MEMÒRIA JUSTIFICATIVA, ECONÒMICA I DE PERSPECTIVA DE GÈNERE DEL PROJECTE DE LLEI DE MESURES PER A LA SEGURETAT DE LES XARXES I DELS SISTEMES D'INFORMACIÓ

I. Consideracions generals prèvies

És crucial per al nostre país aprofitar tots els avantatges de l'era digital per a potenciar el nostre creixement econòmic i reforçar la nostra capacitat d'innovació, dins uns límits segurs i ètics.

L'enclavament geopolític del Principat d'Andorra, la nostra consciència situacional, la creixent dependència que la nostra economia té de les xarxes i dels sistemes d'informació nacionals i transfronterers, les possibles sinergies en la prevenció d'amenaces i en els desafiaments que suposaran els ciberincidents, i l'anàlisi que s'ha realitzat en relació a les normatives necessàries per a regular la correcta transformació digital que s'està projectant per al nostre país, comporten la necessitat d'aproximar les nostres capacitats en matèria de ciberseguretat a les que la Unió Europea exigeix als seus estats membres mitjançant la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol del 2016, relativa a las mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i dels sistemes de informació en la Unió. El projecte de Llei que es presenta es basa en l'esmentada directiva, i l'adapta conforme a les particularitats del Principat d'Andorra i a l'experiència que la mateixa Unió Europea ha compilat en relació a la necessitat de reduir la càrrega normativa per als organismes competents i els costos per a les entitats públiques i privades a les que aplica aquesta normativa, prenent en consideració allò que estableix la Proposta de la Comissió Europea COM (2020) 823 final, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat, la qual proposa la derogació de la referida Directiva (UE) 2016/1148.

Per les mateixes raons esmentades a l'inici del paràgraf anterior, ens és igualment necessari dedicar encara més atenció a les entitats crítiques, enteses com aquelles que, a més de proveir un servei essencial per al Principat d'Andorra, tenen la peculiaritat d'utilitzar una infraestructura que no es pot redundar o reemplaçar per una altra en cas de mal funcionament. El bon funcionament del nostre país requereix exigir a aquestes entitats dues coses: un nivell de protecció mínim per a les denominades infraestructures

crítiques, i que es dotin d'una capacitat de recuperació enfront d'incidents en aquest tipus d'infraestructures, molt major que l'exigible a les entitats essencials, que sí que compten amb solucions alternatives per a evitar l'alteració del servei essencial en tots els possibles casos en què un incident afecti una única infraestructura. És per tot això que, addicionalment a l'esmentat en el paràgraf anterior, el projecte de Llei que es presenta adapta a les particularitats del Principat d'Andorra la Directiva (UE) 2008/114 del Parlament Europeu i del Consell, de 8 de desembre de 2008, sobre identificació i designació d'infraestructures crítiques europees i avaluació de la necessitat de millorar-ne la seva protecció, i s'adequa igualment a les lliçons apreses per la Unió Europea en relació a la necessitat d'ampliar el focus en la protecció d'aquestes infraestructures crítiques, amb l'objectiu d'aconseguir la major i més ràpida recuperació de l'entitat que gestiona la infraestructura crítica si les mesures de protecció fallen, lliçons les quals estan recopilades en la Proposta de la Comissió Europea COM(2020) 829 final, relativa a la resiliència de les entitats crítiques.

Mitjançant el projecte de Llei que es presenta, s'estableixen les obligacions de definir, implementar, i evolucionar una estratègia nacional de ciberseguretat, de gestionar els riscos de ciberseguretat, d'incrementar la cooperació amb altres estats, especialment els propers, i de millorar la resiliència de les entitats públiques i privades que resulten "essencials" o "crítiques" per prestar o tenir el potencial de prestar serveis fonamentals per a l'economia i la societat andorranes en l'àmbit de vuit sectors digitalitzats o en vies de digitalització (energia, transports, banca, infraestructures dels mercats financers, sanitat, aigües potables i residuals, infraestructura digital, i administració pública), i de determinades entitats "importants" que operen en altres sectors no essencials però considerats importants (serveis postals i de missatgeria, gestió de residus, fabricació, producció i distribució de substàncies i mescles químiques, producció, transformació i distribució d'aliments, fabricació, i prestadors de serveis digitals), i s'exigeix que el nostre país garanteixi que les nostres entitats essencials i importants, ja siguin de naturalesa pública o privada, comptin amb requisits en matèria de ciberseguretat i notifiquin els incidents que pateixin en relació amb aquesta matèria.

Igual que estan fent cada cop més les normatives en matèria de protecció de dades personals i les que regulen els actius digitals, el projecte de Llei que es presenta canvia el paradigma del repartiment de rols i responsabilitats entre les autoritats de control i les entitats incloses en els seus àmbits d'actuació. La creixent transformació digital ha

demostrat ineficient el model d'autoritat de control que pretén definir i imposar les mesures tècniques i organitzatives amb les quals s'hauria de reduir l'exposició de tot tipus d'entitats als riscos que tenen el seu origen en els ciberincidents. Per a poder contemplar l'enorme diversitat dels riscos de les ciberincidències i adequar-se a la velocitat amb la que canvien tant aquests riscos com les mesures que han d'implantar les entitats, és necessari adoptar una aproximació de responsabilitat descentralitzada. El projecte de Llei que es presenta estableix, per tant, que sigui cada entitat essencial o important la que quedi obligada a demostrar la seva responsabilitat proactiva en la identificació i gestió dels riscos per als serveis que la classifiquen com a essencial o important, de forma proporcionada en relació amb els riscos que presenten les xarxes i els sistemes d'informació que utilitza, i tenint en compte l'estat de la tècnica. Són doncs aquestes entitats, independentment de si s'encarreguen elles mateixes del manteniment de les seves xarxes i sistemes d'informació o l'externalitzen, les que es responsabilitzen de determinar els seus propis requisits de seguretat, i d'implantar les mesures tècniques i organitzatives que elles mateixes considerin necessàries i suficients per a reduir el seu risc de patir ciberincidències greus fins a un nivell que l'autoritat de control consideri suficient, sobre la base d'uns criteris definits, i les que queden obligades a notificar molt ràpidament els seus incidents de ciberseguretat per a, entre d'altres raons, evitar la seva propagació, i que altres entitats puguin beneficiar-se tant de l'alerta com de les lliçons apreses. I, fins i tot, són les pròpies entitats les que queden obligades a informar els seus usuaris quan aquesta informació pugui reduir el risc de la ciberamenaça per a aquests. En aquest nou paradigma, el paper de l'autoritat de control deixa de ser el de reguladora que dicta mesures suposadament eficients per al conjunt dels sectors i activitats, i passa a ser, principalment, el de supervisora de la responsabilitat proactiva de les entitats, amb capacitat per a sancionar-les amb, entre d'altres, multes administratives que han de ser efectives, proporcionades i dissuasives, i per a, fins i tot, imposar prohibicions temporals per a que determinades persones físiques exerceixin funcions de direcció.

Aquesta nova aproximació s'ha mostrat més eficient que la del regulador clàssic per a minimitzar el cost total dels ciberincidents, resultant de sumar els costos associats al compliment de la normativa i els costos associats als danys i perjudicis econòmics i socials que causen els ciberincidents. Així, la seva ràpida i adequada implantació és estrictament necessària per a aconseguir els objectius específics de transformació digital del Principat d'Andorra de manera satisfactòria.

El projecte de Llei que es presenta es divideix en un total quatre títols i dos annexos, en els quals s'hi estableix el seu objecte, àmbit d'aplicació i definicions, el marc estratègic i institucional, les obligacions tant per a les entitats essencials, siguin o no crítiques, i importants com per a les autoritats de control competents i l'equip de referència de resposta del Principat d'Andorra per al tractament d'incidents de ciberseguretat, el règim sancionador, els sectors a considerar per a la identificació d'entitats essencials, i els sectors a considerar per a la identificació d'entitats importants

Així mateix, el projecte de Llei que es presenta inclou una disposició addicional i cinc disposicions finals.

La disposició addicional encomana al Govern que, en el termini màxim de dos anys, avaluï la conveniència de constituir o no una entitat amb personalitat jurídica pròpia que assumeixi funcions diverses en matèria de digitalització, o relacionades amb aquesta matèria, incloent-hi l'ANC-AD i el CSIRT-AD.

Pel que fa a les disposicions finals, les dues primeres modifiquen la Llei 4/2020, del 23 de març, qualificada dels estats d'alarma i d'emergència, i la Llei 30/2018, del 6 de desembre, qualificada de seguretat pública, modificada per la Llei 19/2020, del 23 de desembre, de seguretat pública, especialment per a l'establiment de mesures en cas que el funcionament de les entitats essencials o importants així o requereixi. Les altres tres disposicions finals, són relatives a l'habilitació per al desenvolupament reglamentari, l'habilitació per a la consolidació de textos i l'entrada en vigor d'aquesta Llei.

II. Contingut del projecte de Llei

II.1. Títols, capítols i articulat

El títols que conformen el cos del projecte de Llei que es presenta, s'estructuren com segueix:

Un **Títol I** per a les disposicions generals, dividit en tres articles que recullen, respectivament:

L'objecte de la Llei (article 1), consistent en regular el reforç de la resiliència de les entitats crítiques i la seguretat de les xarxes i dels sistemes d'informació utilitzats per a la prestació de serveis essencials i importants al Principat d'Andorra.

L’àmbit d'aplicació de la Llei (article 2), consistent en que la mateixa aplica a les entitats públiques i privades contemplades en el marc de les entitats essencials i importants que ocupen a 50 o més persones o el volum anual de negocis de les quals o el seu balanç general anual superi els €10M. Addicionalment, la Llei aplica a les entitats essencials i importants, amb independència de la seva grandària i volum anual de negoci o balanç general anual, quan es compleixen determinades circumstàncies establertes al referit article 2 .

Les definicions que apliquen en el context d’aquesta llei (article 3).

Un **Títol II** en el que es regula el marc estratègic institucional, i que es divideix en dos capítols:

Un primer capítol per al marc estratègic, amb dos articles que regulen:

El marc estratègic de seguretat de les xarxes i dels sistemes d’informació (article 4), i el marc nacional de gestió de crisis de ciberseguretat (article 5).

I un segon capítol dedicat al marc institucional, que conté quatre articles que nomenen dues autoritats competents per a la supervisió del compliment de la Llei en els sectors d’especialització (l’AFA per als sectors de la seva competència, i l’ANC-AD), amb l’ànim d’evitar la fragmentació de responsabilitats, i el seu consegüent sobrecost, obligant-les a col·laborar en les noves obligacions que els són comunes (article 6).

Així mateix, en aquest capítol es nomena al CSIRT-AD com l’equip de referència de resposta als incidents de seguretat de les xarxes i els sistemes d’informació de totes les entitats essencials i importants (article 8), i es regulen les funcions que, dins de l’àmbit de la Llei, tenen les autoritats competents (article 7) i el CSIRT-AD (article 9).

Un **Títol III** que regula les obligacions que la Llei imposa a cadascun dels ens que estan dins del seu àmbit d’aplicació, i que es divideix en quatre capítols:

Un primer capítol dedicat a regular les principals obligacions de ciberseguretat, que conté set articles que regulen:

L’obligació que tenen les entitats d’identificar-se com essencials o importants, d’acord amb les definicions d’aquestes donada en la pròpia Llei (article 10).

L’obligació que tenen les autoritats competents d’identificar les entitats crítiques conforme a la forma en que han estat definides en la Llei (article 11).

Les obligacions de ciberseguretat de les entitats essencials i importants (article 12).

Les obligacions d'aquestes entitats d'adoptar mesures tècniques i d'organització adequades i proporcionades per a gestionar els riscos de ciberseguretat existents per a la seguretat de les seves xarxes i sistemes d'informació (article 13), de resoldre els seus incidents (article 14), i de notificar aquests incidents al CSIRT-AD, que al seu torn ho notificarà a la corresponent autoritat competent (article 15).

I, finalment, la possibilitat que té qualsevol tipus d'entitat de notificar al CSIRT-AD qualsevol tipus d'incident de seguretat, sense que aquesta notificació, sempre que sigui voluntària i no obligada per la Llei, suposi cap obligació per a l'entitat notificant addicional a la de resoldre l'incident (article 16),

Un segon capítol, que estableix la resta d'obligacions de les entitats essencials i importants, que conté cinc articles amb els quals es regulen:

La governança de la ciberseguretat dins les entitats essencials i importants (article 17).

La figura del Delegat de la Seguretat de la Informació (article 18). D'acord amb aquest article, les entitats essencials i les entitats importants, a través dels seus òrgans de direcció, han de designar una persona física, una unitat o un òrgan col·legiat, perquè actuï com a Delegat de la Seguretat de la Informació i sigui el punt de contacte i coordinació tècnica entre l'entitat que l'ha nomenat i l'autoritat competent i el CSIRT-AD.

La figura del Representant al Principat d'Andorra, necessària quan l'entitat que proveeix un servei essencial o important pel país no té establiment dins el Principat (article 19).

També es preveu l'aprovació per via reglamentària d'esquemes de certificació dels diferents àmbits de la ciberseguretat, que d'una banda siguin d'obligació per determinades entitats o categories d'entitats seleccionades per les autoritats competents, i de l'altra, serveixin a les entitats per acreditar davant els seus usuaris el seu compliment en matèria d'aquests àmbits de la ciberseguretat (article 20).

Finalment, es preveu la protecció del notificador que actua de bona fe, davant les possibles represàlies de l'entitat que ha patit l'incident de seguretat (article 21).

Un tercer capítol dedicat a la supervisió del compliment de la Llei, amb tres articles que regulen, respectivament:

L'obligació de les autoritats competents de controlar el compliment de la Llei, i la potestat per demanar la col·laboració del CSIRT-AD en les funcions de control que duen a terme (article 22).

El règim de supervisió, a priori preventiva, que ha d'aplicar a les entitats essencials (article 23).

I, finalment, el règim de supervisió a posteriori (quan es disposi de proves o indicis d'incompliment) que aplicarà a les entitats importants (article 24), per a evitar així carregar excessivament a les autoritats competents i al CSIRT-AD.

Un quart capítol dedicat a la resta d'obligacions de les autoritats competents i del CSIRT-AD, que conté un total de cinc articles, que regulen:

L'obligació dels intervinents de mantenir la confidencialitat respecte a la informació sensible a la que tinguin accés per raó d'aquesta Llei (article 29).

Les obligacions de cooperació en els àmbits nacional (article 27) i transfronterer (article 28).

I, finalment, la resta d'obligacions que la Llei imposa a les autoritats competents (article 25) i al CSIRT-AD (article 26).

Un **Títol IV**, que regula el règim sancionador, i consta de dotze articles que recullen, respectivament:

La potestat sancionadora (article 30), que correspon a l'autoritat que en cada moment estigui al capdavant de l'ANC-AD, també pel que fa a les entitats que estiguin sota la supervisió de l'AFA, a petició d'aquesta última. La instrucció dels expedients correspon als tècnics designats per l'ANC-AD.

Els subjectes responsables de les infraccions (article 31), és a dir les entitats essencials i importants sotmeses al compliment dels preceptes de la Llei.

El detall de l'expedient sancionador (article 32), així com la identificació d'allò que es considera infracció (article 33), la classificació de les infraccions (article 34), i el cas especial d'infraccions que comporten una violació de la seguretat de les dades personals (article 35).

Les sancions associades a les infraccions (article 36), la seva graduació (article 37), la seva proporcionalitat (article 38), i la seva eventual concurrència amb altres sancions (article 39).

Finalment, es preveuen els terminis per a la prescripció de les infraccions (article 40) i de les sancions (article 41).

El cos del projecte de Llei que es presenta també compta amb **dos annexos que completen el cos de la Llei,** que estableixen els sectors, subsectors, i tipus d'entitats que s'han de considerar com a essencials (annex I) i com a importants (annex II).

II.2. Disposicions

El projecte de Llei que es presenta compta amb una **Disposició Addicional** que té com a finalitat encomanar al Govern que, en el termini màxim de dos anys, avaluï la conveniència de constituir o no una entitat amb personalitat jurídica pròpia que assumeixi funcions diverses en matèria de digitalització, o relacionades amb aquesta matèria, incloent-hi l'ANC-AD i el CSIRT-AD.

Pel que fa a les **Disposicions Finals** que inclou el projecte de Llei que es presenta, són cinc, i tenen com a finalitat:

La Primera i la Segona, modificar, respectivament, la Llei 4/2020, del 23 de març, qualificada dels estats d'alarma i d'emergència (disposició final primera), i la Llei 30/2018, del 6 de desembre, qualificada de seguretat pública, modificada per la Llei 19/2020, del 23 de desembre, de seguretat pública (disposició final segona), per tal d'alinear-les amb aquesta Llei,

La Tercera i la Quarta, respectivament, habilitar al Govern per al desenvolupament reglamentari i per a la consolidació de textos de les Lleis modificades.

I la Cinquena, establir la entrada en vigor de la Llei. Concretament, es proposa que la Llei entri en vigor l'endemà de ser publicada al Butlletí Oficial del Principat d'Andorra, no obstant el Capítol Tercer del Títol III (supervisió) i el Títol IV (règim sancionador) de la Llei entrarien en vigor en el termini de dos anys a comptar de l'entrada en vigor de la resta de l'articulat de la Llei.

III. Valoració de l'impacte econòmic

L'entrada en vigor del projecte de Llei que es presenta, ha de ser el motivant per a dotar a l'Agència de Ciberseguretat d'Andorra de tots aquells recursos necessaris per a poder desenvolupar amb garanties la seva missió, funcions, activitats i obligacions que se li encomanen.

En aquest sentit, dins d'un marc temporal acotat i entès com de consolidació, l'Agència requerirà en un primer terme d'una estructura mínima de recursos materials i humans que li permetin donar inici a la seva base de funcionament i activitat.

En termes temporals, aquesta fase d'inici de l'activitat i consolidació dels serveis no hauria de ser superior a dos exercicis pressupostaris, i pels que s'han estimat preliminarment uns costos generals associats que se situarien al voltant dels 400.000€ per exercici.

Les valoracions econòmiques inclouen tant partides per fer front a les necessitats estructurals del propi funcionament de l'Agència (instal·lacions, infraestructura de xarxa, serveis TIC, o d'altres de naturalesa similar), com de partides considerares per a donar cobertura a aquells serveis que l'Agència preveu oferir. En relació amb la primera agrupació de necessitats econòmiques, s'ha previst una dotació de 150.000€ anuals, mentre pel que fa a la cobertura dels serveis a oferir, s'estimen uns 250.00€ per exercici, dins dels quals en quedaria inclosa l'operació.

Durant aquesta primera fase de consolidació – 2 exercicis - el finançament de l'agència es farà mitjançant els recursos de la fundació Andorra Recerca i Innovació, i més concretament del pressupost d'Andorra Digital.

Posteriorment, una vegada superada aquesta fase inicial de llançament i consolidació de serveis, es requerirà avaluar noves necessitats en funció, entre altres, de l'evolució de l'estratègia nacional en ciberseguretat, i de totes aquelles consideracions emergents pròpiament dins l'àmbit de la ciberseguretat. Per tant, dins d'aquest nou cicle s'identificaran, avaluaran i concretaran noves iniciatives que hauran de complementar les activitats en curs.

Així mateix, les dotacions econòmiques hauran de ser ajustades i convenientment introduïdes als pressupostos generals de l'Estat, assignant aquells mitjans necessaris per

a garantir la seva viabilitat i execució, així com per avalar la continuïtat global de les funcions, finalitats i activitats de l'Agència Nacional de Ciberseguretat en el temps.

Per altra banda, i no menys important, aquesta llei ha de generar un impacte favorable envers l'economia, especialment gràcies a la mitigació del nombre d'incidents de ciberseguretat registrats al país. El desenvolupament per part de l'Agència d'activitats encaminades a la sensibilització i conscienciació que tinguin principalment com a públic objectiu el teixit empresarial i la ciutadania, haurien de contribuir a l'augment del grau de prevenció d'aquests col·lectius, i per tant, a la reducció dels incidents en l'àmbit de la ciberseguretat.

En clau de contextualitzar amb xifres els possibles beneficis que podrien aportar a l'economia de l'Estat una adequada prevenció, a tall d'exemple i en termes de ciutadania, la recepció de missatges fraudulents (phishing) representa la tipologia d'incidència més destacada, amb un 26% dels atacs, mentre que la redirecció cap a pàgines web falses sol·licitant informació personal (pharming) se situa al 13% de mitjana a nivell europeu. Pel que fa als negocis, aproximadament el 50% dels ciberatacs es dirigeixen a petites empreses, de les quals una ampla majoria no disposa dels coneixements bàsics per a fer front a un atac d'aquesta naturalesa.

En un país proper com Espanya, en el darrer any es van gestionar 133.155 incidents de seguretat, es van documentar 19.211 noves vulnerabilitats, i es van atendre 47.503 consultes relacionades amb la ciberseguretat.

En definitiva, tots aquests valors donen ordres de magnitud sobre la importància i el benefici que una adequada activitat preventiva per part de l'Agència pot aportar en clau econòmica al país.

Finalment, i també a mode d'impacte positiu cap a l'economia del país, les mesures que s'estableixen dins del present text legislatiu han de representar una garantia pel creixement de l'activitat econòmica, no únicament vinculada als negocis de base digital, l'emprenedoria o la innovació, sinó també a tota mena d'activitat que requereixi d'un entorn segur i confiable per al seu adequat desenvolupament.

IV. Perspectiva de gènere

La Llei 13/2019, del 15 de febrer, per a la igualtat de tracte i la no-discriminació estableix al seu article 5 que "el dret a la igualtat de tracte i a la no-discriminació informa, amb caràcter transversal, l'actuació de tots els poders públics. Les administracions públiques l'han d'integrar en l'adopció i l'execució de totes les disposicions normatives i les polítiques públiques. En particular, els poders públics i les administracions públiques han d'integrar el principi d'igualtat de tracte i d'oportunitats entre dones i homes en totes les seves actuacions i en l'adopció i l'execució de les disposicions normatives i les polítiques públiques".

Tanmateix, es considera que una norma no té rellevància de gènere quan no afecta directament o indirectament persones, o, fent-ho, afecta de forma molt limitada l'accés als recursos econòmics i socials de les dones i els homes, la seva participació en els àmbits de presa de decisions, o les normes socials i els valors que influeixen en l'origen i el manteniment de les desigualtats de gènere.

En aquest sentit, el projecte de Llei que es presenta no té una repercussió directa o indirecta pel que fa a les qüestions de gènere.

A Andorra la Vella, l'1 de desembre del 2021