptar les mesures de seguretat que, en el marc d’aquest procediment, s’ha evidenciat que no estaven implementades, malgrat ser necessàries. Aquest extrem tampoc apareix recollit al contracte d’encarregat del tractament, ni es va concretar amb posterioritat.

En aquest punt, escau indicar que, tal com s’argumenta en la sentència 188/2022, de 15 de febrer, del Tribunal Suprem, l’article 32.1 de l’RGPD recull una obligació de mitjans, i no de resultats. En efecte, l’Autoritat coincideix a l’hora de considerar que no es pot exigir a les organitzacions un risc zero però sí que s’implementin mesures amb la màxima diligència, en atenció a les circumstàncies concurrents en cada cas. Precisament, l’esmentada sentència, que confirma una resolució de l’Agència Espanyola de Protecció de Dades (AEPD) assenyala que:

> “en el 2018 existía un sistema de verificación del correo electrónico conocido como ‘doble opt in’ consistente en un proceso de adaptación de unes normas o condiciones de uso cuyo principal objetivo es el de verificar que los usuarios son quienes dicen ser (...). De modo que, en el momento en que se produjeron estos hechos existían medidas técnicas referidas al proceso de registro, que hubiesen evitado la filtración de datos producida.”

Doncs bé, tenint en compte tot el que s’ha exposat fins aquí, no hi ha dubte que la sensibilitat de la informació que tractava l’HCB – per compte de la FRCB-IDIBAPS -, l’estat de la tècnica, els costos, i la tendència creixent d’atacs amb programari de segrest evidenciaven la necessitat d’implementar més seguretat per protegir la informació.

En efecte, malgrat que la Fundació ha defensat la pertinença de les mesures que s’havien implementat, el cert és que d’acord amb els paràmetres exigits per l’RGPD, en consonància amb l’ENS 2010 i l’estat de la tècnica imperant al mes de març de 2023, aquestes mesures no eren les apropiades per garantir un nivell de seguretat adequat al risc. I, en relació amb això, escau destacar que tampoc va vetllar per la correcta aplicació de les mesures per part del seu encarregat, l’HCB.

Durant la tramitació d’aquest procediment s’ha acreditat el fet descrit al punt 1r de l’apartat de fets provats, que és constitutiu de la infracció prevista a l’article 83.4 de l’RGPD, que tipifica la vulneració de “las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43”, d’entre les quals s’hi inclou la prevista a l’article 32.1 de l’RGPD .

La conducta que aquí s’aborda s’ha recollit com a infracció greu a l’article 73.*f* de l’LOPDGDD, de la manera 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.”

6.2 Fet provat 2n

Pel que fa al fet descrit al punt 2n de l'apartat de fets provats, referent a la manca de realització d'una anàlisi de riscos, cal acudir a l'article 32.2 de l'RGPD, que disposa el següent:

> "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 autorizado a dichos datos."

També l'article 28.2 de l'LOPDGDD preveu l'obligació del responsable del tractament d'adoptar les mesures tècniques i organitzatives apropiades a fi de garantir i acreditar que un tractament és conforme l'RGPD, tenint en compte en particular, els riscos superiors que es poden produir en els supòsits que es transcriuen tot seguit:

> 2. Per a l'adopció de les mesures a què es refereix l'apartat anterior els responsables i encarregats del tractament han de tenir en compte, en particular, els riscos superiors que es poden produir en els supòsits següents:
>
> a) Quan el tractament pugui generar situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per als afectats.
> b) Quan el tractament pugui privar els afectats dels seus drets i llibertats o els pugui impedir l'exercici del control sobre les seves dades personals.
> c) Quan es produeixi el tractament no merament incidental o accessori de les categories especials de dades a què es refereixen els articles 9 i 10 del Reglament (UE) 2016/679 i 9 i 10 d'aquesta Llei orgànica o de les dades relacionades amb la comissió d'infraccions administratives.
> d) Quan el tractament impliqui una avaluació d'aspectes personals dels afectats amb la finalitat de crear o utilitzar perfils personals d'aquests, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment a la feina, la seva situació econòmica, la seva salut, les seves preferències o interessos personals, la seva fiabilitat o comportament, la seva solvència financera, la seva localització o els seus moviments.
> e) Quan es dugui a terme el tractament de dades de grups d'afectats en una situació d'especial vulnerabilitat i, en particular, de menors d'edat i persones amb discapacitat.
> f) Quan es produeixi un tractament massiu que impliqui un gran nombre d'afectats o comporti la recollida d'una gran quantitat de dades personals.
> g) Quan les dades personals hagin de ser objecte d'una transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals respecte dels quals no s'hagi declarat un nivell adequat de protecció.
> h) Qualssevol altres que segons el parer del responsable o de l'encarregat puguin tenir rellevància i en particular els previstos en codis de conducta i estàndards definits per esquemes de certificació.

Al seu torn, aquest precepte s'ha d'interpretar d'acord amb l'article 24 de l'RGPD, referit a la responsabilitat del responsable del tractament, que exigeix analitzar els riscos de diversa probabilitat i gravetat, associats a un tractament de dades personals concret, per als drets i llibertats de les persones físiques.

En efecte, l'RGPD parteix d'una concepció basada en la gestió dels riscos associada als tractaments de dades personals. Aquest enfocament es refereix directament a la necessitat de disposar de sistemes preventius tendents a minimitzar els riscos pels drets i llibertats de les persones titulars de les dades personals que són objecte de tractament. Per això s'imposa l'obligació d'identificar aquests riscos i avaluar-ne l'impacte i la probabilitat que es materialitzin.

Vinculat amb l'anterior, tal com estableix el Tribunal de Justícia de la Unió Europea a la sentència de 14/12/2023 (ECLI:EU:C:2023:986), cal identificar els riscos i les seves possibles conseqüències per als drets i llibertats de les persones físiques, tenint en compte, en cada cas, la probabilitat i gravetat de les amenaces. En termes literals:

> "Del citado artículo 32, apartados 1 y 2, se desprende que el carácter apropiado de tales medidas técnicas y organizativas debe apreciarse de manera escalonada. **Por una parte, es preciso identificar los riesgos de violación de la seguridad de los datos personales que entrañe el tratamiento y sus posibles consecuencias para los derechos y libertades de las personas físicas.** Esta apreciación debe llevarse a cabo en cada caso concreto, tomando en consideración cuál es la probabilidad de los riesgos identificados y la gravedad de estos. Seguidamente, debe comprobarse si las medidas adoptadas por el responsable del tratamiento se adaptan estos riesgos, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento."

En aquest cas, la FRCB-IDIBAPS no ha aportat cap evidencia que permeti constatar que va fer una anàlisi de riscos en relació amb el tractament de dades personals que va encarregar a l'HCB i que aquest duia a terme per mitjà de la plataforma corporativa afectada. Sobre això, no es pot obviar que els tractaments de les dades, per mitjà de la plataforma de l'HCB, entren dins els supòsits especificats als apartats *a* a *f* de l'article 28.2 LOPDGDD i que, per tant, calia tenir en compte els riscos superiors que es podien materialitzar, per poder definir mesures adequades. Respecte d'això, si bé l'RGPD no estableix el llistat de mesures que cal aplicar, l'anàlisi de riscos constitueix una eina essencial per determinar-les correctament, juntament amb la regulació de l'ENS. Tanmateix, el fet de no haver identificat les amenaces existents, ni la probabilitat que es materialitzessin, va dificultar l'exercici posterior, que consistia a identificar i implementar adequadament les mesures necessàries per protegir la informació.

De conformitat amb el que s'ha exposat, el fet recollit al punt 2 de l'apartat de fets provats, constitueix la infracció prevista l'article 83.4.*a* de l'RGPD, que tipifica la vulneració de "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43".

Al seu torn, aquesta conducta s'ha recollit com a infracció greu a l'article 73.*p* de l'LOPDGDD, en la forma següent:

> "p) El tractament de dades personals sense dur a terme una valoració prèvia dels elements que esmenta l'article 28 de la Llei orgànica."

6.3 Fet provat 3r

Pel que fa a la conducta descrita al punt 3r de l'apartat dels fets provats, referent a la manca d'un contracte d'encarregat del tractament que preveiés el contingut de l'article 28 RGPD, cal acudir a l'esmentat precepte que disposa el següent (la negreta és de l'Autoritat):

> "3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, **que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.**
> Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
> a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
> b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
> c) tomará todas las medidas necesarias de conformidad con el artículo 32;
> d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
> e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
> f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
> g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
> h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
> En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros. (...)
> 9.El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico."

Tal com s'ha argumentat a l'apartat 5.2 d'aquesta resolució, l'Acord multilateral que van celebrar la Fundació i l'HCB no regulava l'encàrrec del tractament de dades personals, en els termes que preveu l'article 28 de l'RGPD. Doncs, no recollia de manera concreta qui assumia el rol de responsable del tractament de les dades; qui era l'encarregat del tractament; els drets i obligacions de cadascuna de les parts afectades; la finalitat dels

diferents tractaments de dades personals, entre d'altres. Tots aquests elements eren bàsics en el marc de la regulació d'un encàrrec del tractament de dades i, ni en el moment de l'encàrrec, ni posteriorment, es varen concretar.

Aquest fet imputat és constitutiu d'infracció, segons l'article 83.4.*a* RGPD, que tipifica així 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 28 de l'RGPD.

La conducta que aquí s'analitza s'ha recollit com a infracció greu a l'article 73.*k* de l'LOPDGDD, de la manera següent:

> "k) Encarregar el tractament de dades a un tercer sense la formalització prèvia d'un contracte o un altre acte jurídic escrit amb el contingut que exigeix l'article 28.3 del Reglament (UE) 2016/679."

7. Sanció i mesures correctores

L'article 77.2 de l'LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'article 77.1 de l'LOPDGDD, l'autoritat de protecció de dades competent:

> "(...) ha de dictar una resolució que declari la infracció i estableixi, si s'escau, les mesures que convingui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès, a excepció de la que preveu l'article 58.2.i del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016.
>
> La resolució s'ha de notificar al responsable o l'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."

I l'apartat 3r de l'article 77 de l'LOPDGDD, estableix que:

> "3. Sense perjudici del que estableix l'apartat anterior, l'autoritat de protecció de dades ha de proposar també la iniciació d'actuacions disciplinàries quan hi hagi indicis suficients per fer-ho. En aquest cas, el procediment i les sancions que s'han d'aplicar són els que estableix la legislació sobre règim disciplinari o sancionador que sigui aplicable.
>
> Així mateix, quan les infraccions siguin imputables a autoritats i directius, i s'acrediti l'existència d'informes tècnics o recomanacions per al tractament que no s'hagin atès degudament, en la resolució en què s'imposi la sanció s'ha d'incloure una amonestació amb la denominació del càrrec responsable i se n'ha d'ordenar la publicació al «Butlletí Oficial de l'Estat» o autonòmic que correspongui."

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.”.

La proposta de resolució preveia requerir a la FRCB-IDIBAPS perquè al més aviat possible, i en tot cas en el termini de 2 mesos a comptar a partir de l'endemà de la notificació de la resolució dictada en aquest procediment, aportés un cronograma en què s'hi indiquin els terminis que necessita per realitzar les anàlisis de riscos associades als tractaments de dades personals de les què n'és responsable, i per definir les mesures tècniques i organitzatives que calgui implementar, en funció dels resultats de les anàlisi de riscos que realitzi, i en coordinació amb l'HCB.

Així mateix, també es requeria a la Fundació perquè, en un termini de dos mesos, revisés l'Acord multilateral celebrat amb l'HCB, en relació amb les dades emmagatzemades a la plataforma atacada, de manera que es recullin tots els extrems previstos a l'article 28 RGPD, i perquè tot seguit, en trameti una còpia a l'Autoritat.

Doncs bé, l'escrit d'al·legacions que l'entitat ha presentat davant l'Autoritat en data 25/06/2024 s'acompanya d'un pla d'adequació a l'ENS de l'HCB, així com d'un document referit al “pla d'acció adoptat arran el ciberatac”. En aquest cronograma s'hi preveu, entre d'altres actuacions, la realització d'anàlisi de riscos en relació amb els drets i llibertats de les persones titulars de les dades objecte del tractament.

Tanmateix, per tal de fer un seguiment sobre la implementació d'aquestes mesures, escau requerir la FRCB-IDIBAPS perquè informi anualment (al mes de juliol de 2025 i de 2026) a l'Autoritat, sobre el grau d'implementació de les actuacions previstes al cronograma, per mitjà d'una certificació que acrediti que s'han implementat degudament.

Així mateix, també es requereix la FRCB-IDIBAPS perquè en un termini de 2 mesos, revisi l'Acord multilateral celebrat amb l'HCB de manera que es recullin tots els extrems previstos a l'article 28 RGPD i específicament, els mecanismes per fer el seguiment de l'encàrrec efectuat a l'HCB i perquè n'aporti còpia a l'Autoritat. Pel que fa a la implementació d'altres mesures tècniques i organitzatives – a banda de les previstes al cronograma – caldrà que tant la Fundació com l'HCB tinguin en consideració els resultats obtinguts als anàlisis de riscos que efectuïn, en les seves respectives condicions.

Per si pot resultar d'utilitat, als efectes de corregir els efectes de la infracció, es facilita l'enllaç a la Guia sobre l'encarregat del tractament en el Reglament general de protecció de dades (RGPD), elaborada per aquesta Autoritat, i actualitzada el mes de juny de 2024.

Tot això sens perjudici de les potestats d'inspecció d'aquesta Autoritat per verificar que s'han implementat les mesures tècniques i organitzatives necessàries, en compliment de l'RGPD i l'LOPDGDD.

Resolució

Per tot això, resolc:

1. Declarar que la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer ha comès tres infraccions: una infracció prevista a l'article 83.4.*a* en relació amb l'article 32.1; una altra infracció prevista a l'article 83.4.*a* en

relació amb l'article 32.2; i una tercera infracció prevista a l'article 83.4.a en relació amb l'article 28, tots ells de l'RGPD.

2. Requerir la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer perquè adopti les mesures correctores assenyalades al fonament de dret 7è i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-les.

3. Notificar aquesta resolució a la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer.

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 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 l'entitat imputada pot 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 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