Número de l'expedient: 002-024_B3

RESOLUCIÓ DEL RECURS DE REPOSICIÓ

Andorra la Vella, el 8 d'abril del 2025,

Examinat el recurs de reposició interposat per ANDORRA TELECOM, SAU, responsable de tractament, contra la resolució dictada per la cap de l'Agència Andorrana de Protecció de Dades en data 27 de febrer del 2025, i sobre la base dels següents;

I

ANTECEDENTS

PRIMER.- Els dies 8 i 9 de novembre del 2024, arran de diverses notícies aparegudes als mitjans de comunicació sobre una presumpta violació de la seguretat de les dades personals d'ANDORRA TELECOM, SAU, en què ciberdelinqüents accedien indegudament a comptes d'alguns clients, comprometent la confidencialitat i integritat de les seves dades personals, el servei d'inspecció va detectar diversos possibles incompliments de la LQPD per part d'aquesta entitat.

Vista la gravetat dels fets i que el servei d'inspecció no havia tingut en cap moment constància de la notificació d'aquesta violació de seguretat per part d'ANDORRA TELECOM, SAU, el servei d'inspecció decidí actuar d'ofici i verificar quines havien sigut les possibles vulneracions de la LQPD.

SEGON.- En data de 20 de novembre del 2024, el servei d'inspecció de l'APDA presentà a la cap les actuacions prèvies a l'autorització d'inspecció.

TERCER.- En data de 21 de novembre del 2024, la cap signà l'autorització d'inspecció.

QUART.- En data de 4 de desembre del 2024, el servei d'inspecció de l'APDA envià el requeriment d'informació a ANDORRA TELECOM, SAU, sol·licitant la informació següent:

- *"Explicar com es dona compliment als principis relatius al tractament de les dades personals en els procediments objecte d'aquesta investigació;*
- *Explicar com es va aplicar la protecció de les dades personals des del disseny i per defecte en els procediments objecte d'aquesta investigació;*
- *Aclarir els motius pels què no es va notificar a l'autoritat de control la violació de la seguretat de les dades personals, dins del termini establert a la LQPD;*
- *Aclarir si es va comunicar l'incident als afectats, i si és el cas, aportar les evidències que ho demostrin. En cas de no haver comunicat als interessats, explicar-ne els motius;*
- *Presentar un informe explicatiu que contingui, com a mínim, la informació del formulari de violacions de seguretat que posa a disposició l'APDA aportant les evidències necessàries que demostrin el compliment de la LQPD;*
- *Aportar els protocols establerts per l'entitat per gestionar violacions de la seguretat de dades personals;*
- *Aportar tota altra informació que es consideri escaient."*

CINQUÈ.- En data de 23 de desembre del 2024, ANDORRA TELECOM, SAU sol·licità una ampliació del termini de resposta al requeriment d'informació, i l'APDA concedí set dies hàbils de pròrroga.

SISÈ.- En data del 8 de gener de 2025, ANDORRA TELECOM, SAU respongué al requeriment d'informació argumentant set punts en la seva carta.

SETÈ.- El 27 de gener del 2025, el servei d'inspecció presentà la proposta d'incoació d'expedient administratiu a ANDORRA TELECOM, SAU a la cap de l'APDA.

VUITÈ.- El 4 de febrer del 2025, la cap de l'APDA emeté l'aute d'incoació d'expedient contra ANDORRA TELECOM, SAU per detectar les possibles infraccions descrites als articles 72.1.a., 72.2.e, 72.2.k i 72.2.l i donant el termini improrrogable de 10 (deu) dies hàbils a comptar des de la des de l'endemà de la seva recepció, perquè el responsable de tractament examinés l'expedient, al·legués i presentés els documents i les justificacions que considerés pertinents per a la millor defensa dels seus drets.

Pel que fa la infracció 72.1.a. *"El tractament de dades personals que vulneri l'article 5"* es va constatar que el responsable de tractament va incomplir el principi d'exactitud, perquè les dades tractades havien resultat incorrectes en relació amb la identitat real dels usuaris. ANDORRA TELECOM, SAU hauria d'haver implementat mecanismes suficients per verificar amb precisió la identitat dels sol·licitants i evitar errors que finalment, van comprometre la seguretat de les dades dels seus usuaris.

El responsable de tractament també va vulnerar el principi d'integritat i confidencialitat, ja que va permetre a tercers no autoritzats accedir a les dades i gestionar serveis en nom d'altres persones posant en risc la protecció de la informació. Així, ANDORRA TELECOM, SAU no va garantir mesures de seguretat adequades per evitar accessos fraudulents i possibles danys als afectats.

Per la seva banda, el responsable de tractament no va poder demostrar el compliment del principi de responsabilitat proactiva. En aquest context, el fet que una tercera persona hagués pogut suplantar la identitat del client i sol·licitar l'eSIM demostrava una manca de controls adequats en el procés d'autenticació. ANDORRA TELECOM, SAU hauria d'haver implementat mecanismes més robustos per verificar la identitat dels seus usuaris, com

l'obligatorietat de la doble autenticació, evitant així el risc de frau. Es va recordar que la responsabilitat proactiva no es limita a reaccionar davant d'incidents, sinó que implica anticipar i prevenir possibles vulneracions de seguretat per protegir els drets dels afectats.

En relació amb les infraccions 72.2.k. *"La falta d'adopció de les mesures tècniques i organitzatives apropiades per garantir que, per defecte, només es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament o que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament"* i 72.2.l. *"L'incompliment, com a conseqüència de la falta de la diligència deguda, de les mesures tècniques i organitzatives que s'hagin implantat"* ANDORRA TELECOM, SAU no va demostrar complir amb els seus deures i obligacions com a responsable del tractament, ni l'aplicació de la protecció de dades des del disseny i per defecte ni tampoc de les mesures de seguretat i confidencialitat del tractament perquè no va adoptar mesures tècniques i organitzatives suficients per garantir la seguretat en el tractament de dades personals. A més, l'absència inicial d'un sistema de doble factor d'autenticació, per a accions crítiques com el canvi de correu electrònic o la sol·licitud d'una eSIM, posava de manifest una manca d'avaluació adequada dels riscos associats a aquests processos.

Finalment, en referència a la infracció 72.2.e *"Incomplir els deures de notificació o de comunicació d'una violació de la seguretat de les dades personals"* l'APDA va concloure que l'incident representava una violació de la seguretat de les dades personals que constituïa un risc per als drets i les llibertats de les persones físiques, i que el responsable de tractament no ho va notificar a l'APDA en els termes establerts a la LQPD.

NOVÈ.- El 14 de febrer del 2025, ANDORRA TELECOM, SAU presentà el seu escrit d'al·legacions:

> *"Primer.- En primer lloc, tot i que aquesta part entén que no hi ha hagut un incompliment de la normativa de protecció de dades i que hem*

actuat amb la màxima diligència possible, des d'Andorra Telecom hem procedit a implementar les diverses mesures indicades en el seu escrit d'incoació d'expedient administratiu, actualitzant el procés intern per tal que es compleixi amb els principis de tractament, implementant formacions específiques als agents telefònics i revisant el protocol intern de gestió d'incidents de seguretat; en base al nostre ferm compromís amb el compliment de la protecció de dades i amb la màxima voluntat de que no tornin a succeir situacions similars en el futur.

Segon.- Addicionalment, aquesta part vol fer constar que Andorra Telecom no ha sigut l'entitat responsable de la comissió del dany que motiva la incoació de l'expedient. L'incident en qüestió es deu a un frau realitzat per un tercer mitjançant enginyeria social, un fet que afecta tant l'Empresa com als clients implicats. En aquest sentit, Andorra Telecom també és una víctima, atès que ha estat objecte d'un intent de frau extern, el qual està actualment judicialitzat.

En aquest sentit, des del moment que vam conèixer els fets succeïts, des d'Andorra Telecom vam realitzar un anàlisis del risc i, en especial, vam analitzar i assegurar l'adopció de les mesures de protecció i l'aplicació d'aquelles mesures que garantissin la no materialització d'un alt risc per als drets i les llibertats de les persones interessades, en aplicació de l'article 36 i 37 de la LQPD, tal com es detallarà al llarg del present escrit. Aquest incident no ha estat causat per una vulneració dels sistemes informàtics ni per cap actuació impròpia de l'Empresa, sinó per la utilització fraudulenta de dades prèviament compromeses per part de tercers desconeguts, els quals ja disposaven de les dades personals dels afectats.

Així mateix, tractant-se d'un cas d'enginyeria social del qual fórem víctima, vam realitzar tots els nostres esforços per a garantir la

minimització del dany. A tal efecte, entre d'altres mesures, ho vam posar immediatament en coneixement de l'Agència Nacional de Ciberseguretat d'Andorra ("ANC-AD"), entitat estatal encarregada de planificar, coordinar, gestionar i controlar la ciberseguretat de xarxes i sistemes d'informació; vam posar-nos en contacte amb la globalitat d'usuaris que podrien haver estat afectats, incloent també tots aquells que van migrar SIM a E-SIM durant dies anteriors a la producció de l'engany; vam suspendre immediatament qualsevol migració de SIM a E-SIM; vam incorporar mesures addicionals per a la protecció de la seguretat en l'accés, entre moltes d'altres.

Andorra Telecom ha actuat en tot moment amb la màxima diligència i ha sigut una víctima més d'uns fets que, presumptament, poden ésser considerats de frau o estafa. Així mateix, hem garantit en tot moment els principis de protecció del tractament de les dades personals previstos, entre d'altres, a l'article 5 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals ("LQPD").

Tercer.- L'APDA ha decidit incoar un expedient sancionador contra Andorra Telecom en base, entre d'altres, a unes notes de premsa que fan referència a uns fets actualment judicialitzats, dels quals es desconeix, pel moment processal en el què es troben, la seva autoria, la forma de realització de l'eventual fet delictiu, els mecanismes que els presumptes infractors van usar per a cometre dits fets o les conseqüències generades, entre d'altres.

En conseqüència, com ja vàrem manifestar en el nostre escrit d'al·legacions de data 8 de gener d'enguany, aquestes informacions poden contenir errors o ser esbiaixades, tant pel fet que les notes de premsa contenen informació no exacta, com pel fet que els fets es troben actualment en fase d'instrucció i, per tant, d'investigació per part de les autoritats competents.

Addicionalment, força és de constatar que en el nostre escrit d'al·legacions, informàvem a l'APDA de que posàvem a la seva disposició tota la informació de que disposem sobre l'assumpte. No obstant, sense haver procedit al seu anàlisis, es decideix incoar l'expedient administratiu que fa objecte del present, donant-se una situació d'indefensió per part nostra.

Pels motius ans exposats, analitzats globalment, aquesta part sol·licita respectuosament l'arxiu immediat de l'expedient administratiu (expedient 002 – 024), sense ulteriors conseqüències jurídiques.

Quart.- Addicionalment, tal com vàrem exposar en el nostre escrit d'al·legacions, Andorra Telecom ha complert amb els principis de tractament de les dades personals previstos, entre d'altres, a l'article 5 de la LQPD, tot en base als següents motius:

1.- Aquesta part es reitera en que en el present cas, no s'ha produït una "Violació de la seguretat de les dades personals", que l'article 4.13 de la LQPD defineix com "qualsevol violació de la seguretat que ocasiona, de manera accidental o il·lícita, en tot cas no autoritzada, la pèrdua, l'alteració, o la divulgació de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzat a aquestes dades".

En el present cas no hi ha hagut una violació de la seguretat ni un accés indegut als sistemes informàtics que permetin l'accés a dades personals d'usuaris d'Andorra Telecom, sinó que aquestes dades personals ja eren conegudes prèviament per part dels infractors, els quals, utilitzant aquestes dades, han pogut accedir a una targeta E-SIM. Per tant, no existeix en aquest cas una "pèrdua, alteració o divulgació de dades personals transmeses, conservades o tractades d'una altra manera", sinó que les dades personals que ja disposava l'eventual infractor, els han permès cometre un fet eventualment delictiu, produint

engany tant a Andorra Telecom com a diverses entitats bancàries del país.

2.- En l'aute d'incoació d'expedient, s'argumenta que Andorra Telecom no ha complert, entre d'altres, amb els principis d'exactitud, integritat i confidencialitat, responsabilitat proactiva, seguretat i confidencialitat del tractament, bàsicament pel fet que les mesures adoptades per l'Empresa no han sigut suficients per evitar la producció dels fets d'autes.

Durant el transcurs del frau els agents del CAT van atendre 60 trucades dels defraudadors, de les quals 4 ens consta que van implicar un frau econòmic al client. Les mesures proactives definides per disseny i per defecte, si bé no van ser suficients per evitar tots els intents de fraus, considerem que van permetre evitar un impacte que hagués estat de ben segur molt superior. Recordem que la resta de casos de frau informats als mitjans de comunicació s'haurien materialitzat sense la intervenció d'Andorra Telecom.

Aquesta part vol recordar que el fet que un tercer hagi dut a terme un fet eventualment delictiu i s'hagi produït engany en els nostres agents telefònics, tal extrem no suposa que Andorra Telecom hagi incomplert amb els principis de tractament de dades personals previstos a l'article 5 de la LQPD. Al contrari, és per causa d'un fet aliè a Andorra Telecom que s'han produït aquests fets. Aquests successos només s'han produït un cop al llarg de dècades de prestació del servei públic universal de telecomunicacions, i és degut a un fet eventualment delictiu extern a l'Empresa. Addicionalment, tant amb caràcter previ com posterior a la producció d'aquests fets, hem assegurat l'adopció de les mesures de protecció i l'aplicació d'aquelles mesures que garanteixen que no es materialitzi un alt risc per als drets i les llibertats de les persones

interessades, amb la màxima diligència possible, entre les quals destaquen les següents,

Mesures existents abans de la producció del dany

Entre d'altres mesures existents abans de produir-se el dany, destaquen les següent:

(a) Les dades personals de què disposem es processen exclusivament per a finalitats legítimes, com la gestió i prestació dels serveis contractats. Els clients són informats de manera clara i transparent a través dels termes i condicions de servei i les nostres polítiques de privacitat, disponibles als canals oficials de comunicació. Les dades personals només es tracten amb la finalitat per la qual van ser recollides. Només es processen les dades estrictament necessàries per a identificar els clients i gestionar les seves sol·licituds.

(b) En tots els casos d'altes o canvis de SIM a E-SIM, els nostres operadors sol·liciten diverses dades per poder contrastar la identitat dels usuaris, essent aquestes el nom complet, cognoms, número de telèfon i document identificatiu (DNI, passaport o número de cens).

(c) En casos sospitosos o d'anomalies, es demanen dades addicionals com l'adreça, la data de naixement i els últims 4 dígits del compte bancari associat. Els sistemes interns que gestionen aquestes dades estan protegits per controls d'accés basats en rols, limitant la consulta i modificació de dades al personal estrictament autoritzat.

Mesures dutes a terme després de la producció del dany

Des del moment en que vam conèixer els fets,

(a) Vam fer que els agents generessin una trucada sortint cap el titular dels serveis abans d'efectuar una migració de SIM física a eSIM (tarja virtual). Aquesta mesura va permetre detectar tots els intents posterior de suplantació dels clients. Val a dir però que, un mes després del frau,

els defraudadors van continuar fent trucades per a intentar suplantar els clients i, per a evitar qualsevol risc d'error humà per part dels agents telefònics, es va acordar suspendre immediatament aquesta operativa des del CAT fins a nova ordre.

(b) Vam informar-ho immediatament a l'Agència Nacional de Ciberseguretat d'Andorra ("ANC-AD"), entitat estatal encarregada de planificar, coordinar, gestionar i controlar la ciberseguretat de xarxes i sistemes d'informació.

(c) Vam notificar a tots els usuaris que podrien ésser afectats, que s'havia produït un fet que podria ésser constituït d'un frau. Aquesta comunicació es va realitzar a tots els usuaris que havien fet migracions durant dies anteriors a la producció del dany.

(d) Vam posar-nos a disposició de les autoritats judicials competents i, per mediació de l' ANC-AD, hem estat en contacte amb les entitats bancàries que també foren afectades per aquests fets, cooperant amb tots ells per a l'esclariment dels fets i la minimització dels danys.

(e) Vam exigir que en endavant, qualsevol nova migració de SIM a E-SIM s'hagi de realitzar presencialment, a les oficines comercials de l'Empresa.

(f) Vam incorporar l'obligatorietat del doble factor d'autenticació (2FA) per a realitzar modificacions de les dades personals de contacte associades als comptes dels clients des del portal del client.

(g) Vam adaptar i complementar el procediment d'autenticació dels clients, per tal de mitigar aquest nou tipus de frau, en relació a la realització de trucades sortints exposades al punt (a).

(h) Vam organitzar formacions específiques per als nostres agents, de tal forma que comptin amb coneixement concret davant d'aquest tipus de frau.

(i) Vam adaptar els nostres protocols interns per a garantir el coneixement d'aquestes situacions per part de tota la companyia.

En definitiva, Andorra Telecom ha realitzat les màximes mesures de protecció i de diligencia deguda per a minimitzar la materialització d'un alt risc per als drets i les llibertats de les persones interessades, sense que això pugui suposar un incompliment de la normativa sobre protecció de dades personals.

3.- En l'aute d'incoació d'expedient, s'argumenta que Andorra Telecom no ha complert, amb el deure de notificació o de comunicació d'una violació de la seguretat de les dades personals.

En el cas que ens ocupa, la investigació realitzada ens va permetre confirmar que l'eventual frau no s'havia produït per una bretxa en els nostres sistemes, sinó per una suplantació d'identitat utilitzant dades prèviament compromeses. Això va portar a una anàlisi interna per determinar si aquest fet constituïa una "violació de la seguretat de les dades personals" atribuïble a Andorra Telecom en el sentit estricte de l'article 4.13 de la LQPD.

Un cop avaluada la situació i seguint el principi de responsabilitat proactiva, vam determinar que la millor manera de gestionar l'incident era segons explicat al punt primer d'aquesta resposta.

Reconeixem el valor de la notificació com a mecanisme de supervisió i coordinació amb l'APDA i, per tant, en futurs casos, procedirem a realitzar la notificació formal en un termini de 72 hores, encara que es consideri que no hi ha hagut una bretxa tècnica en els nostres sistemes o en el cas de dubtar si hauríem de fer-la. Tanmateix, a la vista dels resultats, considerem que la notificació formal a l'APDA no hauria alterat de manera significativa la gestió operativa realitzada ni hauria suposat una millora en la seva resolució. L'actuació immediata, basada en una anàlisi detallada de la situació i la implementació de mesures correctores efectives, va permetre contenir el frau amb celeritat i minimitzar-ne l'impacte per als nostres clients.

Cinquè.- Per tots els motius ans exposats, aquesta part conclou que Andorra Telecom ha actuat amb la màxima diligència en la gestió d'aquest incident, tant en la resposta immediata com en la implementació de mesures de millora per prevenir situacions similars en el futur.

A la llum de les accions correctores implementades i del nostre compromís ferm amb la protecció de les dades personals, sol·licitem respectuosament que es vulgui procedir a l'arxivament sense ulteriors conseqüències jurídiques de l'expedient sancionador instat contra Andorra Telecom.

Volem reafirmar la nostra disposició total a col·laborar amb l'APDA i a seguir millorant els nostres protocols per garantir el més alt nivell de protecció de dades."

DESÈ.- En data del 27 de febrer del 2025, la cap de l'Agència Andorrana de Protecció de Dades dictà la resolució de l'expedient núm. 022-024_B3, en virtut de la qual s'imposava a ANDORRA TELECOM, SAU les infraccions descrites als articles 72.1.a., 72.2.e, 72.2.k i 72.2.l de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD), tipificades a l'article 74 de la mateixa llei, com a AMONESTACIÓ.

ONZÈ.- En data 27 de març del 2025, ANDORRA TELECOM SAU, presentà un recurs de reposició de la resolució de l'expedient 002-024.

II

FONAMENTS DE DRET

És competent per resoldre aquest procediment la cap de l'Agència Andorrana de Protecció de Dades, de conformitat amb el que disposa l'article 65.3.b i l'article 65.5 de la Llei 29/2021, del 28 d'octubre, qualificada de Protecció de Dades Personals (D'ara endavant, la «LQPD»), i desenvolupat a l'article 14 del

Reglament de l'Agència Andorrana de Protecció de Dades del 14 de setembre de 2022 (D'ara endavant, el «RQLPD»).

L'article 49 de la Llei 29/2021, de 28 d'octubre, qualificada de Protecció de Dades Personals així com l'article 4 del Reglament de l'Agència Andorrana de Protecció de Dades del 14 de setembre de 2022, disposen que, entre altres, és potestat de l'Agència andorrana de protecció de dades, vetllar, fomentar i vigilar el compliment de la legislació andorrana sobre protecció de dades.

III

FETS PROVATS

De les actuacions practicades en el present procediment i de la documentació de la que es disposa en l'expedient, queden acreditats els fets següents:

PRIMER.- ANDORRA TELECOM, SLU reconeix que va existir un frau de SIM SWAPPING i que els seus agents telefònics van ser enganyats.

SEGON.- ANDORRA TELECOM, SLU reconeix que va atendre 60 trucades dels defraudadors, de les quals 4 van implicar un frau econòmic al client. També reconeix que es van arribar a fer 7 migracions de SIM física a eSIM no sol·licitades pel titular del servei.

TERCER.- ANDORRA TELECOM, SLU, reconeix que les mesures definides per disseny i per defecte no van ser suficients.

QUART.- ANDORRA TELECOM, SLU va aplicar mesures de seguretat addicionals després de la producció del dany.

CINQUÈ.- ANDORRA TELECOM, SLU reconeix que no va dur a terme la notificació de violació de seguretat de les dades personals en els termes establerts en la LQPD.

IV

RESPOSTA AL RECURS DE REPOSICIÓ

ANDORRA TELECOM, SAU manifesta que no ha sigut l'entitat responsable de la comissió del dany que motiva la incoació de l'expedient. Explica que l'incident en qüestió es deu a un frau realitzat per un tercer mitjançant enginyeria social, un fet que afecta tant l'empresa com als clients implicats. En aquest sentit, ANDORRA TELECOM, SAU també és una víctima, atès que ha estat objecte d'un intent de frau extern.

L'APDA considera que si és cert que l'emissió de duplicats de la targeta eSIM o la migració de SIM físiques a eSIM no és suficient per a realitzar operacions bancàries en nom dels titulars per a completar l'estafa, però sí és necessari que una tercera persona "suplanti la identitat" del titular de les dades davant de l'entitat financera. Per aquesta mateixa raó, aquest és un procés on la diligència prestada per la operadora telefònica és fonamental per a evitar aquest tipus d'estafes i vulneracions de la LQPD. Diligència que necessàriament és tradueix en l'establiment de mesures tècniques i organitzatives adequades per a garantir que el tractament de dades sigui conforme la LQPD.

La emissió d'un duplicat de la targeta eSIM o la migració d'una SIM física a una eSIM suposa el tractament de les dades personals del seu titular, ja que es considerarà persona física identificable tota persona de la qual la seva identitat pugui determinar-se, directa o indirectament, en particular mitjançant un identificador (article 4.1 de la LQPD). Per tant, la targeta SIM física com virtual identifica un número de telèfon i aquest número alhora, identifica al seu titular.

Amb tot, **tant les dades que es tracten per emetre un duplicat d'eSIM, per migrar la targeta física a una virtual, així com la targeta SIM o eSIM que identifica de forma inequívoca i unívoca l'abonat a la xarxa, són dades de**

caràcter personal, sent el seu tractament subjecte a la normativa de protecció de dades.

En relació amb la responsabilitat d'ANDORRA TELECOM, SAU, s'ha d'indicar que, amb caràcter general, ANDORRA TELECOM, SAU tracta les dades dels seus clients sota la condició descrita a l'article 6.1.b de la LQPD, per considerar-se un tractament necessari per a la execució d'un contracte en el que l'interessat és part o per a l'aplicació a petició d'aquest de mesures precontractuals.

ANDORRA TELECOM, SAU com depositària de dades de caràcter personal a gran escala, per tant, habituada o dedicada específicament a la gestió de dades personals dels clients, ha de ser especialment diligent i curosa en el seu tractament. L'APDA considera que es tracta d'un error vencible, ja que amb l'aplicació de les mesures tècniques i organitzatives adequades, aquestes suplantacions d'identitat es podrien haver evitat.

Tenint en compte que, tal com s'explica a l'exposició de motius de la LQPD, aquesta llei s'acull al Reglament general de protecció de dades (d'ara endavant, l'«RGPD»), l'APDA té en compte els considerants establerts en aquesta normativa per la interpretació de les disposicions de la norma andorrana. En aquest context, cal recordar que el considerant 74 de l'RGPD estableix el següent: *"Ha de quedar establerta la responsabilitat del responsable del tractament per qualsevol tractament de dades personals realitzat per ell mateix o per compte seu. En particular, el responsable ha d'estar obligat a aplicar mesures oportunes i eficaces i ha de poder demostrar la conformitat de les activitats de tractament amb el present Reglament, inclosa l'eficàcia de les mesures. Aquestes mesures han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com el risc per als drets i les llibertats de les persones físiques".* De la mateixa manera, el considerant 79 de l'RGPD determina el següent: *"La protecció dels drets i llibertats dels interessats, així com la responsabilitat dels responsables i*

encarregats del tractament, també pel que fa a la supervisió per part de les autoritats de control i a les mesures adoptades per aquestes, requereixen una atribució clara de les responsabilitats en virtut del present Reglament, inclosos els casos en què un responsable determini les finalitats i els mitjans del tractament de manera conjunta amb altres responsables, o en què el tractament es dugui a terme per compte d'un responsable."

ANDORRA TELECOM, SAU, entén que no hi ha hagut un incompliment de la normativa de protecció de dades i sol·licita l'arxivament de l'expedient sancionador.

Tanmateix, l'APDA no pot procedir a l'arxivament, ja que ANDORRA TELECOM, SAU, no ha pogut demostrar que va obrar amb tota la diligència que li era exigible.

Amb tot, ens hem de remetre a l'article 5.3 de la LQPD (principi de responsabilitat proactiva), que transfereix al responsable de tractament la obligació no només de complir amb la normativa, sinó també la de poder demostrar aquest compliment.

El Dictamen 3/2010, del Grup de Treball de Protecció de Dades de l'article 29 (GT29) sobre el principi de responsabilitat afirma que l'essència de la responsabilitat proactiva és l'obligació del responsable del tractament d'aplicar mesures que, en circumstàncies normals, garanteixin que en el context de les operacions de tractament es compleixin les normes en matèria de protecció de dades i en tenir disponibles documents que demostrin als interessats i a les Autoritats de Control quines mesures s'han adoptat per aconseguir el compliment de les normes en matèria de protecció de dades.

L'article 5.3 es desenvolupa en l'article 27 de la LQPD que obliga el responsable a adoptar les mesures tècniques i organitzatives apropiades "per garantir i poder demostrar" que el tractament és conforme amb la LQPD. El precepte estableix:

"1. Tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i de gravetat diversa per als drets i les llibertats de les persones físiques, el responsable del tractament ha de garantir l'aplicació de les mesures tècniques i organitzatives adequades i ha de poder demostrar que el tractament és conforme a aquesta Llei i a les seves normes de desplegament. Aquestes mesures s'han de revisar i actualitzar quan sigui necessari.

2. Quan siguin proporcionades en relació amb les activitats de tractament, entre les mesures esmentades a l'apartat 1 s'hi ha d'incloure l'aplicació, per part del responsable del tractament, de les polítiques de protecció de dades oportunes.

3. El responsable del tractament pot determinar les mesures tècniques i organitzatives en un codi de conducta en matèria de protecció de dades personals, segons previstos a l'article 40. Un cop adoptat el codi de conducta pel responsable del tractament, o la seva modificació o ampliació, el codi es diposita prop de l'Agència Andorrana de Protecció de Dades."

L'article 28 de la LQPD, "*Protecció de dades des del disseny i per defecte*", estableix:

"1. Tenint en compte l'estat de la tècnica, el cost d'aplicació i la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i de gravetat diversa per als drets i les llibertats de les persones físiques, tant en el moment de determinar els mitjans de tractament com en el moment de procedir al tractament, el responsable ha d'implantar les mesures tècniques i organitzatives adequades per aplicar de manera efectiva els principis de protecció de dades i integrar les garanties necessàries en el tractament.

2. (...)"

Això suposa que ANDORRA TELECOM, SAU no hauria identificat i analitzat de forma adequada els riscos del protocol d'identificació del titular de la targeta per als drets i les llibertats de les persones físiques, ni previst ni aplicat des del disseny les mesures tècniques i organitzatives apropiades, per aplicar de forma efectiva els principis de protecció de dades, que exigeix l'article 28 de la LQPD.

Amb tot, **l'APDA considera que les al·legacions presentades no són suficients per eximir l'entitat de la seva responsabilitat** en virtut de l'article 35 de la LQPD, que estableix l'obligació d'aplicar mesures tècniques i organitzatives adequades per garantir un nivell de seguretat apropiat al risc.

En aquest sentit, és rellevant assenyalar que **les autoritats de protecció de dades que apliquen l'RGPD**, han abordat en repetides ocasions situacions similars relacionades amb atacs de SIM SWAPPING, **considerant que les operadores de telefonia tenen el deure d'implementar procediments de verificació robustos abans d'autoritzar el duplicat SIM o la migració de targetes SIM físiques a virtuals**, especialment quan aquests processos permeten l'accés a informació personal sensible o credencials bancàries.

Un exemple clar es troba en la resolució de l'Agència Espanyola de Protecció de Dades (d'ara endavant, l'«AEPD») núm. EXP202303020, en la qual es va imposar una sanció de **200.000 euros a VODAFONE ESPAÑA, S.A.U**. En aquest cas, l'AEPD, entre altres qüestions, va considerar que l'empresa, **a més de tenir la responsabilitat** d'actuar amb la màxima diligència, **no havia seguit el procediment establert per identificar correctament la persona que va sol·licitar el duplicat de la targeta SIM**. Si s'hagués aplicat adequadament, la sol·licitud hauria estat denegada. Aquesta manca de diligència va permetre un tractament il·lícit de dades personals.

Així mateix, en la resolució núm. EXP202105333, l'AEPD va reiterar aquest criteri en imposar una sanció de **70.000 euros a DIGI SPAIN TELECOM, S.L**. Entre altres qüestions, **l'AEPD va considerar DIGI responsable d'haver**

facilitat un duplicat de la targeta SIM a un tercer aliè al legítim titular de la línia, evidenciant **un incompliment del deure de protegir la informació dels clients**. Aquest incident demostra la manca de diligència deguda, ja que no es va seguir adequadament el protocol de verificació establert, permetent la superació dels mecanismes de seguretat per part de tercers. **L'AEPD destaca que la responsabilitat última en el tractament de dades recau en el responsable, qui ha d'assegurar les garanties necessàries segons el principi de responsabilitat proactiva**.

Finalment, en la resolució núm. EXP202213023, l'AEPD va sancionar amb **1.000.000 d'euros a ORANGE ESPAGNE, SAU**, per incompliment de l'article 25 de l'RGPD (equivalent a l'article 28 de la LQPD) **relatiu a la protecció de dades des del disseny i per defecte** i va ordenar-la, en un termini de sis mesos a notificar les mesures adoptades per garantir que la sol·licitud del duplicat es presentava pel titular del número de telèfon, sigues quin sigues el procediment utilitzat per la seva emissió.

Aquests **precedents posen de manifest** que existeix un estàndard clar sobre les expectatives en matèria de seguretat per prevenir fraus de SIM SWAPPING, i que **les operadores de telefonia han d'implementar mecanismes que minimitzin aquests riscos, com ara la verificació reforçada d'identitat**, notificacions proactives a l'usuari i controls addicionals per a processos crítics.

En el present cas, s'ha evidenciat que ANDORRA TELECOM,SAU no va adoptar mesures adequades per mitigar el risc conegut de suplantació, ja que, tot i que l'agent telefònic va seguir el protocol establert per a la migració de la targeta SIM a eSIM, aquest procediment presentava deficiències que van permetre a un tercer completar la sol·licitud de manera fraudulenta. Aquesta manca de garanties en el sistema de verificació va facilitar l'accés a dades personals i va derivar en un perjudici significatiu per a les persones afectades. En aquest sentit, ANDORRA TELECOM, SAU reconeix que va arribar a fer 7

migracions de SIM física a eSIM no sol·licitades pel titular quedant acreditat així, que l'eSIM va ser facilitada a un tercer no autoritzat.

ANDORRA TELECOM, SAU exposa, en el seu escrit d'al·legacions, que aquest incident no ha estat causat per una vulneració dels sistemes informàtics ni per cap actuació impròpia de l'Empresa, sinó per la utilització fraudulenta de dades prèviament compromeses per part de tercers desconeguts, els quals ja disposaven de les dades personals dels afectats.

Com ja s'ha anat dient de forma repetida en aquest escrit, **la manca de mesures de seguretat efectives per part d'ANDORRA TELECOM, SAU a l'hora d'identificar el titular de la SIM, són un element clau que van determinar els fraus posteriors, fet que implica una responsabilitat directa per part de l'empresa en la protecció de les dades personals dels afectats**.

ANDORRA TELECOM, SAU explica, en el seu escrit d'al·legacions, que ha actuat en tot moment amb la màxima diligència i ha sigut una víctima més d'uns fets que, presumptament, poden ésser considerats de frau o estafa. Així mateix, han garantit en tot moment els principis de protecció del tractament de les dades personals previstos, entre d'altres, a l'article 5 de la LQPD.

El principi d'exactitud imposa al responsable de tractament l'obligació de garantir que les dades personals es mantinguin correctes i actualitzades. La possibilitat que, mitjançant tècniques fraudulentes com el SIM SWAPPING, es puguin alterar o desactualitzar les dades evidencia una manca de mecanismes de control i verificació suficients, fet que no pot ser compensat simplement amb la invocació d'un comportament diligent.

Al mateix temps, el principi d'integritat i confidencialitat requereix que es protegeixin les dades contra accessos no autoritzats. L'explotació de vulnerabilitats que permeten el SIM SWAPPING reflecteix, de manera directa, una **deficiència en les mesures tècniques i organitzatives destinades a salvaguardar la seguretat de la informació, responsabilitat que recau**

exclusivament en l'empresa. **ANDORRA TELECOM, SAU va facilitar la migració de la SIM física a la virtual a un tercer diferent al legítim titular de la línia, després de la superació per terceres persones del protocol de seguretat existent, el que evidencia un incompliment del deure de protegir la informació dels clients**.

Per tant, encara que es pugui afirmar que els fets podrien tenir una connotació fraudulenta des d'un punt de vista extern, aquesta realitat no eximeix a ANDORRA TLECOM, SAU de la seva obligació de complir amb els principis fonamentals de protecció de dades. **La manca de mesures eficaces per garantir l'exactitud, la integritat i la confidencialitat de la informació implica una vulneració de les obligacions legals**, independentment de l'existència d'un suposat frau extern.

El responsable de tractament també exposa que l'APDA ha decidit incoar un expedient sancionador contra ANDORRA TELECOM, SAU en base, entre d'altres, a unes notes de premsa que fan referència a uns fets actualment judicialitzats, dels quals es desconeix, pel moment processal en el què es troben, la seva autoria, la forma de realització de l'eventual fet delictiu, els mecanismes que els presumptes infractors van usar per a cometre dits fets o les conseqüències generades, entre d'altres. Expliquen que aquestes informacions poden contenir errors o ser esbiaixades, tant pel fet que les notes de premsa contenen informació no exacta, com pel fet que els fets es troben actualment en fase d'instrucció i, per tant, d'investigació per part de les autoritats competents. Continuen exposant que van posar a disposició de l'APDA tota la informació que disposen sobre l'assumpte. Tanmateix, l'APDA no va procedir a la seva anàlisis, i va decidir incoar l'expedient administratiu comportant una situació d'indefensió a ANDORRA TELECOM, SAU.

Resulta insostenible la tesi d'indefensió d'ANDORRA TELECOM, SAU, ja que l'inici de l'expedient sancionador es va fonamentar en indicis objectius recollits tant en notificacions d'altres entitats sobre violacions de seguretat com en

publicacions de mitjans de comunicació, les quals, tot i la seva possible imprecisió, eren suficients per sospitar d'incompliments de la LQPD i justificar l'actuació d'ofici de l'APDA, la qual té la competència de valorar la correcta aplicació de la normativa en el tractament de dades sense haver de pretendre investigar els delictes externs. En aquest context, i d'acord amb l'article 63 de la LQPD, l'APDA disposa de poders d'investigació que pot exercir per iniciativa pròpia quan el responsable o encarregat del tractament incompleixi les obligacions establertes per la Llei. Atès que l'APDA posseeix aquests poders i en virtut dels indicis d'incompliment detectats, **va decidir actuar d'ofici, considerant la gravetat de la situació i amb l'objectiu de salvaguardar els drets a la protecció de dades de tots els abonats a ANDORRA TELECOM, SAU**. Cal tenir en compte que, en aquest cas, **es tracta de l'única operadora telefònica present a tot el país, la qual concentra la totalitat dels números de telèfon i per tant, el nivell d'exigència pel que fa el compliment de la normativa de protecció de dades ha de ser estricta, i més, quan els afectats no tenen alternatives per escollir altres companyies de telefonia**.

Cal recordar que l'APDA, en el seu requeriment d'informació ja va sol·licitar a ANDORRA TELECOM, SAU, que aportessin "tota altra informació escaient". En aquest context, recordem que el Decret 368/2022, del 14-9-2022, d'aprovació del Reglament de l'Agència Andorrana de Protecció de Dades, estableix que una vegada els inspectors han practicat la investigació, han de presentar una proposta a la cap de l'APDA, a qui correspon resoldre si s'ha d'incoar l'expedient sancionador. En aquest sentit, ANDORRA TELECOM, SAU ja era coneixedora del procediment, i per tant, és en el moment del requeriment d'informació que hauria d'haver aportat tota la informació necessària per resoldre l'assumpte.

ANDORRA TELECOM, SAU reitera que no es va produir una "Violació de la seguretat de les dades personals", en els termes establerts a la LQPD. Expliquen que no va haver-hi una violació de la seguretat ni un accés indegut als sistemes informàtics que permetessin l'accés a dades personals d'usuaris

d'ANDORRA TELECOM, SAU, sinó que aquestes dades personals ja eren conegudes prèviament per part dels infractors, els quals, utilitzant aquestes dades, van poder accedir a una targeta eSIM. Per tant, insisteixen que no existeix en aquest cas una "pèrdua, alteració o divulgació de dades personals transmeses, conservades o tractades d'una altra manera", sinó que les dades personals que ja disposava l'eventual infractor, els van permetre cometre un fet eventualment delictiu, produint un engany tant a ANDORRA TELECOM, SAU com a diverses entitats bancàries del país.

Com ja s'ha dit de forma reiterada en aquest escrit, i **des del prisma de la normativa de protecció de dades**, **la responsabilitat de la companyia no recau en els delictes posteriors de frau bancari o altres activitats il·lícites, sinó en la manca de mesures tècniques i organitzatives des del disseny per garantir la correcta identificació del titular de la eSIM**. **En absència d'un sistema de verificació d'identitat robust, es va facilitar la realització d'actuacions fraudulentes, la qual omissió configura una vulneració dels principis de protecció, integritat i confidencialitat de les dades personals**.

L'APDA reafirma que en el present cas es va configurar una violació de la seguretat de les dades personals, tal com es defineix com qualsevol incident que ocasiona, de manera accidental o il·lícita i en tot cas no autoritzada, la pèrdua, alteració o divulgació de dades personals, o la comunicació o accés no autoritzat a aquestes dades. Així, en el cas de SIM SWAPPING, **la violació es va produir en el moment en què l'agent telefònic va aplicar uns protocols d'identificació del titular que, com es va demostrar posteriorment, no eren suficientment segurs ni estaven dissenyats de manera que garantissin els principis de confidencialitat, integritat i seguretat previstos per la LQPD**. En aquest sentit, l'article 35 de la LQPD exigeix l'adopció de mesures tècniques i organitzatives adequades per protegir les dades personals, requisit que, en aquest cas, va quedar desatès. A més, cal destacar que el formulari de notificacions de violacions de seguretat de

dades, posat a disposició per l'APDA, contempla explícitament situacions en què es podria haver assenyalat una fallada del protocol, com ara "dades personals mostrades a l'individu incorrecte", incidències en la confidencialitat o integritat, o incidents accidentals, fet que reforça la interpretació que els esdeveniments que han tingut lloc van constituir una clara violació de la seguretat de les dades. En aquesta mateixa línia, el fet que ANDORRA TELECOM, SAU hagi modificat el protocol per la identificació dels titulars de les targetes SIM, afegint noves mesures tècniques i organitzatives després de l'incident de SIM SWAPPING, evidencia que les mesures inicials no eren les adequades, ja que van provocar accessos indeguts, és a dir una violació de seguretat de les dades personals. També, cal fer avinent que les violacions de seguretat no només es produeixen per accessos indeguts derivats d'atacs als sistemes informàtics, sinó també qualsevol situació que permeti un accés no autoritzat a dades personals.

En aquest sentit, cal subratllar que, que **aquesta violació de la seguretat de les dades personals derivada de l'aplicació d'un protocol d'identificació inadequat, ANDORRA TELECOM SAU, no va complir amb la seva obligació de notificació a l'APDA**. L'article 36 de la LQPD exposa que, en cas de violació de la seguretat de les dades personals, l'APDA ha de ser informada dins del termini màxim de 72 hores des de la seva detecció, excepte en situacions en què la notificació no comporti riscos per als drets i llibertats dels afectats. I com s'ha constatat, **l'aplicació d'un protocol d'identificació feble, va comportar que els clients quedessin desprotegits de forma que amb l'eSIM i altres dades personals obtingudes il·lícitament fossin víctimes de fraus posteriors**.

ANDORRA TELECOM SAU al·lega que no va complir amb el deure de notificació d'una violació de la seguretat de les dades personals, argumentant que l'eventual frau no va ser causat per una bretxa als seus sistemes, sinó per una suplantació d'identitat amb dades prèviament compromeses. L'empresa indica que, en analitzar la situació, va valorar que no s'atribuïa la violació de

seguretat als seus sistemes segons l'article 4.13 de la LQPD. Tot seguit, reconeix el valor de la notificació com a mecanisme de supervisió i coordinació amb l'APDA, i es compromet a notificar en futurs casos dins del termini de 72 hores, tot i que consideren que, en aquest cas, la notificació formal no hauria alterat significativament la gestió operativa ni millorat la resolució dels fets.

En aquest context, **l'APDA recorda que l'obtenció fraudulenta de la targeta eSIM genera greus riscos per als afectats**. **El control de l'eSIM permet als tercers accedir, sota determinades circumstàncies, als contactes i a aplicacions o serveis que utilitzen l'enviament d'un SMS amb un codi com a procediment de recuperació de contrasenya. Aquesta vulnerabilitat facilita la suplantació d'identitat dels titulars legítims, permetent als infractors accedir i controlar comptes de correu electrònic, comptes bancàries, aplicacions com WhatsApp o xarxes socials com Facebook i Twitter, entre altres**. Un cop modificades les credencials d'accés, les víctimes perden el control de les seves comptes i serveis, exposant-se a fraus i accions malicioses. Aquesta situació constitueix una amenaça significativa per als drets i llibertats dels afectats i evidencia la importància d'aplicar protocols de seguretat robustos per prevenir aquests riscos.

L'APDA recorda que la normativa en matèria de protecció de dades exigeix, de manera independent de la causa subjacent del frau, el compliment estricte del deure de notificació de qualsevol violació de la seguretat de les dades personals que impliqui un risc elevat en els drets i les llibertats de les persones. L'argument que la notificació no hauria afectat l'operativitat no exonera l'empresa del compliment de les seves obligacions. Així doncs, l'APDA manté que la manca de notificació en el termini establert configura un incompliment de la LQPD.

ANDORRA TELECOM SAU al·lega que, durant el transcurs del frau, els agents del CAT van atendre un total de 60 trucades dels defraudadors, de les quals consten 4 que van implicar un frau econòmic directe als clients. Segons

la companyia, les mesures proactives adoptades per disseny i per defecte, tot i no haver estat suficients per evitar tots els intents fraudulents, van contribuir a mitigar un impacte que, en absència d'aquestes, hauria estat significativament superior. Així mateix, ANDORRA TELECOM, SAU recorda que la resta dels casos de frau publicats als mitjans de comunicació s'haurien materialitzat sense la seva intervenció. A més, la companyia sosté que el fet que un tercer hagi dut a terme un acte eventualment delictiu, induint a error els seus agents telefònics, no implica en cap cas un incompliment dels principis de tractament de dades personals establerts a l'article 5 de la LQPD, sinó que aquests fets són conseqüència d'un acte delictiu extern a l'empresa. Finalment, ANDORRA TELECOM, SAU afirma que, tant abans com després de la producció dels fets, es van adoptar les mesures de protecció pertinents per garantir que no es materialitzés un alt risc per als drets i les llibertats de les persones interessades, actuant amb la màxima diligència possible.

L'APDA considera que la mera imputació d'un fet eventualment delictiu extern no exonera a ANDORRA TELECOM SAU de la seva responsabilitat com a responsable de tractament, d'acord amb l'article 27 de la LQPD, que exigeix l'adopció de mesures tècniques i organitzatives adequades per garantir la seguretat de les dades personals. **La concentració de la totalitat dels números de telèfon en una única operadora comporta, per tant, un alt nivell d'exigència en la implementació de protocols d'identificació robustos**. Així, el fet que s'hagi constatat que els protocols aplicats no eren suficientment segurs, facilitant fraus a través de SIM SWAPPING, evidencia una vulnerabilitat que contravé els principis establerts en l'article 5 de la LQPD, independentment de la naturalesa aïllada dels fets.

Pel que fa **les mesures existents abans de produir-se el dany** explicades per ANDORRA TELECOM, SAU en el seu escrit d'al·legacions, l'APDA considera que **aquestes eren insuficients en el context on un agent va transmetre l'eSIM a una persona que suplantava la identitat del titular**. En concret, la sol·licitud exclusiva de dades com el nom complet, cognoms,

número de telèfon i document identificatiu, i, en casos d'anomalia, informació addicional (adreça, data de naixement i últims quatre dígits del compte bancari), no va ser suficient per impedir la suplantació d'identitat. **Això evidencia que els protocols d'identificació adoptats no complien amb el rigor exigit per l'article 27 de la LQPD, que demanda mesures tècniques i organitzatives adequades en funció del risc, i això és especialment important en un entorn de concentració de dades tan elevat com el que gestiona ANDORRA TELECOM, SAU.**

Pel que fa les mesures adoptades per ANDORRA TELECOM, SAU després de l'incident, mostren una resposta correctiva i un esforç per reforçar la seguretat en la gestió dels procediments de migració de SIM a eSIM. Tanmateix, el fet que fos necessari suspendre l'operativa a causa de la persistència d'intents fraudulents, així com la imposició de la migració presencial i altres mesures posteriors, **evidencia que els controls inicials eren insuficients per prevenir els fets vinculats al SIM SWAPPING**. Aquestes **mesures**, encara que positives en el seu caràcter correctiu i de millora contínua (incloent-hi la implementació del 2FA, la revisió dels procediments d'autenticació, la formació específica dels agents i l'adaptació dels protocols interns), **resulten essencialment reactives**. En conseqüència, s'ha de valorar que la responsabilitat de garantir la seguretat de les dades personals, tal com estableix la LQPD, **requereix mesures de seguretat proactives i suficients que minimitzin, des de l'origen i des del seu disseny, qualsevol risc de frau, cosa que no es va aconseguir**.

Com a fonament del recurs de reposició, ANDORRA TELECOM, SLU reitera en gran part les al·legacions ja exposades anteriorment, tot i que incorpora algun argument nou que, tanmateix, no resulta suficient per justificar una modificació de la resolució impugnada.

En relació amb els arguments exposats per ANDORRA TELECOM, SLU en el seu recurs de reposició, aquesta Autoritat vol manifestar que no es pot compartir la seva interpretació ni la conclusió que se'n deriva. En primer lloc,

cal deixar constància que el **procediment establert pel responsable de tractament per a la migració de la targeta SIM a E-SIM presentava deficiències en matèria de seguretat i confidencialitat del tractament**. El protocol establert per a la migració de la SIM a E-SIM, tal com ha estat exposat en l'escrit d'al·legacions, **es limitava a verificar dades bàsiques del client com el nom complet, cognoms, número de telèfon i número de document identificatiu** (DNI, passaport o número de cens). En casos considerats sospitosos o en què es detectaven anomalies, s'hi afegien altres dades com l'adreça, la data de naixement i els darrers quatre dígits del compte bancari associat. Tanmateix, totes aquestes dades són fàcilment accessibles per terceres persones, ja sigui per mitjans legítims (per exemple, dades compartides a través de xarxes socials o per gestions administratives) o per mitjans fraudulents (enginyeria social, *phishing* o compra en mercats il·lícits de dades). **No es tracta de dades que puguin garantir de manera robusta la identitat del sol·licitant, especialment en un tràmit que, com és el cas, implica un risc elevat de suplantació amb accés a serveis personals i informació confidencial. L'ús d'aquestes dades com a únic mecanisme de verificació era clarament insuficient.** És per això que es considera que el protocol aplicat era deficient, independentment que fos seguit pels agents telefònics de manera formal, ja que la seva concepció no incorporava mesures de seguretat adequades al nivell de risc del tractament, des del disseny i per defecte. Aquest fet representa una vulnerabilitat clara davant possibles intents de suplantació d'identitat, com es va acabar materialitzant en aquest cas, amb conseqüències negatives per a la persona afectada.

Pel que fa a la suposada manca d'anàlisi de la documentació aportada per ANDORRA TELECOM, SAU, l'APDA desmenteix categòricament aquesta afirmació. Aquesta Autoritat va requerir informació a l'entitat en el marc del procediment i va analitzar detalladament tota la documentació rebuda. És precisament a partir d'aquesta informació que es va poder constatar que el procediment aplicat no era adequat ni proporcionat als riscos associats.

L'anàlisi es va fer tenint en compte el contingut aportat per l'entitat i amb ple respecte als principis del procediment administratiu, de manera que no es pot acceptar que la resolució es basi en fets "no provats" ni "aliens", com es pretén argumentar. A més, **la pròpia entitat, en les seves al·legacions, reconeix els fets essencials del cas, per la qual cosa no es pot parlar de manca de fonament ni d'inexistència de proves.**

Finalment, **el fet que l'entitat es presenti com a víctima d'una possible acció delictiva no altera el seu deure com a responsable del tractament de garantir la seguretat de les dades personals que tracta**. En aquest àmbit, la responsabilitat no es dilueix per l'existència d'un atac extern si no s'han adoptat mesures adequades per prevenir-lo. Per tant, queda acreditat que ANDORRA TELECOM, SAU no va actuar amb la diligència exigible i que la resolució impugnada es fonamenta en fets provats, en l'anàlisi de la informació facilitada per l'entitat i en la normativa aplicable.

Respecte a l'argument segons el qual una eventual vulneració de dades com a resultat d'un frau no hauria de comportar sanció per a una entitat que també en resulta víctima, cal recordar que la normativa de protecció de dades exigeix que les entitats responsables prenguin mesures adequades per prevenir riscos previsibles. **El fet que la suplantació sigui comesa per un tercer no elimina la responsabilitat d'ANDORRA TELECOM, SAU si el protocol aplicat era insuficient per detectar i evitar aquest tipus de situacions. La sanció no deriva del frau en si mateix, sinó de no haver implementat mesures de seguretat adequades per evitar-lo**.

Pel que fa a la referència que fa ANDORRA TELECOM, SAU a la STS 543/2022, de 15 de febrer, en què es defineix l'obligació de seguretat com una obligació de mitjans i no de resultat, aquesta Autoritat coincideix plenament amb aquest criteri. Ara bé, cal destacar que precisament aquesta doctrina exigeix que els mitjans adoptats siguin adequats, suficients i aplicats amb diligència, en funció del risc del tractament i de l'estat de la tecnologia. **Basar la verificació únicament en dades fàcilment accessibles per tercers (com**

el nom, número del document d'identitat i telèfon) no s'ajusta a cap estàndard raonable de seguretat, especialment tenint en compte que es tracta d'un tràmit sensible i exposat a intents de suplantació d'identitat. La manca d'una capa addicional de verificació (com una doble autenticació) demostra que les mesures aplicades no eren suficients ni conformes a la diligència exigible, fins i tot sota el criteri de "mitjans raonables" que estableix la jurisprudència citada.

Per tant, **no es sanciona l'entitat pel fet que s'hagi produït un frau, sinó per no haver implementat un protocol adequat per evitar-lo, dins dels mitjans que eren raonablement exigibles segons la normativa i la tecnologia disponible**.

Respecte a la manifestació que l'expedient sancionador s'ha iniciat únicament a partir de notes de premsa, cal aclarir que aquesta afirmació no és correcta. Tal com consta en el procediment, l'APDA va requerir formalment a ANDORRA TELECOM,SAU la informació necessària per valorar els fets, i la incoació de l'expedient es va fonamentar en la informació recollida i aportada per la pròpia entitat, no pas en fonts periodístiques que sí bé van ser indiciàries de possibles incompliments de la normativa andorrana de protecció de dades. Així, les notes de premsa només van actuar com a indicis inicials, que van motivar l'inici d'actuacions preliminars, com és habitual en aquests casos.

Pel que fa a la suposada manca d'anàlisi de la documentació posada a disposició de l'APDA, cal recordar que el procediment administratiu exigeix que les parts aportin efectivament la documentació requerida dins del termini i forma establerts. Manifestar que aquesta es trobava "a disposició" a les oficines de l'entitat no eximeix del deure de presentar-la degudament, especialment quan l'autoritat havia requerit la seva aportació per escrit. En cap cas l'APDA ha rebut accés efectiu a la totalitat de la documentació que ara es diu haver posat a disposició, i per tant no es pot acceptar que s'hagi incomplert el deure d'anàlisi quan la informació no ha estat degudament presentada.

Finalment, quant a l'afirmació que la resolució es basa en informacions errònies o esbiaixades, aquesta no es fonamenta en fonts externes no contrastades, sinó en dades i reconeixements expressos per part de la pròpia entitat en les seves al·legacions i documentació aportada. És, per tant, una resolució fonamentada en fets provats i en la manca de mesures adequades de seguretat, tal com exigeix la normativa aplicable.

Pel que fa a l'afirmació que l'APDA no ha analitzat el protocol ni escoltat les gravacions de veu, cal deixar constància que d'acord amb la informació aportada per l'entitat, aquesta Autoritat ha pogut constatar que el procediment establert per a la migració de targetes SIM a E-SIM presentava deficiències importants, ja que es basava en la simple verificació de dades bàsiques, sense cap mecanisme d'autenticació reforçada, malgrat el risc evident de suplantació d'identitat associat a aquest tràmit.

Pel que fa a les gravacions, s'ha de remarcar **que l'objecte de la valoració no era la conducta de l'agent, sinó el disseny del protocol. Encara que aquest s'hagués aplicat correctament, les mesures establertes no eren suficients per garantir la seguretat del tractament, i per tant, la responsabilitat recau en el disseny inadequat del procediment.**

Quant a l'al·legació referida a la desproporcionalitat de la resolució, fonamentada en el reduït impacte econòmic del frau i el nombre limitat d'afectats, cal recordar que la normativa andorrana en matèria de protecció de dades no condiciona la comissió d'una infracció al volum del perjudici causat ni al nombre d'afectats, sinó a la gravetat del risc generat per l'incompliment dels principis bàsics relatius a la protecció de dades personals.

En aquest sentit, el fet que el dany econòmic derivat hagi estat limitat no resta importància al fet que el protocol aplicat era inadequat per protegir les dades personals dels usuaris, ni eximeix l'entitat de la seva responsabilitat com a responsable del tractament. **La protecció de dades personals no es valora exclusivament en funció de conseqüències quantificables en euros, sinó**

també en funció del risc generat per a drets fonamentals, com són el dret a la protecció de dades personals davant la suplantació d'identitat.

Pel que fa al suposat "dany reputacional" derivat de la resolució, s'ha de recordar que el règim sancionador aplicable a les entitats públiques, com és el cas d'ANDORRA TELECOM, SAU, preveu l'amonestació com a mesura en comptes d'una sanció econòmica. En conseqüència, **no pot considerar-se desproporcionada una resolució que s'ha limitat a aplicar el règim previst legalment, en proporció a la infracció comesa, i que no comporta, en si mateixa, cap conseqüència econòmica directa per a l'entitat. Per tant, l'argument basat en un suposat perjudici reputacional no pot ser acceptat com a fonament per anul·lar ni modificar la resolució dictada.**

La LQPD estableix clarament que la seguretat del tractament s'ha d'avaluar tenint en compte els riscos que pot comportar, no únicament els danys efectivament produïts. **La sanció no es fonamenta en un escenari hipotètic, sinó en la constatació d'un protocol insuficient que va permetre una vulneració de la seguretat efectiva, encara que amb impacte limitat segons explica el mateix responsable de tractament**. L'existència d'un intent de frau reeixit, encara que parcialment contingut, confirma la debilitat del sistema i justifica l'actuació d'aquesta Autoritat.

En conseqüència, procedeix desestimar el recurs de reposició interposat i mantenir íntegrament els termes de la resolució dictada.

V

OBLIGACIONS INCOMPLERTES

S'imputa a ANDORRA TELECOM SAU, la comissió de les infraccions següents:

- **Infracció considerada molt greu** :
  - **Article 72.1.a) El tractament de dades personals que vulneri l'article 5.**

En concret, s'imputa **l'incompliment per part d'ANDORRA TELECOM SAU, del principi d'exactitud, el principi d'integritat i confidencialitat i el principi de responsabilitat proactiva**.

Vist que el responsable de tractament no va obtenir les dades per part de les persones interessades (sinó de tercers no autoritzats), **no va respectar el principi d'exactitud**. Tot i disposar d'un protocol per a la identificació del titular de la targeta SIM, **el responsable de tractament no ha pogut demostrar que aquest permetia garantir que les dades facilitades corresponien amb la identitat real dels usuaris**.

El responsable de tractament **també vulnera el principi d'integritat i confidencialitat**, ja que, amb els protocols dels que disposava abans de l'incident, **facilitava a tercers no autoritzats a accedir a les dades i gestionar serveis en nom d'altres persones posant en risc la protecció de la informació**. Així, ANDORRA TELECOM, SAU no va garantir mesures de seguretat adequades per evitar accessos fraudulents i possibles danys als afectats.

Pel que fa el **principi de responsabilitat proactiva**, ANDORRA TELECOM SAU, **no demostra que va anticipar i prevenir possibles vulneracions de seguretat per protegir els drets dels afectats**.

- **Infraccions considerades greus:**
  - **Article 72.2.e) Incomplir els deures de notificació o de comunicació d'una violació de la seguretat de les dades personals (incompliment de l'article 36).**

Es conclou que ANDORRA TELECOM SAU **no va notificar la bretxa de seguretat de les dades personals, en concret, la fallada del protocol aplicat per a la identificació dels titulars de la targeta SIM, a l'APDA en els termes establerts en la LQPD**.

  - **Article 72.2.k) La falta d'adopció de les mesures tècniques i organitzatives apropiades per garantir que, per defecte, només es tracten les dades personals necessàries per a**

cadascuna de les finalitats específiques del tractament o que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament (incompliment de l'article 28).

L'APDA conclou que el protocol d'identificació dels titulars de les targetes SIM establert per ANDORRA TELECOM SAU no va ser dissenyat des d'un primer moment amb les precaucions necessàries per atenuar els riscos de suplantació d'identitat.

- **Article 72.2.l) L'incompliment, com a conseqüència de la falta de la diligència deguda, de les mesures tècniques i organitzatives que s'hagin implantat (incompliment dels articles 27 i 35).**

Es conclou que va existir un incompliment dels articles 27 i 35, atès que **protocol per a la identificació dels titulars de la targeta SIM no era l'adequat, fet que demostra la falta de diligència deguda per part del responsable de tractament**, per adequar les mesures tècniques i organitzatives al nivell del risc per als interessats.

Amb tot, és rellevant assenyalar que **ANDORRA TELECOM, SAU comptava amb un protocol d'identificació dels titulars de targeta SIM que presentava mancances significatives. Aquestes deficiències van permetre l'engany dels agents telefònics i, per tant, van facilitar la migració de targetes a persones que no eren els legítims titulars. Així, si algú es fes passar pel titular durant una trucada, les mesures de verificació resultaven insuficients per confirmar la seva veritable identitat, demostrant que el protocol no complia amb la seva funció principal.**

VI

De conformitat amb tot l'anterior i sobre la base de l'article 128 de la Llei 14/2023, del 3 de juliol, de text consolidat del Codi de l'Administració, resultant que s'ha acreditat l'existència d'una vulneració de la normativa andorrana de protecció de dades atribuïble a la conducta d'ANDORRA TELECOM, SAU, es procedeix a resoldre el present expedient administratiu.

Vist l'article 74 de la LQPD que determina el següent:

> *1. El règim establert en aquest article és d'aplicació als tractaments dels quals siguin responsables o encarregats:*
>
> > *a) L'Administració general i els òrgans que estan sota la seva direcció.*
> >
> > *b) Els comuns i els òrgans que en depenen.*
> >
> > *c) El Consell General, el Consell Superior de la Justícia, el Raonador del Ciutadà, i el Tribunal de Comptes.*
> >
> > *d) Els òrgans jurisdiccionals.*
> >
> > *e) Els organismes públics i les entitats parapúbliques vinculades o dependents de les Administracions públiques.*
> >
> > *f) Les corporacions de dret públic quan les finalitats del tractament es relacionin amb l'exercici de potestats de dret públic.*
>
> *2. Per excepció al que disposa l'article anterior, quan els responsables o encarregats enumerats a l'apartat 1 cometin alguna de les infraccions previstes en aquesta Llei, l'Agència Andorrana de Protecció de Dades ha de dictar resolució sancionant-los amb amonestació. La resolució ha d'establir també les mesures que procedeixi adoptar perquè cesi la conducta o es corregeixin els efectes de la infracció que s'hagués comès.*

La resolució s'ha de notificar al responsable o encarregat del tractament, a l'òrgan del que depengui jeràrquicament i als afectats que tinguin la condició de persones interessades, si s'escau.

3. Sense perjudici del que estableix l'apartat anterior, l'Agència Andorrana de Protecció de Dades també ha de proposar la iniciació d'actuacions disciplinàries quan existeixin indicis suficients al respecte. En aquest cas, el procediment i les sancions a aplicar són les establertes a la legislació sobre règim disciplinari o sancionador que resulti d'aplicació.

Tanmateix, quan les infraccions siguin imputables a autoritats i directius, i s'acrediti l'existència d'informes tècnics o recomanacions per al tractament que no haguessin estat degudament atesos, a la resolució en la que s'imposi la sanció s'ha d'incloure una amonestació amb denominació del càrrec responsable i s'ha d'ordenar la publicació al Butlletí Oficial del Principat d'Andorra.

4. Les resolucions que recaiguin en relació amb les mesures i actuacions referides als apartats anteriors han de ser comunicades a l'Agència Andorrana de Protecció de Dades.

5. L'Agència Andorrana de Protecció de Dades ha de publicar a la seva pàgina web, amb la deguda separació, les resolucions relatives a les entitats enumerades a l'apartat 1, amb expressa indicació de la identitat del responsable o encarregat del tractament que hagués comés la infracció.

Vista la consideració d'ANDORRA TELECOM, SAU com a societat pública,

Vistos els preceptes citats i altres de general aplicació,

La cap de l'Agència Andorrana de Protecció de Dades, fent expressa aplicació del preceptuat pels articles 49 i 50 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals;

RESOL

PRIMER.- DESESTIMAR el recurs de reposició interposat per ANDORRA TELECOM, SAU contra la resolució de l'Agència Andorrana de Protecció de Dades dictada amb data 27 de febrer del 2025, en l'expedient 002-024_B i mantenir així, la sanció d'**AMONESTACIÓ** imposada en base del que disposa els articles 67.b) i 74 de la LQPD per les infraccions descrites als articles 72.1.a., 72.2.e, 72.2.k i 72.2.l. de la LQPD així com, les mesures correctores dictades: **ORDENAR** a ANDORRA TELECOM, SAU, que en compliment a l'article 67.d) de la LQPD, faci arribar a l'APDA el nou protocol per la identificació dels titulars de les targetes SIM en les sol·licituds de duplicats o migracions de targetes físiques a virtuals, en termini de 15 dies hàbils de l'emissió d'aquesta resolució.

SEGON.- NOTIFICAR la present resolució a ANDORRA TELECOM, SAU.

TERCER.- RECOMANAR a ANDORRA TELECOM, SAU, que inclogui la simulació dins dels seus processos relatius a la correcta aplicació de les mesures de seguretat.

QUART.- NOTIFICAR la present resolució a ANDORRA TELECOM,SAU amb seu social: C/ Mossen Lluis Pujol, 8 – 14, Santa Coloma, AD500 Andorra La Vella.

CINQUÈ.- PUBLICAR aquesta resolució a la plana web de l'Agència Andorrana de Protecció de Dades, d'acord amb l'article 74.5 LQPD.

De conformitat al que es disposa a l'apartat 4 de l'article 129 de la Llei 14/2023, del 3 de juliol, de text consolidat del Codi de l'Administració, la resolució del recurs posa fi a la via administrativa.

Contra aquesta resolució, que posa fi a la via administrativa, es pot interposar recurs davant la jurisdicció administrativa, en la forma i els terminis establerts per la Llei que regula el procediment davant d'aquesta jurisdicció.

I, com a prova de conformitat, signo la present resolució, al lloc i data esmentada en l'encapçalament.

Signat digitalment per:
RESHMA HARISH PUNJABI
(SIGNATURA)
Cap de l'Agència Andorrana de Protecció de Dades

Agència Andorrana de Protecció de dades

DATA: 08/04/2025
REGISTRE DE SORTIDA DE DOCUMENTS
Núm. SO – 23498