Identificació de l'expedient

Resolució del procediment sancionador núm. PS 1/2024, referent a l'Hospital Clínic de Barcelona.

Antecedents

1. En data 04/03/2023, a les 21:30 h aproximadament, l'Hospital Clínic de Barcelona (HCB) va detectar una incidència a la seva xarxa per mal funcionament de les comunicacions, que afectava diferents serveis. Arran d'aquesta detecció, la Direcció de Sistemes d'Informació de l'HCB (DSI) va fer una primera anàlisi interna sobre aquesta incidència. En data 05/03/2023, a les 10:35 hores aproximadament, la DSI va concloure que la infraestructura de l'Hospital, en concret la plataforma corporativa de virtualització de l'HCB, havia patit un atac amb programari de segrest (*ransomware*) que afectava els sistemes d'informació del mateix HCB i els de les entitats que hi estan vinculades -en concret, Barnaclínic, SA; el Consorci d'Atenció Primària de Salut Barcelona Esquerra (CAPSBE) i la Fundació de Recerca Clínic Barcelona-Institut d'Investigacions Biomèdiques August Pi i Sunyer (FRCB-IDIBAPS)-, que s'hi allotjaven.

El mateix dia 05/03/2023, a les 11:17 hores aproximadament, l'HCB va notificar el ciberatac 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, i per tant dins del termini de 72 hores previst a l'article 33 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), l'HCB va notificar a l'Autoritat Catalana de Protecció de Dades (APDCAT) la violació de la seguretat de les dades que havia patit.

L'atacant va aconseguir (...).

Això va suposar una interrupció molt greu del funcionament normal dels centres (entre d'altres serveis, se'n va veure afectada la prestació de serveis de laboratori, farmàcia, urgències i quiròfans), de manera que els casos més crítics es van derivar immediatament a altres centres del sistema sanitari.

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 diagnòstics, tractaments, resultats de laboratori i informes radiològics de pacients, 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 de l'RGPD i l'article 19 de la Llei 32/2010 de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i d'acord amb les competències que té atribuïdes, l'APDCAT va obrir un expedient informatiu contra l'HCB (IP núm. 213/2023) i cadascuna de les entitats vinculades, amb la finalitat d'esbrinar les circumstàncies dels fets. En concret, per esbrinar si l'HCB i les entitats vinculades, 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, conseqüentment, 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 núm. 213/2023, en data 26/04/2023 es va requerir l'HCB perquè:

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 contingudes a la infraestructura de l'HCB (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 dels documents a què feia referència l'informe de l'Agència de Ciberseguretat "Context de ciberseguretat previ a la materialització de l'atac", que l'HCB va lliurar a aquesta Autoritat en data 21/04/2023.

3.6. Aportés còpia del Pla de continuïtat, si en tenia, amb indicació de les proves de restauració que s'haguessin fet durant els dos anys anteriors a l'incident.

3.7. Aportés còpia de l'anàlisi forense sobre l'incident de ciberseguretat que, entre d'altres aspectes, recollís els 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 26/05/2023, l'HCB va respondre el requeriment amb un escrit en què responia cadascuna de les peticions efectuades per l'APDCAT. (...)

5. En data 05/07/2023, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit de denúncia d'una persona ciutadana contra l'HCB (IP 343/2023), amb motiu del ciberatac patit. En aquest escrit manifestava literalment el següent:

> "A l'atenció del màxim responsable de l'entitat, pel tractament de les dades personals. Després de patir per les meves dades personals i veure a la DarkWeb les dades de molts catalans i catalanes, sol·licito una explicació per escrit i formal al més aviat possible. (...) Si empreses i institucions hem de complir amb la llei de protecció de dades rigorosament, com a institució pública demano una explicació tècnica, molt detallada i que demostri que les meves dades i les de tots els catalans i catalanes estan assegurades i tenen bons plans de contingència, amb la nova política de transparència pels ciutadans. Resto a l'espera. Moltes gràcies per l'ajuda i col·laboració amb la seguretat ciutadana"

De conformitat amb el que disposa l'article 57 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (LPAC), aquesta denúncia es va acumular a la fase d'informació prèvia (IP núm. 213/2023) oberta per l'Autoritat contra l'HCB, atesa la identitat amb els fets objecte de denúncia i l'entitat a què fan referència.

6. En data 18/01/2024, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'Hospital Clínic de Barcelona, per dues presumptes infraccions: una infracció prevista a l'article 83.4.*a*, en relació amb l'article 32.1; i una altra infracció de l'article 83.4.*a*, en relació amb l'article 32.2, tots ells de l'RGPD. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 18/01/2024.

En aquesta mateixa data, també es va acordar iniciar un procediment sancionador contra el Consorci d'Atenció Primària de Salut de l'Eixample (PS núm. 2/2024), contra Barnaclínic, SA (PS núm. 3/2024) i contra la Fundació de Recerca Clínic Barcelona – Institut d'Investigacions Biomèdiques August Pi i Sunyer (PS núm. 4/2024).

7. 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.

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

9. En data 29/01/2024, l'Autoritat va acordar ampliar en cinc dies més el termini per formular al·legacions.

10. En data 08/02/2024, l'HCB va formular al·legacions a l'acord d'iniciació, que s'aborden a l'apartat 5è dels fonaments de dret.

L'entitat imputada aportava amb el seu escrit documentació diversa. En concret, la següent:

10.1 Correus electrònics intercanviats entre la DSI i la Direcció de Persones de l'HCB, els anys 2021 i 2022, sobre l'activació de la mesura de seguretat referida a (...).

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

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

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

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

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

10.7 Informe sobre l'impacte assistencial del ciberatac patit per l'Hospital Clínic elaborat pel director assistencial de l'HCB.

10.8 (...)

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

10.10 Auditories de seguretat. (...)

10.11 Mesures aplicades després de l'atac.

10.12 Avaluacions d'impacte en protecció de dades (AIPD). En concret, s'aporta l'informe d'avaluació d'impacte del tractament de dades personals en projectes científics amb finalitats de recerca, datat a agost de 2021. També, unes captures de pantalla referides a una eventual anàlisi de riscos del tractament "investigació."

10.13 Metodologia interna per a la realització d'AIPD.

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

11. En data 12/04/2024, a petició de la instructora del procediment, l'Àrea de Tecnologia i Seguretat de la Informació d'aquesta Autoritat va emetre un informe tècnic sobre les al·legacions formulades per l'HCB en l'escrit de 07/02/2024. Les conclusions d'aquest informe es transcriuen tot seguit:

> "(...) 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 atacats 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."

12. En data 22/04/2024, l'Àrea d'Inspecció de l'Autoritat va fer una sèrie de comprovacions a través d'internet, a l'efecte d'aixecar una diligència sobre els comunicats oficials que va fer l'HCB arran del ciberatac. Així, va constatar que al comunicat de data 30/03/2023 s'hi afirma

que “s’ha vist compromesa la confidencialitat de: 1. Dades identificatives i de salut de pacients. 2. Dades personals de treballadors. 3. Dades personals d’entitats col·laboradores i proveïdors.”

13. En data 24/04/2024, la instructora del procediment va sol·licitar a l’Àrea de Tecnologia i Seguretat de la Informació d’aquesta Autoritat que es pronunciés respecte de les mesures de seguretat que preveia el Reial decret 3/2010, que aprova l’Esquema Nacional de Seguretat, pel que fa a (...).

14. En data 29/04/2024, l’Àrea de Tecnologia i Seguretat de la Informació d’aquesta Autoritat va resoldre la qüestió plantejada a l’antecedent anterior.

15. En data 15/05/2024, 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 l’Hospital Clínic de Barcelona havia incorregut, en primer lloc, en una infracció prevista a l’article 83.4.*a* en relació amb l’article 32.1; i, en segon lloc, en una infracció prevista a l’article 83.4.*a* en relació amb l’article 32.2, tots ells de l’RGPD.

Aquesta proposta de resolució es va notificar en data 15/05/2024 i es concedia un termini de 10 dies per formular al·legacions.

16. En data 16/05/2024, l’HCB va sol·licitar l’ampliació del termini atorgat per formular al·legacions, a l’empara de l’article 32 de l’LPAC.

17. En data 17/05/2024, l’Autoritat va acordar l’ampliació sol·licitada.

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

Fets provats

1. L’HCB no va implementar les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat als riscos associats als tractaments de dades que duia a terme per mitjà de la plataforma corporativa atacada. De manera més concreta, l’entitat no va implementar les mesures adequades ni respecte de les dades que tractava com a responsable, ni respecte de les que tractava com a encarregat.

En relació amb aquest extrem, en el marc de la informació prèvia, s’ha constatat que l’Hospital Clínic de Barcelona presta els serveis de seguretat de la informació no tan sols en relació amb les dades tractades en el marc de dita entitat, sinó també en relació amb les entitats vinculades amb la mateixa, d’acord amb el que aquestes han manifestat, i que varen ser igualment objecte de ciberatac.

Aquest és el cas de Barnaclínic, SA, el CAPSBE i la Fundació de Recerca Clínic (FRCB-IDIBAPS), que no disposen d’un sistema d’informació propi, sinó que el servei el presta la Direcció de Sistemes d’Informació (DSI) de l’Hospital Clínic de Barcelona, en virtut d’un acord multilateral d’encarregat del tractament. Aquestes entitats han estat igualment objecte d’investigació en el marc de les corresponents informacions prèvies, a l’efecte de determinar el grau de responsabilitat i participació en les eventuals infraccions que s’hagin comès.

En resum, la responsabilitat que s'atribueix a l'Hospital Clínic de Barcelona deriva, tal com s'ha indicat, de l'incompliment de les seves obligacions com a responsable de tractament, així com de les que va assumir com a encarregat del tractament.

La implementació de mesures de seguretat adequades hauria situat l'HCB i les entitats vinculades en una millor situació de protecció enfront del cibercriminal i, també, en una millor capacitat de detecció i de resposta. Això hauria contribuït a minimitzar els efectes adversos de l'atac per als drets i llibertats de les persones (com a conseqüència de l'atac, es van filtrar dades especialment sensibles i es va interrompre greument el normal funcionament de l'assistència sanitària, a causa de la impossibilitat d'accedir a les dades encriptades).

(...)

Més enllà de les consideracions més generals, de les actuacions dutes a terme i de la documentació analitzada es desprèn que, abans de patir el ciberatac, l'HCB no tenia implementades les mesures de seguretat de prevenció, detecció i contenció que s'indiquen a continuació, essencials per a una prevenció mínima envers els ciberatacs i reacció adequada en cas d'incident:

(...)

2. Amb anterioritat a l'atac, l'HCB no va fer l'anàlisi de riscos necessària per definir les mesures de seguretat aplicables al tractament de dades que duia a terme per mitjà de la plataforma corporativa atacada.

La qualificació jurídica d'aquests fets provats, no ha quedat desvirtuada per les al·legacions que ha presentat l'Hospital Clínic de Barcelona, 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 les al·legacions presentades per l'HCB al llarg d'aquest 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 l'HCB permeten constatar que, (...).

Tanmateix, no és fins el dia 05/03/2023 que l'HCB va notificar a l'Agència de Ciberseguretat de Catalunya l'incident de ciberseguretat sofert, relacionat amb el desplegament de programari de segrest a la infraestructura de l'hospital, (...).

L'incident esmentat també va comprometre 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 aquest sentit, 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, l'HCB 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 de l'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 5.2 i 6.2 d'aquesta resolució, l'HCB no ha acreditat haver analitzat els riscos que s'associaven al tractament de les diferents tipologies de dades personals –dels quals en uns casos era el responsable i, en d'altres, encarregat del tractament–. Per tant, difícilment podia definir i implementar les mesures tècniques i organitzatives adequades en relació amb els riscos existents.

(...) En aquest punt, escau avançar que, malgrat que l'obligació d'adoptar mesures de seguretat constitueixi una obligació de mitjans –i no de resultat–, el cert és que exigeix que s'adoptin mesures 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 encara 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 serveis 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 de 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, extrem que no ha estat rebutjat per part de l'HCB, el nivell mínim exigible era el corresponent al de categoria mitjana, en relació amb el qual s'ha avaluat el compliment o no de les seves previsions per part de l'HCB.

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:

> Article 32
>
> 1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
>
> a) la seudonimización y el cifrado de datos personales;
> b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
> c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

> d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento."
>
> 2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
>
> (...)"

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 l'HCB no va realitzar l'anàlisi de riscos, respecte els tractaments de dades que duia a terme, ni havia implementat les mesures tècniques i organitzatives adequades per protegir la informació que tractava.

En aquest sentit, 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 arran del ciberatac

Aquesta Autoritat no pot ignorar que l'HCB és un centre públic de salut referent 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.

Pel que fa les conseqüències del ciberatac a l'HCB, escau fer notar que, gràcies als esforços ingents del seu personal, l'entitat va poder continuar oferint l'activitat assistencial habitual i va minimitzar el greuge que s'hagués pogut ocasionar a les persones usuàries d'aquests serveis de salut.

Així mateix, tal com s'exposarà amb més detall al fonament de dret 5è d'aquesta resolució, l'Autoritat valora molt positivament les diferents mesures tècniques i organitzatives que l'HCB va adoptar després del ciberatac per tal de reforçar la seguretat dels seus sistemes d'informació, així com la celeritat amb què les va implementar. Entre d'altres actuacions destaquen: (...).

D'acord amb l'anterior, escau subratllar que, actualment, en termes de seguretat l'HCB té un escenari més favorable davant eventuals intents d'intromissió il·lícita als seus sistemes d'informació. En efecte, d'acord amb la documentació aportada al llarg d'aquest procediment sancionador, es constata que, des del moment del ciberatac fins a data d'aquesta resolució, l'HCB ha estat implementant mesures que milloren el nivell de seguretat en el si de la seva organització i sistemes d'informació.

Tanmateix, les actuacions esmentades no desvirtuen els fets que aquí s'imputen, referits a la manca de realització d'una anàlisi de riscos i a la manca d'implementació de les mesures tècniques i organitzatives adequades, que eren exigibles ja abans de la materialització del ciberatac, en compliment de l'RGPD i de l'ENS 2010.

5. Anàlisi de les al·legacions

L'entitat imputada ha formulat al·legacions tant a l'acord d'iniciació com a la proposta de resolució. Les primeres ja es va analitzar en la proposta de resolució, però tot i això es considera procedent tractar-les, atès que en l'escrit d'al·legacions que ha presentat l'entitat en data 06/06/2024 es fa una remissió global al contingut de l'escrit que va presentar en data 08/02/2024 davant l'Autoritat (antecedent 10è). Així, tot seguit s'analitzen el conjunt d'al·legacions formulades per l'entitat imputada.

L'HCB addueix un seguit de consideracions jurídiques i tècniques per defensar la procedència de sobreseure aquest procediment sancionador, atès que, segons afirma, no hi ha indicis racionals d'haver-se produït els fets que van motivar la incoació del procediment. Entre d'altres qüestions, afirma que, d'acord amb l'estat de la tècnica, les mesures que l'HCB havia adoptat eren adequades, i que havia fet l'anàlisi de riscos pertinent.

Tot seguit, a partir del contingut dels informes emesos des de l'Àrea de Tecnologia i Seguretat de la Informació d'aquesta Autoritat (antecedents 11è i 14è) -reproduïts en la part jurídicament rellevant-, es donarà resposta a cadascuna de les al·legacions presentades des d'una perspectiva tècnica pel que fa l'incompliment de l'obligació d'implementar mesures organitzatives i tècniques adequades, d'acord amb l'estat de la tècnica, la naturalesa, l'abast, el context, les finalitats del tractament i els riscos i gravetats variables per als drets i llibertats de les persones.

Igualment, aquest fonament de dret i el fonament jurídic 6è inclouen l'argumentació jurídica per la qual escau concloure que l'HCB no havia fet l'anàlisi de riscos en relació amb els tractaments de dades que duia a terme, ni implementat les mesures de seguretat adequades al risc.

5.1 Sobre la inexistència de mesures tècniques i organitzatives adequades per garantir un nivell de seguretat al risc

Sobre aquesta imputació, l'escrit d'al·legacions que l'entitat va presentar a l'acord d'iniciació d'aquest procediment sancionador posava de manifest que, en base a les anàlisis de riscos que hauria realitzat, va implementar el conjunt de mesures "que va considerar pertinents" per garantir un nivell de seguretat adequat al risc, ja abans de la data en què es va materialitzar el ciberatac descrit a l'antecedent 1r.

Al fil de l'anterior, a l'escrit d'al·legacions de l'HCB presentat davant la proposta de resolució s'hi addueix que l'Autoritat equipara erròniament l'obligació d'implementar les mesures tècniques organitzatives adequades a una obligació de resultat. I afegeix que, complementàriament a les evidències aportades al llarg del procediment, es matisaran diferents aspectes que "no s'haurien valorat per part de l'APDCAT i que acrediten l'existència d'aquestes mesures."

Doncs bé, a continuació s'analitza el conjunt d'al·legacions de l'entitat, en relació amb les diferents mesures tècniques i organitzatives, del que es pot avançar que les mesures que aparentment hauria implementat no eren les legalment exigibles.

5.1.1 (...)

(...)

5.1.2 (...)

(...)

5.1.3 (...)

(...)

5.1.4 (...)

(...)

5.1.5 (...)

(...)

5.1.6 (...)

(...)

5.2 Sobre la manca de realització d'anàlisi de riscos

En l'escrit d'al·legacions de 06/06/2024 s'hi afirma que l'HCB, a banda d'aportar "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, també 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." Respecte d'aquesta qüestió, l'HCB assenyala que el "Pla Director de Seguretat" (doc. 5 de la IP 213/2023) "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".

Així mateix, l'HCB també assenyala que, "d'acord amb el Document núm. 10 de l'Escrit de contestació, la realització d'auditories va contribuir a l'avaluació permanent de l'estat de la seguretat dels actius de l'HCB, 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."

En línia amb l'anterior, també a l'escrit d'al·legacions que l'HCB va presentar en data 08/02/2024 s'hi afirmava que "l'HCB sí que ha tingut en compte els riscos que presenten els tractaments de dades en l'adopció de mesures." Per acreditar-ho, s'adjuntava la còpia de dues avaluacions d'impacte en protecció de dades realitzades els anys 2020 i 2021, relatives a tractaments de dades concrets, així com el document número 13, referit a la "Metodologia interna d'AIPDs." Així mateix, també es feia referència al Pla director de seguretat (doc núm. 5 IP 213/2023), a les auditories de seguretat dels anys 2016, 2018 i 2021 i a la instal·lació d'un EDR, "així com la recepció d'alertes de noves vulnerabilitats i tendències de ciberseguretat."

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 personals (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 –com és el cas de l'HCB– ha de dur a terme l'anàlisi de riscos pertinent. La finalitat d'aquesta anàlisi és mitigar o eliminar la probabilitat que els riscos es materialitzin i, en darrera instància, evitar que es perjudiquin els drets i llibertats de les persones titulars de les dades personals. En aquest sentit, l'anàlisi esmentada és un document que pot aportar prou informació per tal que el responsable del tractament decideixi si cal 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 l'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.

En efecte, l'anàlisi de riscos ha de contenir una aproximació tècnica per identificar els actius més valuosos d'un sistema i les amenaces que poden afectar-los, així com l'impacte que suposaria per als 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 documents, escau evidenciar que l'entitat imputada no ha acreditat que hagi fet l'anàlisi de riscos en relació amb els diferents tractaments de dades personals que duia a terme per mitjà de la plataforma corporativa que va ser atacada. 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, tal com s'afirma al comunicat de l'HCB de 30/03/2023, que s'incorpora a aquest expedient (antecedent 12è), la plataforma que va ser atacada contenia dades identificatives i de salut de pacients, vinculades a tractaments assistencials, així com d'investigació clínica; també, dades personals de treballadors i de tercers col·laboradors interns i externs, així com de proveïdors. En conseqüència, les anàlisis de riscos eren exigibles respecte del tractament de totes aquestes dades.

La rellevància d'efectuar aquesta anàlisi de riscos és encara més evident si es té en compte que, d'una banda, a l'AIPD aportada per l'HCB s'hi descriuen fins a 32 riscos associats a un tractament de dades molt concret –relacionat amb la investigació en projectes de recerca– i que, d'altra banda, ja al document núm. 2, aportat en el marc de la fase d'informació prèvia, s'hi afirmava que: "Todos los sistemas sujetos a esta política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá: Regularmente, al menos una vez al año (...)."

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, en primer terme calia que l'HCB identifiqués i caracteritzés de manera precisa les finalitats de les operacions dels tractaments de dades personals que duia a terme, per mitjà de la plataforma corporativa que va ser atacada. Aquesta eina emmagatzemava dades de tipologia molt diversa, de les quals n'era l'entitat responsable del tractament; però també tractava d'altres dades, per compte de les entitats que s'especifiquen als antecedents (en concret, CAPSBE, FRCB-IDIBAPS i Barnaclínic, SA).

Un cop identificada la finalitat dels diferents tractaments de dades, l'anàlisi dels riscos exigia la descripció concreta del tractament. En efecte, per gestionar les amenaces per als drets i llibertats que representa una determinada operació de dades personals, cal conèixer-ne l'abast i les diferents etapes del tractament. Concretament, les descripcions del tractament de dades inclouen: la seva finalitat; el flux de les dades personals; el cicle de vida de les dades; els rols de les persones que accedeixen a la informació en cada etapa; les característiques de les tecnologies que s'empren; l'extensió o volum d'informació; la periodicitat de recollida de dades; l'extensió geogràfica; el termini de conservació; les comunicacions de dades previstes. Això entre d'altra informació que, en funció de les especificitats dels tractaments, poden caracteritzar-lo.

Per tant l'anàlisi del risc que preveu l'RGPD exigia conèixer l'abast de cadascun dels tractaments que es duien a terme per mitjà de la plataforma corporativa atacada i, tot seguit, identificar les amenaces concretes per a cadascun dels drets i llibertats potencialment afectats, en cada etapa del tractament. Respecte d'aquesta afectació, a més, calia valorar la probabilitat de la materialització del risc i el nivell global d'amenaça per als diferents 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 de tratamiento de datos suponen un riesgo o si el riesgo es alto."

Respecte d'aquest punt, l'HCB pretén considerar acomplerta aquesta obligació a partir del document núm. 5 "Pla Director de Seguretat" de l'any 2018, que al seu punt 2.3 assenyala fins a deu riscos associats als sistemes d'informació de l'entitat. Tanmateix, aquest document, tal com reconeix la mateixa entitat, 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, el document núm. 5 no conté cap referència als drets fonamentals i llibertats que es podien veure potencialment afectats davant una intrusió als sistemes de l'HCB; tampoc no descriu els tractaments de dades concrets que es duien a terme per mitjà de la plataforma corporativa atacada, ni analitzava els riscos en funció del tractament i la tipologia de dades afectades. En les auditories aportades per l'entitat tampoc s'analitzen aquests elements, malgrat que és del tot necessari d'acord amb l'LOPDGDD i l'RGPD.

En aquest context, és evident que la filtració de les dades de salut pot tenir un impacte diferent per als drets fonamentals de les persones que en són titulars, en comparació amb la filtració, per exemple, de dades identificatives de treballadors. I que, per tant, calia analitzar el risc per a cadascun d'aquests tractaments així com la potencial afectació als drets que podien veure's

afectats (dret a la intimitat; dret a la vida; dret a la protecció de dades personals; dret a no ser discriminat, entre d'altres).

D'acord amb l'exposat fins aquí, escau concloure que l'HCB no ha acreditat la realització d'una anàlisi de riscos en els termes exigits per l'RGPD, en connexió amb l'article 28 de l'LOPDGDD.

5.3 Sobre els principis aplicables a l'exercici de la potestat sancionadora

L'HCB afirma que mantenir les imputacions que recullen l'acord d'iniciació i la proposta de resolució d'aquest procediment sancionador seria contrari als principis referits a la potestat administrativa, recollits als articles 25 a 31 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, i torna a insistir en la necessitat de sobreseure aquest procediment. Doncs bé, tot seguit s'analitzen els arguments pels quals aquesta al·legació tampoc pot reeixir.

5.3.1 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, tal com s'assenyalava a la proposta de resolució, i contràriament al que pretén l'HCB, les conductes referides a la manca d'implementació deguda de mesures tècniques i organitzatives apropiades, així com a la manca de realització d'una anàlisi de riscos, constitueixen conductes tipificades d'acord amb l'article 83.4.*a* de l'RGPD. En aquestes circumstàncies, per tot el que s'ha exposat al llarg d'aquesta resolució, s'aprecia identitat entre els seus components fàctics i els elements descrits pel precepte esmentat, en connexió amb l'article 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 es 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 dues infraccions que aquí s'imputen, en consonància amb els fets que han resultat provats.

En darrer terme, l'entitat defensava la seva innocència i argumentava que l'Autoritat no té prou elements probatoris per afirmar que des de l'HCB s'han comès les infraccions esmentades. Respecte d'això, invocava 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. Tanmateix, hi ha la presumpció de "no existència de responsabilitat administrativa" mentre no es demostri el contrari. I, d'acord amb la documentació que l'HCB ha aportat al llarg d'aquest procediment, hi ha prou proves documentals que sostenen les imputacions que s'efectuen en aquest procediment, i que cal atribuir a l'HCB. Proves que no han estat desvirtuades per l'entitat.

5.3.2 Sobre el principi de proporcionalitat

L'HCB assenyalava la importància de tenir present el principi de proporcionalitat, quan una administració pública valora la imposició d'una sanció. En aquest sentit, recordava la línia d'argumentació seguida per l'Audiència Nacional (Sala del Contenciós Administratiu, Secció 1a) de 21/11/2017 (recurs núm. 208/2014), que sostè que l'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 l'HCB 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, l'HCB assenyala 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 els principals afectats van ser 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 indicava que, encara durant el primer trimestre del 2023, la Covid-19 era la primera causa de mortalitat a Espanya i que, durant l'any 2022, hi va haver noves onades d'infeccions que van provocar que els hospitals públics "estiguessin recurrentment col·lapsats." Amb tot, les mesures que aquests centres sanitaris van haver d'adoptar van suposar una gran inversió de recursos i centrar esforços en l'atenció dels pacients i el correcte desenvolupament de la sanitat pública. Tot seguit, l'HCB destacava que, entre els anys 2020 i 2023, es van adoptar diferents mesures legislatives encaminades a flexibilitzar diversos aspectes de l'activitat de les administracions públiques, com ara la suspensió de terminis per interposar recursos contenciosos administratius. D'acord amb aquestes actuacions, considera desproporcionada "la conclusió de l'APDCAT respecte a la falta de mesures de seguretat en relació amb les dades personals tractades per l'entitat, tenint en compte el context de dificultat anteriorment descrit. Aquest argument, a més, es veu reforçat si tenim en compte que l'entitat a qui ara s'exigeix que hauria d'haver implementat certes mesures de seguretat, es tracta d'un hospital públic."

L'entitat imputada també indica que, amb anterioritat al març de 2023, "havia patit ciberatacs que va poder evitar gràcies a les mesures implementades", i indica que la sofisticació de l'atac patit al març de 2023 i la tecnologia que s'hi va emprar han de ser elements a tenir en compte a l'hora de valorar la diligència de l'HCB. Així mateix també assenyala que, ja abans de l'incident, havia implementat les mesures que s'emmarquen en el llistat de recomanacions emès per l'Agència de la Unió Europea de Ciberseguretat, l'any 2023. (...)

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, a 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 que imposi 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 l'HCB, aquesta Autoritat és coneixedora de les nombroses dificultats amb què es van trobar els centres sanitaris durant la situació de pandèmia sanitària ocasionada per la Covid-19, que els va obligar a implementar noves fórmules organitzatives per preservar la continuïtat de l'atenció sanitària. Tanmateix, l'excepcionalitat d'aquestes circumstàncies no eximeix els responsables del tractament de continuar garantint el dret fonamental a la protecció de dades personals. I, en aquest sentit, el fet que s'aprovessin determinades mesures de flexibilització administrativa –com ara la suspensió de terminis durant un període concret– tampoc eximia els responsables del tractament de les seves obligacions en matèria de protecció de dades. Més encara en un context en què el nombre de ciberatacs va augmentar, tal com s'afirma al mateix escrit d'al·legacions aportat per l'HCB.

De fet, cal tenir ben present que –tal com s'ha avançat en aquesta resolució- la manca de la implementació deguda 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, l'HCB havia de protegir els seus sistemes d'informació d'acord amb les previsions de l'ENS 2010 i l'RGPD. 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 eximeix l'HCB de la seva responsabilitat respecte dels fets imputats, que venia 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.

En darrer terme, l'entitat imputada insisteix en la necessitat d'interpretar l'estat de la tècnica en consonància amb el principi de proporcionalitat. Sobre això, afegeix que una eventual sanció sobre la base d'una bretxa de seguretat, causada per un esdeveniment fortuït, implicaria configurar l'obligació d'implementar mesures tècniques i de seguretat com una obligació de resultats. Aquest fet, segons assenyala l'HCB, suposaria invalidar "tot l'esforç i inversió tecnològica i organitzativa realitzats i desincentivar la presa de mesures de prevenció i seguretat (...)." A l'anterior, l'HCB afegeix 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, en el cas d'altres incidents molt similars, no hi ha hagut conseqüències més enllà de l'incident de seguretat.

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

Al fil de l'anterior, aquesta resolució –com també l'acord d'iniciació d'aquest procediment i la proposta de resolució que la precedeix– 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 l'HCB; 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 el principi esmentat.

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 de l'HCB, en termes de proporcionalitat, no tan sols pel temps transcorregut, sinó per l'entitat dels incompliments.

Així mateix, escau posar de manifest que aquest procediment no s'inicia pel fet que l'HCB hagi estat víctima d'una violació de seguretat, sinó que els fets que se li imputen són la manca de mesures tècniques i organitzatives exigibles, d'acord amb el marc normatiu referit al llarg d'aquesta resolució, així com la manca de realització d'una anàlisi de riscos. Respecte d'això, escau destacar que, a banda de la notificació de la violació de seguretat feta pel mateix HCB, en data 05/07/2023 una tercera persona va presentar una denúncia davant l'Autoritat que comportava necessàriament l'obertura d'una fase d'informació prèvia, per investigar els fets que han donat lloc a l'inici d'aquest procediment (antecedent 5è).

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 l'HCB, ja molt abans del ciberatac del mes de març de 2023, no havia implementat degudament les mesures que li eren exigibles d'acord amb l'RGPD i l'ENS 2010, i tampoc no havia realitzat la anàlisi de riscos pertinent en relació amb el tractament de dades personals que duia a terme.

5.3.3 Sobre el principi de culpabilitat

Tot seguit, l'HCB adduïa que el principi de culpabilitat impedeix sancionar-lo i que sostenir el contrari suposaria exigir un grau de diligència inassumible, que no és proporcional tenint en compte la naturalesa d'entitat pública de l'HCB i les circumstàncies descrites amb anterioritat (vid. 5.3.2). En aquests termes, l'entitat cita diferents sentències en base a les quals l'apreciació d'aquest principi està condicionada a l'existència de dol, culpa "o, fins i tot una ignorància inexcusable." Segons assenyalen, reforça aquest posicionament el fet que l'HCB és una entitat adherida al codi tipus de la Unió Catalana d'Hospitals, per contribuir a la correcta aplicació de l'RGPD i, segons s'afirma, aquesta adhesió suposaria que s'ha superat satisfactòriament la revisió del compliment dels requisits bàsics en matèria de protecció de dades.

D'acord amb l'exposat, l'HCB sosté que l'eventual imposició d'una sanció implicaria una vulneració del principi de culpabilitat, que regeix en el dret administratiu sancionador.
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."

En aquest sentit, considera que, per atribuir la responsabilitat per les infraccions comeses al seu autor, cal que hi concorri l'element de culpa, dins del qual hi 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 en què l'HCB coneixia la insuficiència d'implementació de les mesures de seguretat en diferents períodes temporals –totes elles anteriors a la materialització del ciberatac del març de 2023-. A tall d'exemple, (...). Totes aquestes inobservances 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 al llarg d'aquesta resolució, escau concloure que l'Autoritat no comparteix que l'HCB actués de manera diligent en la implementació i aplicació de mesures de seguretat –tant tècniques com organitzatives–, respecte dels tractaments de dades personals que duia a terme per mitjà de la plataforma corporativa que va ser atacada. En conseqüència, es considera que les imputacions que s'efectuen no contravenen el principi de culpabilitat, en els termes que planteja l'HCB.

5.3.4 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, l'HCB considera que quan l'Agència de Ciberseguretat de Catalunya va elaborar el seu 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'administrat que les mesures que havia implementat eren suficients i que l'incident no comportaria represàlies, com la que suposa que aquesta Autoritat iniciés un procediment sancionador.

En relació amb l'anterior, l'HCB afegeix que, d'acord amb les conclusions de l'esmentat informe, "amb caràcter previ al ciberatac, comptava amb mesures de detecció i prevenció, així com amb una arquitectura i estratègia de ciberseguretat." En conseqüència, considera que les imputacions que aquí s'efectuen contradiuen les conclusions de l'informe, que consideraven que la seva actuació era ajustada a dret.

En darrer terme, l'entitat argumenta 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 (...) que es veu posteriorment frustrada en veure's front una possible sanció per la presumpta inadequació de les mateixes."

En resposta als aspectes plantejats per l'HCB, 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 conforme la qual les mesures que havia implementat l'HCB eren suficients. Respecte d'aquesta circumstància escau fer notar que, malgrat que l'entitat argumenti que, precisament, en base a aquesta confiança va assumir "que l'incident no comportaria represàlies", el cert és que l'entitat coneixia la fase d'informació prèvia que va iniciar aquesta Autoritat i que podia derivar amb l'inici d'aquest procediment.

Per altra banda, el fet que l'acord d'iniciació del procediment sancionador es notifiqués a l'HCB al mes de gener de 2024 no és un element que permeti sostenir el pretès "trencament de la confiança que havia dipositat en l'HCB." Des del moment en què l'Autoritat va tenir coneixença de l'abast del ciberatac, va iniciar una investigació per valorar les circumstàncies del cas i la situació de l'HCB en termes de seguretat. Aquesta circumstància era del tot coneguda per l'HCB i, per aquest motiu, en cap cas es pot afirmar que l'inici d'aquest procediment fos un fet inesperat per a l'entitat, que vulnerés l'article 3.1.*e* de la Llei 40/2015.

A més, al marge del que s'ha exposat anteriorment, al llarg de la tramitació de la notificació de violació de seguretat per part de les entitats afectades l'APDCAT va donar un suport continu a l'HCB i, fins i tot, en algun ofici de requeriment d'informació se'ls va traslladar que la prioritat temporal era la restitució i el restabliment dels serveis, així com la protecció dels afectats. Això traslladava, com no podia ser d'altra manera, que aquesta primera prioritat obligava a posposar-ne d'altres no prioritàries en el temps, com va ser la informació prèvia oberta i la posterior tramitació del procediment sancionador, que ara ens ocupa.

En resum, ni es produeix 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 adopten els mínims estàndards de seguretat legalment exigibles per protegir-ne aquelles.

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

5.4 Altres qüestions

5.4.1 Sobre l'estat de la tècnica

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

Doncs bé, tal com s'ha argumentat a l'apartat 5.3.2 d'aquesta resolució, referit a la proporcionalitat de la sanció, l'HCB va ometre una obligació que venia de lluny. Cal tenir en compte que la implementació deguda de les mesures tècniques i organitzatives que aquí se sanciona no és una obligació exigible arran de la Covid-19, sinó que, ja abans de la situació de

crisi sanitària, l'HCB ja havia d'haver adoptat una major seguretat per als seus sistemes d'informació i, en darrer terme, per als drets i llibertats dels titulars de les dades personals. Respecte d'això, tal com s'assenyalava a la proposta, tampoc es pot compartir que existís una dificultat tècnica o econòmica insalvable per prendre determinades mesures tècniques i organitzatives, si tenim en compte que aquestes mesures es van implementar immediatament després del ciberatac. A títol d'exemple, (...).

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 pressupostària o la complexitat del ciberatac sofert no constitueixen factors eximents de la responsabilitat de l'HCB per la manca d'atenció de l'obligació prevista per la normativa esmentada.

Pel que fa a l'estat de la tècnica, l'HCB insisteix que 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 ha imputat a l'HCB la seva manca de certificació d'acord amb l'ENS. De fet, aquesta és una circumstància que únicament l'ha plantejat el mateix HCB. 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-les i, d'altra banda, a la seva configuració com a paràmetre de referència envers les mesures tècniques i organitzatives que eren adequades i necessàries, d'acord amb l'estat de la tècnica.

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.

5.4.2 Sobre la presumpta indefensió causada per la proposta de resolució

En darrer terme, l'HCB 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 per justificar que ha vulnerat els principis aplicables a la potestat sancionadora de l'Administració. Respecte d'aquest fet, l'HCB argumenta que, 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 l'HCB, 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 jurisprudencials que segons l'HCB li hauria causat indefensió no és tal, tenint en compte que l'Autoritat ha argumentat abastament el seu posicionament jurídic en les 37 pàgines de la seva proposta de resolució, així com també en aquest acte administratiu. L'HCB és plenament coneixedor 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.

Més enllà del que s'ha exposat, no escau entrar a valorar amb més deteniment si les diferents referències jurídiques incloses a la proposta de resolució són suficients, quan el mateix HCB ha reconegut que la presumpta manca de recursos doctrinals i jurisprudencials no van afectar la motivació de la proposta i, en aquest sentit, si l'entitat admet que la resolució es troba motivada, no s'arriba a entendre que consideri que no pot conèixer la ratio decidendi, o que la resolució sigui arbitrària, quan a l'escrit d'al·legacions, d'altra banda, no ha rebatut cap dels extrems que, com incompliments greus en matèria de seguretat, li són imputables.

Tot seguit, l'HCB 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 concret, 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 l'HCB no ha tingut accés, no va respectar els drets d'audiència i de bona fe de les administracions públiques. En relació amb l'anterior, l'HCB considera que no és ajustat a dret fonamentar arguments centrals 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 apartat de la proposta s'exposa "quina va ser la conclusió o el sentit de tals pronunciaments" de l'Àrea de Tecnologia i Seguretat de la Informació de l'Autoritat.

Per recolzar la seva argumentació, l'HCB cita la sentència del Tribunal Suprem de 30 de juny de 2011 (recurs 2682/2009), en què s'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 constitutius 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 de resolució incorpora el contingut dels aspectes tècnics de l'informe. De fet, s'hi incorpora tota la informació necessària per justificar la decisió de l'Autoritat – tant en la Proposta de resolució, com en aquest acte administratiu -. La suficiència de l'explicació de cada raonament, impedeix sostenir que l'entitat desconeix el contingut de l'Informe esmentat, el qual s'ha incorporat a la proposta de resolució i serveix de motivació a aquesta.

Vinculat amb l'anterior, l'HCB addueix que la Proposta no recull "el sentit de tals pronunciaments" en referència a l'Informe de l'Àrea de Tecnologia i Seguretat d'aquesta Autoritat i que tampoc inclou la conclusió d'aquest. Tanmateix, aquestes afirmacions no s'ajusten a la realitat dels fets tenint present que, d'una banda, l'antecedent 11è de la Proposta – i també d'aquesta Resolució - transcriu en termes literals la conclusió a la què va arribar l'Àrea esmentada, i que conté nombroses remissions literals i referències explícites a l'Informe. En darrer terme, cal fer avinent que, l'HCB – com a part interessada en aquest procediment – podia accedir a qualsevol document d'aquest procediment sancionador i que, en cap moment, va exercir l'accés.

D'acord amb l'exposat, escau concloure que, la proposta de resolució fixa de manera motivada els fets i la seva qualificació jurídica, determina la infracció que constitueixen i el subjecte que n'és responsable, estableix la sanció proposada i conté una àmplia argumentació respecte dels fonaments bàsics de la resolució que es proposa.

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

6. Qualificació jurídica dels fets provats

6.1 Fet provat 1r

En relació amb el fet descrit al punt 1r de l'apartat de fets provats, relatiu a la manca d'implementació de mesures tècniques i organitzatives adequades, cal acudir a l'article 32.1 de l'RGPD, transcrit al punt 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 l'obligació d'adoptar mesures tècniques i organitzatives. En aquest sentit, les Directrius 4/2019 del Grup de treball 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 i 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 5è d'aquesta resolució, l'HCB ha adduït diferents situacions que, al seu parer, demostren que havia implementat 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 assenyalar 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, com pretén l'HCB. La seguretat, en definitiva, és un concepte integral, que 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 de seguretat que, fins aleshores, no s'havien implementat per diferents motius, com ara "dificultats pràctiques." A tall d'exemple, tal com ja s'ha avançat al punt 5.1.1 d'aquesta resolució, per contenir i erradicar l'impacte del ciberatac es va desplegar la tecnologia (...); per tant, no es pot sostenir que abans del ciberatac aquesta mesura constituís un "repte difícil d'assumir." Així mateix, també és van implementar altres mesures de seguretat com ara (...) o bé (...).

En aquest punt, escau indicar que, tal com s'argumenta a la sentència núm. 188/2022, de 15 de febrer, del Tribunal Suprem (Recurs núm. 7359/2020), invocada per l'HCB, 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, i 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 unas 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 emmagatzemaven els sistemes d'informació de l'HCB, 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 l'HCB ha defensat la pertinença de les mesures implementades, 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 març de 2023, aquestes mesures no eren les apropiades per garantir un nivell de seguretat adequat al risc.

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", entre les quals s'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, aquests preceptes s'han 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.

En efecte, l'RGPD parteix d'una concepció basada en la gestió dels riscos associats als tractaments de dades personals. Aquest enfocament es refereix directament a la necessitat de disposar de sistemes preventius tendents a minimitzar els riscos per als 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 la 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 a 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, tal com s'ha exposat a l'apartat 5.2 d'aquesta resolució, l'HCB no ha aportat cap evidència que permeti constatar que va fer una anàlisi de riscos en relació amb el tractament de dades personals que duia a terme per mitjà de la plataforma corporativa atacada.

No es pot obviar que els tractaments de dades que efectuava l'HCB –tant en la seva condició de responsable com d'encarregat del tractament– entren dins dels supòsits especificats als apartats *a* a *f* de l'article 28.2 de l'LOPDGDD; per tant, per definir les mesures adequades calia tenir en compte els riscos superiors que es podien materialitzar. 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 que conté 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.

Durant la tramitació d'aquest procediment s'ha acreditat el fet recollit al punt 2 de l'apartat de fets provats, que 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, de la manera 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."

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. A més, pot proposar, si escau, la iniciació d'actuacions disciplinàries d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. Aquesta resolució s'ha de notificar a la persona responsable del fitxer o del tractament, a l'encarregada del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha".

La proposta de resolució proposava requerir l'HCB 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 que es dicti en aquest procediment, aportés un cronograma en què s'indiquin els terminis que necessita per realitzar les anàlisis de riscos associades als tractaments de dades personals que duu a terme per mitjà de la plataforma corporativa que va ser atacada, així com per implementar les mesures que es preveuen al pla proposat per l'Agència de Ciberseguretat de Catalunya, entre d'altres mesures que calgui implementar d'acord amb els resultats de les anàlisi de riscos.

Doncs bé, l'escrit que l'entitat ha presentat davant la proposta de resolució s'acompanya d'un "relat sobre el pla d'acció adoptat arran de l'incident", en què s'indiquen les actuacions dutes a terme des del mes de juny de 2023 fins el mes de maig de 2024. També ha aportat un cronograma, en el qual s'identifiquen les actuacions que s'han de dur a terme els anys 2024, 2025 i 2026, amb la finalitat de millorar la seguretat dels sistemes de l'HCB. En aquest cronograma s'hi preveu, entre d'altres actuacions, la realització d'anàlisis de riscos en relació amb els drets i llibertats de les persones titulars de les dades objecte de tractament.

D'acord amb la documentació rebuda, es constata que l'HCB ja ha implementat diverses mesures tècniques i organitzatives enfocades a la millora de la seva seguretat. Així mateix, també es descriuen d'altres millores que s'han d'implementar entre els anys 2024, 2025 i 2026, que s'estima que permetrien corregir les deficiències en matèria de seguretat, detectades al llarg d'aquest procediment.

Tanmateix, als efectes de fer un seguiment sobre la implementació d'aquestes mesures, escau requerir l'HCB perquè informi anualment (juliol 2025 i 2026) a l'Autoritat sobre el grau d'implementació de les actuacions previstes al cronograma, per mitjà d'una certificació que identifiqui quines han estat degudament implementades. 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 l'Hospital Clínic de Barcelona ha comès dues infraccions: una infracció prevista a l'article 83.4.*a* en relació amb l'article 32.1 i una altra infracció prevista a l'article 83.4.*a* en relació amb l'article 32.2; tots ells de l'RGPD.

2. Requerir a l'Hospital Clínic de Barcelona perquè adopti la mesura correctora assenyalada al fonament de dret 7è, i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-la.

3. Notificar aquesta resolució a l'Hospital Clínic de Barcelona.

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