SINTEZA
obiecțiilor și propunerilor/recomandărilor
în cadrul consultării publice a proiectului hotărârii de Guvern
cu privire la aprobarea proiectului de lege privind securitatea cibernetică

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
1.	**Asociația Băncilor din Moldova** nr. 02-10/9 din 12.01.2023	***1)***	Potrivit Notei informative, proiectul de lege are drept scop soluționarea problemei privind protecția împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, datorită dezvoltării rapide, pe parcursul ultimilor ani, a tehnologiei informației și comunicațiilor electronice și a proceselor de transformare digitală. Astfel, în contextul dezvoltării rapide a digitalizării economiei considerăm binevenită adoptarea unui cadru normativ ce are drept scop reducerea riscurilor în domeniul securității rețelelor și a sistemelor informatice. Totodată, analizând prevederile din proiectul de lege, în special art.(3) alin. (1) și (2), nu se constată cu certitudine aplicabilitatea legii asupra sectorului bancar. În acest context, este de menționat că riscurile aferente denaturării securității și integrității sistemelor informaționale, ca subcategorie a riscului operațional, precum și riscul tehnologiei informației și comunicațiilor (risc TIC), pentru sistemul bancar sunt reglementate de către Regulator prin Regulamentul privind cadrul de administrare a activității băncilor, nr. 322/2018 (a se vedea pct. 259-272, inclusiv pct. 4). Mai mult, începând cu data de 21.03.2022, Banca Națională a Moldovei a inițiat consultarea publică a proiectului Hotărârii Comitetului executiv al Băncii Naționale a Moldovei „Pentru aprobarea Regulamentului privind cerințele minime pentru	**Precizare.** Proiectul de lege are, printre altele ca obiectiv armonizarea legislației naționale la legislația Uniunii Europene. Din această perspectivă, în conformitate cu prevederile cadrului normativ național proiectul de lege este o primă acțiune cu caracter normativ de inițierea procesului de transpunere în legislația și sistemul administrativ intern a Directivei NIS2. Acest act al UE a fost publicat la data de 27 decembrie 2022, împreună cu alte două acte legislative - Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (Directiva CER); - Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Regulamentul DORA). În context, ținem să evidențiem că Directiva NIS2, ca de altfel și Directiva NIS, sunt acte cu un efect orizontal, nefiind un instrument de sine stătător. Prin urmare, transpunerea Directivei NIS2 în legislația națională nu poate fi concepută fără demararea imediată a proceselor de transpunere și a celorlalte două acte, parte a pachetului legislativ european direcționat spre creșterea și

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			gestiunea riscurilor TIC și de securitate a informației", care are ca scop să asigure că băncile vor dispune de un cadru intern adecvat pentru gestiunea riscurilor TIC și de securitate a informației aliniat la strategia generală de afaceri, iar procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele TIC ale băncii și protejează în mod corespunzător sistemele TIC ale băncilor, precum și de aliniere a cerințelor BNM, în acest domeniu, la "Ghidul EBA privind administrarea riscurilor TIC și de securitate" și la standardele internaționale în domeniu.	îmbunătățirea rezilienței sectoarelor de o importanță critică fundamentală pentru funcționarea economiei și a statului. Importanța acestui exercițiu este determinată și de interconexiunile dintre cele trei documente. Regulamentul DORA are un caracter de lex specialis față de prevederile conținute în Directiva NIS2[1], iar interconexiunile[2] dintre Directiva CER și Directiva NIS2 urmează a fi abordate din perspectiva unor cadre de politici coerente pentru o coordonare consolidată și cooperare eficientă dintre autoritățile competente conform ambelor directive, inclusiv din punctul de vedere al raționalizării activităților de supraveghere și reducerii la minimum a sarcinii administrative. Desincronizarea acestor procese la nivel național, de transpunere a celor trei acte europene, constituie un risc serios de implementare a prevederilor proiectului de lege. De asemenea, autoritățile administrației publice centrale de specialitate responsabile de realizarea politicii de stat în sectoarele și subsectoarele enumerate în anexele II și III ale directivei NIS2 urmează să efectueze o evaluare a gradului de transpunere a legislației UE la care se face referire în aceste anexe, și după caz, să inițieze modificarea legislației sectoriale relevante. Potrivit proiectului de lege sectoarele și subsectoarele critice urmează a fi stabilite de către Guvern. Cu toate acestea, urmând conceptele și institutele juridice consacrate în directiva NIS2, în proiectul de lege au fost stabilite prevederi fundamentale privind aplicabilitatea prevederilor legii privind securitatea cibernetică în raport cu legile care reglementează activitatea furnizorilor de servicii în

[1] Considerentul (28) din Directiva NIS2: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555
[2] Considerentul (30) din Directiva NIS2: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				sectoarele/subsectoarele critice, inclusiv cel financiar și cel bancar. Astfel, art. 3 alin.(6) prevede expres că în cazul în care legile sectoriale specifice stabilesc implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor semnificative, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile prezentei legi. Autoritatea competentă urmând a fi responsabilă de aplicarea acestei prevederi legale. Această normă legală se înscrie în contextul conceptelor propuse în Directiva NIS2 în ce privește interconexiunea cu actele sectoriale al UE. În situația în care, chestiunile ce țin de gestionarea riscurilor și obligațiile de raportare ale entităților financiare vor fi reglementate în actul sectorial de o manieră care va institui obligații de un nivel mai redus decât cele stabilite de proiectul de lege, proiectul de lege ar trebui să fie aplicabil.
2.		***2)***	Pe această cale solicităm respectuos consultarea suplimentară a proiectului de lege urmare revizuirii acestuia prin prisma propunerilor în procesul actual de avizare.	**Se acceptă.** Proiectul, conform procedurilor stabilite de Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, În mod special punctele 201-202 urmează a fi supus examinării suplimentare de către părțile interesate, inclusiv cele ale căror obiecții și propuneri în procesul de consultare publică și avizare oficială nu au fost acceptate. În continuare, potrivit pct. 203 din același act, în cazul existenţei obiecţiilor neacceptate sau acceptate parţial, pentru a ajunge la un consens în privinţa acestora, autorul convoacă o şedinţă comună interministerială (interinstituţională). În acest scop, autorul expediază participanţilor la avizare, cu cel puţin 5 zile lucrătoare înainte de desfășurarea şedinţei, informația privind locul,

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				data și ora desfășurării ședinței respective, proiectul elaborat, nota informativă la acesta, sinteza obiecțiilor și propunerilor la proiect, precum și alte documente relevante pentru depășirea divergențelor existente pe marginea proiectului. De asemenea, în conformitate cu prevederile Legii nr. 100/2017 privind actele normative, dacă proiectul de lege va suferi ajustări esențiale, acesta urmează a fi supus repetat consultării publice și avizării oficiale. Astfel potrivit art. 32 alin. (7) din această lege *dacă, în urma avizării şi consultării publice, proiectul actului normativ a fost completat cu aspecte şi concepte noi sau dacă mai mult de 30% din textul proiectului actului normativ a fost modificat, acesta trebuie remis repetat spre avizare şi consultare publică*.
3.	**MoldovaGaz** Nr. 07-348 din 25.01.2023	***3)***	Menționam ca, în cazul incidentelor de securitate Autoritatea competentă va acumula, în urma raportărilor, informații confidențiale, în special, cauza apariției vulnerabilității de securitate. Prin urmare, nu este exclus că, din motivul respectării unor proceduri corporative, care necesita niște investiții sau aprobări, aceste vulnerabilități nu vor fi înlăturate imediat, dar vor fi exploatate cu asumarea unui risc. Toate aceste informații vor fi în gestiunea exclusivă a Autorității competente, însă proiectul legii nu specifica gradul de protecție a informației confidențiale și a datelor cu caracter personal, de cine sunt accesate aceste informații fumizate și cu ce scop, modalitatea de păstrare. Consideram ca astfel de informații prezintă un interes sporit în rândul persoanelor de rea-credința, respectiv furnizorii de informații, sunt în drept să cunoască cum are loc protejarea informațiilor transmise, care este responsabilitatea Autorității competente în protejarea datelor confidențiale și a datelor cu caracter personal.	**Se acceptă.** La art. 7 alin. (4) punctul 9) a fost completat cu textul *precum şi asigură, în conformitate cu legislaţia, protecţia informaţiilor de care ia cunoştinţă în procesul exercitării atribuţiilor sale*. De asemenea art. 15 alineatul 4 a fost îmbunătățit, rezultând următoarea redacție: *În exercitarea competenței sale în procesul gestionării incidentelor cibernetice, autoritatea competentă este obligată să țină cont de interesele de afaceri ale furnizorului de servicii, să asigure păstrarea secretului comercial în condițiile legislației. Autoritatea competentă asigură protecția informațiilor atribuite la secretul de stat și a datelor cu caracter personal în conformitate cu prevederile actelor normative din aceste domenii.* De asemenea, ținem să remarcăm faptul că proiectul de lege nu are ca obiect de reglementare stabilirea anumitor mecanisme de protecție a diferitelor categorii de informații. Aceste problematici sunt obiectul altor legi în funcție de

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			Urmare celor expuse, consideram ca proiectul de lege ar fi mai executiv, daca ar fi completat cu prevederi ce reglementează sugestiile expuse mai sus.	categoria informațiilor. Astfel, spre exemplu informațiile care vor conține date cu caracter personal și vor constitui obiectul procesării în cadrul exercitării de către autoritatea competentă și a furnizorilor de servicii beneficiază de protecție în condițiile și conform regimului juridic stabilit de Legea nr. 133/2011 privind protecția datelor cu caracter personal. Actualmente potențialii furnizori de servicii deja procesează date cu caracter personal și prelucrarea acestora se efectuează în conformitate cu legea, chiar și contextul relațiilor cu autoritățile publice sau cu alte persoane juridice sub imperiul normelor juridice de drept privat. În consecință preluarea sau referirea declarativă la actele normative relevante în ce privește necesitatea de a proteja anumite informații cu regim special est inutilă din punctul de vedere al activității de legiferare.
4.	**Asociația Națională a Companiilor din sectorul TIC** Nr. 552 din 26.01.2023	***4)***	**1.**La art. 1 se propune de adăugat un aliniat, conform recit. 143 din Directiva NIS 2.0, cu urmatorul text: "*Prezenta lege respectă drepturile fundamentale, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare. Prezenta lege va fi pusă în aplicare în conformitate cu drepturile și principiile menționate*."	**Nu se acceptă.** Textul propus deși este unul relevant, este totuși lipsit de utilitate normativ-juridică din perspectiva obiectului de reglementare al proiectului de lege propus spre consultare. Astfel, principiile și drepturile fundamentale invocate sunt deja obiectul atât normelor constituționale, cât și normelor juridice cuprinse în actele legislative ce reglementează domenii specifice de intervenție, cum ar fi Legea nr. 133/2011 privind protecția datelor cu caracter personal, Codul de procedură penală, Codul civil, Legea cu privire la antreprenoriat și întreprinderi, etc. Principiile activității de legiferare, stabilite de art. 3 din Legea nr. 100/2017 privind actele normative, precum sunt constituționalitatea; respectarea drepturilor și libertăților fundamentale; legalitatea și echilibrul între reglementările concurente; oportunitatea, coerența, consecutivitatea, stabilitatea și predictibilitatea normelor juridice, sunt principii ce urmează a fi aplicate în procesul elaborării oricărui act

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				normativ, fără însă a fi necesar de a fi expres menționată dacă aceasta nu este oportun pentru reglementare respectivă.
		5)	**2.**La art. 2 pct. 2), nu este clar ce se înțelege prin "persoană juridică care prestează servicii": furnizor de servicii în sensul legii în cauză sau orice prestator de servicii. De remarcat ca Directiva NIS2 se refera la entitate, definita drept o persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații.	**Precizare.** Sintagma „persoană juridică care prestează servicii" este utilizată în sens larg, nu de furnizor de servicii. Relația dintre aceste două concepte consistă în mod principal în exercitarea de către autoritatea competentă a prerogativelor sale de identificare a „persoanelor juridice ce prestează servicii" ca fiind furnizori de servicii căruia i se incumbă obligațiile prevăzute de lege. Din altă perspectivă în contextul noțiunii de amenințare cibernetică semnificativă sintagma persoane juridice ce prestează servicii are obiectivul de a extinde aria de subiecți care ar putea fi afectați și la aceia care sunt în relații contractuale cu furnizorii de servicii.
		6)	**3**.La art. 7, alin. 2, lit. g), se propune definirea mai clară a tipurilor de scanare proactivă și identificarea principalelor categorii de date cu caracter personal implicate, deoarece aici se referă nu doar la scanarea în rețea, ci și la scanarea sistemelor informatice în general (aplicații, servere și baze de date) și respectiv, nu se delimitează suficient natura prelucrării datelor cu caracter personal implicate în scanarea proactivă.	**Nu se acceptă.** Prevederea respectivă este suficientă din perspectiva cadrului funcțional al autorității competente. Completarea cu informațiile propuse de autorul obiecției ar putea restrânge nejustificat posibilități și metodele de acordate de suport furnizorilor de servicii de către autoritatea competentă. În același timp este important de menționat faptul că stabilirea procesului de monitorizare a rețelelor și sistemelor informatice reprezintă o măsură elementară pentru asigurarea securității acestora, care este introdusă implicit în toate sistemele de standarde de securitate a informației recunoscute la nivel internațional. Din punctul de vedere al Directivei NISD și al Directivei NISD2, în măsura în care este necesar și proporțional în scopul asigurării securității rețelelor și a sistemelor informatice de către entitățile esențiale și importante,

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				prelucrarea datelor cu caracter personal ar putea fi considerată legală pe baza faptului că această prelucrare respectă o obligație legală la care este supus operatorul, în conformitate cu cerințele articolului 6 alineatul (1) litera (c) și ale articolului 6 alineatul (3) din GDPR. Prelucrarea datelor cu caracter personal ar putea fi, de asemenea, necesară pentru interesele legitime urmărite de entități esențiale și importante, în conformitate cu articolul 6 alineatul (1) litera (f) din GDPR, inclusiv atunci când o astfel de prelucrare este necesară pentru securitatea cibernetică, pentru acorduri de schimb de informații sau pentru notificarea voluntară a informațiilor relevante în conformitate cu NISD2. În plus, prelucrarea datelor cu caracter personal de către autoritățile competente, punctele unice de contact și CSIRT-urile naționale ar putea constitui o obligație legală sau ar putea fi considerată necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul, în conformitate cu articolul 6 alineatul (1) literele (c) sau (e) și cu articolul 6 alineatul (3) din GDPR, sau pentru urmărirea unui interes legitim al entităților esențiale și importante, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din GDPR. Din perspectiva legislației naționale prevederile literelor b) - e) ale art. 5 alin. (5) din Legea nr. 133/2011 privind protecția datelor cu caracter personal în mod special sunt relevante în acest sens.
		7)	**4.Reținem prevederile următoarelor articole din Directiva NIS 2.0:** - *Art.8 alin. (1)* Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VII (autorități competente). **(3)** Fiecare	**Nu se acceptă.** Prevederile proiectului de lege care abordează cadrul instituțional în domeniul securității cibernetice este reprezentat în principal de articolele 6 și 7. Astfel, coordonarea strategică la nivel național este atribuită Guvernului, care va aproba un set de acte normative

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			stat membru desemnează sau instituie un punct unic de contact. În cazul în care un stat membru desemnează sau instituie o singură autoritate competentă conform alin.(1), autoritatea competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv. - *Art. 9 alin.(1)-(2)* Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor (denumite în continuare „autorități de gestionare a crizelor cibernetice"). În cazul în care un stat membru desemnează sau instituie mai mult de o autoritate de gestionare a crizelor cibernetice în temeiul alin. (1), acesta indică în mod clar care dintre autoritățile respective servește drept coordonator pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor. - *Art. 10 alin.(1)* Fiecare stat membru desemnează sau instituie una sau mai multe echipe CSIRT. Echipele CSIRT pot fi desemnate sau instituite din cadrul unei autorități competente. Așadar, având în vedere prevederile Directivei NIS 2.0 citate supra, se propune modificarea art. 7 din proiectul Legii privind securitatea cibernetică, care la momentul actual indică: *„(1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia. (2) Autoritatea competentă desemnată de Guvern exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național."* Se propune excluderea prevederii legale privind desemnarea unei singure autorități competente ce va exercita cumulativ și funcțiile de punct național unic de contact și funcțiile echipei de răspuns la incidentele cibernetice la nivel național.	orientate spre punerea în aplicare a prevederilor legii. În nota informativă, la compartimentul al șaselea este dată lista chestiunilor care vor necesita intervenția pe dimensiunea reglementării din partea Guvernului, inclusiv Strategia privind securitatea cibernetică.. Pentru asigurarea realizării acestei funcții – de coordonare strategică – Guvernului, conform art. 6 alin. (2), i se deleagă competența de a institui un consiliu coordonator în acest domeniu. Potrivit art. 7 alin. (1) Guvernului i se deleagă atribuția de a desemna o autoritate competentă în domeniul securității cibernetice și să stabilească modul de organizare și funcționare a acesteia. Din perspectivă instituțională, conceptul propus în proiect, ca Guvernul să decidă desemnarea autorității competente în domeniul securității cibernetice se înscrie în spectrul exercitării de către Guvern a prerogativelor sale în stabilirea modului de organizare și funcționare a persoanelor juridice de drept public din structura guvernamentală. Astfel, potrivit prevederilor art. 6 literele b), d) și e) din Legea nr. 136/2017 cu privire la Guvern, Guvernul este împuternicit să constituie în structura sa atât autorități administrative centrale, cât și structuri organizaționale în sfera de competență a acestora și cea a ministerelor, precum și să le reglementeze modul de organizare și funcționare. Bineînțeles această marjă discreționară acordată de către Parament Guvernului este limitată, pe de o parte de obiectivele strategice ce urmează a fi realizate și de necesitatea asigurării eficienței și eficacității activității administrative, iar pe de alta de normele legale primare care reglementează administrația publică centrală de specialitate.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				Modul de organizare și funcționare a persoanelor juridice de drept public în structura Guvernului este stabilit de Legea nr. 98/2014 privind administrația publică centrală de specialitate. Conform proiectului autoritatea competentă în domeniul securității cibernetice, de rând cu funcțiile de echipă de răspuns la incidentele cibernetice la nivel național și de punct național unic de contact urmează să exercite și funcția de supraveghere și control a modului de realizare a obligațiilor stabilite de lege de către furnizorii de servicii, precum și alte atribuții care vizează implementarea politicii statului în domeniul securității cibernetice. Prevederile respective ale proiectului de lege în coroborare cu prevederile art. 4 pct. 1) lit. b), ale art. 14 alin. (5) și ale art. 25 alin. (2) lit. c) ne permit să identificăm forma juridică de organizare a viitoarei autorități competente și anume de autoritate administrativă subordonată unui minister sau unei autorități administrative centrale. Această opțiune specifică în exercitarea de către Guvern a acestei prerogative ar putea fi revăzută la discreția Guvernului, în limitele expuse mai sus, în funcție de evoluția situației atât la nivelul activității administrative guvernamentale, cât și la nivelul sectorului specific asigurării securității cibernetice. În ce privește așa-numita funcție de „*autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*”. , menționăm că aceasta nu este o funcție a autorității competente în domeniul securității cibernetice, ci este o sintagmă legală care, prin prisma prevederilor Legii nr. 98/2012, reprezintă un minister sau o autoritate administrativă centrală care realizează politica de stat în acest domeniu. Din perspectiva delimitării funcțiilor în

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				interiorul structurii unui minister menționăm că un minister (o autoritate administrativă centrală) nu trebuie confundat cu aparatul central al acestuia care, potrivit prevederilor art.30 din Legea nr. 98/2012 este responsabil de elaborarea, elaborarea, monitorizarea și evaluarea politicilor publice în domeniile de activitate ale acestuia, pe când realizarea celorlalte funcții prevăzute de art. 25 din Legea nr. 98/2014 (supraveghere și control, prestare de servicii publice, alte funcții de implementare), în vederea respectării unui principiu fundamental în organizarea și funcționarea administrației publice delimitarea funcțiilor de elaborare a politicilor de cele de implementare, urmează a fi atribuite unor autorități administrative subordonate ministerului responsabil de realizarea politicii respective. Aceste autorități administrative sunt prin excelență instrumente instituționale ale unui minister în procesul de implementare a politicii de stat. Actualmente realizarea politicii de stat în domeniul securității cibernetice este prerogativa Ministerului Dezvoltării Economice și Digitalizării. Prin urmare, în temeiul cadrului normativ enunțat mai sus în coroborare cu conceptul funcțional pentru CSIRT-urile naționale, oferit de Directiva NIS2 (care de altfel este transpusă parțial în proiectul de lege), ne permite identificarea cu precizie înaltă locul și forma de organizare juridică a viitoarei autorități competente și anume de autoritate administrativă subordonată ministerului responsabil de realizarea politicii statului în domeniul securității cibernetice (actualmente Ministerul Dezvoltării Economice și Digitalizării). O opțiune alternativă ar fi crearea unei autorități administrative centrale. Acestea însă, prin prisma prevederilor legii menționate, sunt cvasi-ministere care urmează să se supună acelorași reguli de delimitare a

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				funcțiilor. În consecință această opțiune ar presupune crearea a cel puțin 2 entități: - unei autorități administrative centrale care va elabora monitoriza și evalua implementarea politicilor în domeniul securității cibernetice, și - în subordinea acesteia a unei autorități administrative (ex. agenție) care va exercita în principal funcțiile de supraveghere și control și de CSIRT național. Având în vedere doar cheltuielile pentru realizarea funcțiilor de suport și cele de conducere examinarea unei astfel de opțiuni se prezintă a fi lipsită de utilitate. În concluzie, atât în proiectul de lege, cât și în documentele de suport al acestuia, în mod special în analiza de impact, s-a propus un model centralizat de configurare a cadrului instituțional în domeniul securității cibernetice, în locul unui descentralizat. Alegerea acestei opțiuni s-a bazat pe recomandările raportului de evaluare privind modelul de guvernanță în domeniul securității cibernetice în Republica Moldova, întocmit de experți europeni în cadrul Proiectului „Asistență rapidă Republicii Moldova în domeniul securității cibernetice”. Modelele centralizate se caracterizează în principal printr-o singură autoritate competentă dedicată tuturor sectoarelor și o legislație cadru cuprinzătoare, iar cel descentralizat prin subsidiaritate, adică autorități competente dedicate fiecărui sector, cooperare din acestea și legislație sectorială specifică. Referitor la funcția de punct unic de contact, menționăm că atribuirea acesteia autorității competente se bazează pe prevederile art. 8 alin. (3) din Directiva NIS2, conform căruia în cazul în care un stat membru desemnează sau instituie o singură autoritate competentă), autoritatea competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
		8)	**5.**Având în vedere prevederile art. 12 alin. (2) din Directiva NIS 2.0 se propune modificarea textului art. 10 alin. (2) în felul următor: „Accesul la registru este limitat, însă la solicitare, datele din registru privind incidentele cibernetice sunt accesibile, părților interesate.	**Nu se acceptă.** Art. 12 alin. (2) din Directiva NIS2 reglementează aspecte ce țin de instituirea și administrarea de către Agenția Europeană pentru Securitate Cibernetică a unei baze de date la nivel european privind vulnerabilitățile. Această prevedere nu are incidență asupra instituirii sau reglementării modului de administrare a unor soluții tehnice în activitatea Statelor membre., Cu atât mai mult această prevedere nu poate constitui obiect al transpunerii în legislația națională. De asemenea, ținem să relevăm că art. 10 din proiectul de lege reglementează la nivelul normelor legale primare organizarea și funcționarea Registrului de stat al incidentelor de securitate cibernetică. Conceptul acestui Registru de stat a fost deja aprobat prin Hotărârea Guvernului nr. 388/2022. Deși acesta abordează problematica instituirii unei platforme dedicate doar la nivel guvernamental, adoptarea și publicarea unei legi cadru în domeniul securității cibernetice va constitui temei pentru revizuirea întregului cadru normativ guvernamental inclusiv cadrul normativ ce vizează nemijlocit acest Registru de stat, în mod special în partea ce ține de extinderea funcționalităților acestuia în corespundere cu mecanismele la nivel național instituite prin Legea privind securitatea cibernetică.
		9)	**6**.La fel, consideră că alin. (1) al art. 10 urmează a fi completat fiind indicat clar și detaliat ce informații anume va conține acest registru: a) informații ce descriu vulnerabilitatea.	**Nu se acceptă.** La nivel juridic-normativ primar prevederile alineatului (1) al art.10 stabilesc suficiente limite discreționare pentru Guvern în contextul exercitării prerogativelor sale legale (art. 22 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat) în vederea instituirii, elaborării și dezvoltării acestui Registru de stat.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			b) produsele TIC sau serviciile TIC afectate şi severitatea vulnerabilităţii în sensul circumstanţelor în care vulnerabilitatea poate fi exploatată; c) disponibilitatea unor măsuri corective a vulnerabilităţii şi, în lipsa unor măsuri corective disponibile, orientări oferite de autoritatea competentă adresate utilizatorilor de produse TIC și servicii TIC vulnerabile cu privire la modul în care pot fi atenuate riscurile rezultate din vulnerabilitățile divulgate.	De asemenea menționăm că prin Hotărârea Guvernului nr. 388/2022 a fost aprobat Conceptul „Sistemului informațional Registrul de stat al incidentelor de securitate cibernetică”. Odată cu intrarea în vigoare a legii acest registru ar trebui să fie deja funcțional, astfel încât Autoritatea competentă și CSIRT național să dispună de un instrumentar tehnic adecvat pentru realizarea atribuțiilor funcționale.
		10)	**7.**La art. 11, alin. 2, lit. b) la sintagma “- politici și proceduri privind utilizarea criptografiei și a criptării”, se propune de adăugat la sfârșit expresia “în special a criptării de la un capăt la altul”, conform recit. 98 din Directiva NIS 2.0.	**Se acceptă.** Prevederea a fost completată corespunzător.
		11)	**8**.La art. 12 alin. (4), definiția noțiunii de incident cibernetic cu impact semnificativ este mult mai larga decât cea din Directiva NIS2, in special cea cuprinsa la lit. b) și c): b) din cauza incidentului cibernetic prestarea serviciului este întreruptă pentru o perioadă mai mare decât perioada maximă de timp permisă pentru întrerupere, prevăzută în acordul corespunzător privind nivelul agreat al serviciilor, stabilit în cadrul relațiilor contractuale ale furnizorului de servicii, c) continuitatea serviciului unui terț este perturbată de incidentul cibernetic; Articolul 23 din Directiva NIS2 preve ca un incident este considerat semnificativ dacă: (a) a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare grave pentru entitatea în cauză; (b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile.	**Se acceptă parțial.** Alin. (5) de la art. 12 a fost revizuit. Totodată ținem să relevăm că Directiva NIS2 stabilește la articolul respectiv criterii minime, dar în același timp neexhaustive, în conformitate cu care anumite incidente urmează a fi calificate ca fiind semnificative. Prevederile legislațiilor naționale trebuie să vină cu soluții practice cum aceste criterii pot fi implementare în cadrul normativ și respectiv identificate la mod practic. De asemenea, pentru a concepe practica de raportare, în activitatea de aplicare a prevederilor legii în ce privește gestionarea incidentelor, ar trebui racordată, ajustată și îmbunătățită continuu, aplicând atât ghidurile și orientările metodologice naționale (adoptate de către autoritatea competentă, în conformitate cu art. 7 alin. (3) lit. b) din proiectul de lege), cât și cele internaționale.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			Întreruperea serviciului pe o perioadă mai mare decât cea prevăzută în acordul corespunzător privind nivelul agreat al serviciilor pentru un singur client sau chiar mai mulţi clienţi ori perturbarea scurtă a serviciului unui terţ nu produce, de regulă, prejudicii considerabile. În plus, sintagma prejudicii considerabile din Directiva nu se refera la un terţ individual, ci per ansamblu, deoarece semnificaţia unui terţ pentru economie sau societate poate fi prea mica ca să justifice angajarea resurselor statului şi furnizorului de servicii destinate tratării incidentelor cibernetice cu impact semnificativ. Astfel, se propune înlocuirea textului menţionat mai sus de la lit. b-d) din lege cu textul corespondent din directiva.	
		12)	**9.** La art. 12 alin. (5), lit. a) pare să dubleze lit. b). Articolul 23 din Directiva NIS2 prevede doar obligatia prevăzuta la lit. b).	**Se acceptă.** Eroarea tehnico-redacțională a fost eliminată. Actuala redacție a acestui alineat este următoarea: *(5) Furnizorul de servicii este obligat să informeze fără întârzieri nejustificate, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre o amenințare cibernetică semnificativă, destinatarii serviciilor pe care le prestează, care ar putea fi afectați de o astfel de amenințare, privind măsurile, inclusiv de ordin corectiv, pe care aceștia le-ar putea lua pentru a evita materializarea amenințării respective. În cazul în care, furnizorul de servicii este în imposibilitate de a identifica și notifica în mod individual destinatarii potențial afectați, acesta informează publicul. În cazul în care constată că materializarea amenințării cibernetice semnificative este iminentă, furnizorul de servicii informează destinatarii serviciilor sale despre amenințarea cibernetică semnificativă propriu-zisă.*
		13)	In plus, daca furnizorul nu notifica destinatarii, autoritatea competenta trebuie sa poată sa ceara furnizorului de servicii sa	**Se acceptă.** Alin. (6) a fost revizuit, rezultând următoarea redacție:

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			facă acest lucru, înainte de a notifica destinatarii de sine stătător.	*(6) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (5) în termenul respectiv, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de notificare a destinatarilor posibil afectați sau publicul, informând despre aceasta furnizorul de servicii. Modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiect de reglementare a actului normativ prevăzut de alin (8).*
		14)	**10.**De asemenea, ar fi util de completat art. 12 cu o norma similara cu cea prevăzută la art. 23 alin. (5) din Directiva NIS2: Echipa CSIRT sau autoritatea competentă furnizează, fără întârzieri nejustificate și, atunci când este posibil, în termen de 24 de ore de la primirea alertei timpurii menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incidentul semnificativ și, la cererea entității, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care echipa CSIRT nu este destinatarul inițial al notificării menționate la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu echipa CSIRT. Echipa CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, echipa CSIRT sau autoritatea competentă furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii.	**Se acceptă.** Articolul 12 a fost completat cu alineatul (2) cu următorul cuprins: *Autoritatea competentă prezintă, fără întârzieri nejustificate însă nu mai târziu de 24 de ore de la primirea informației menționate la alineatul (1), furnizorului de servicii un răspuns, inițial cu privire la incidentul semnificativ și, dacă furnizorul de servicii solicită, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare impactului incidentului cibernetic*
		15)	**11.La art. 12 se propune de adăugat următoarele aliniate:** a) conform recit. 92 din Directiva NIS 2.0, cu următorul text: "*Pentru a raționaliza obligațiile impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de*	**Nu se acceptă.** Completarea respectivă ar depăși obiectul de reglementare al proiectului de lege. Chestiunile invocate de autorul

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			comunicații electronice accesibile publicului și prestatorilor de servicii de încredere în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, normele privind impunerea cerinţelor de securitate şi de notificare asupra entittăţilor respective prevăzute de Legea nr. 124 din 19.05.2022 privind identificarea electronică şi serviciile de încredere și Legea comunicațiilor electronice nr. 241 din 15.11.2007 nu se aplică entităţilor care cad sub incidenţa prezentei legi, iar normele privind obligațiile de raportare prevăzute în prezenta lege nu aduc atingere nici Legii nr. 124 din 19.05.2022 privind identificarea electronică şi serviciile de încredere și nici Legii comunicaţiilor electronice nr. 241 din 15.11.2007." b) conform recit. 108 și art. 31, alin. 3 din Directiva NIS 2.0, cu următorul text: "*În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritatea competenta va coopera și va face schimb de informații cu privire la toate aspectele relevante cu autoritățile de supraveghere menționate în legea privind protecţia datelor cu caracter personal și Legea nr. 241 din 15.11.2007 privind comunicațiilor electronice."* *c)* conform recit. 51 din Directiva NIS 2.0, cu următorul text: "*Utilizarea oricărei tehnologii inovatoare, inclusiv a inteligenței artificiale, a cărei utilizare ar putea îmbunătăți detectarea și prevenirea atacurilor cibernetice, permițând alocarea resurselor către prevenirea şi combaterea atacurilor cibernetice într-un mod mai eficace, nu ar trebui să interfereze în mod nejustificat cu drepturile și libertățile persoanelor. Primul pas pentru evitarea sau atenuarea acestor riscuri este aplicarea cerințelor privind protecției datelor cu caracter personal începând cu momentul conceperii și în mod implicit, care va contribui la integrarea garanțiilor adecvate, cum ar fi criptarea, acuratețea datelor, minimizarea datelor, echitatea,*	obiecției intră în sfera de reglementare a actelor normative invocate în propunere. Totodată pentru punerea în aplicare a prevederilor legii în speță, în cel mai scurt timp va fi inițiată elaborarea proiectului de lege pentru modificarea unor acte normative în vederea aducerii acestora în concordanță cu prevederile proiectului. În acest context, dacă va fi cazul va fi examinată și oportunitatea completării legislației cu propunerile respective.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			transparenţa şi securitatea datelor în proiectarea şi utilizarea acestor tehnologii și sisteme." d) *"În cazul externalizării parțiale sau a întregii activități de securitate cibernetică către furnizori externi de servicii, trebuie să fie în deplină conformitate cu legea privind protecţia datelor cu caracter personal."* e) "*Întru realizarea unei sinergii pozitive, funcționarii responsabili cu securitatea cibernetică au obligația de a coopera îndeaproape cu responsabilul cu protecția datelor desemnat în conformitate cu legea privind protecţia datelor cu caracter personal atunci când se ocupă de activități care se suprapun".*	
		16)	**12.**La art. 15 se propune de adăugat un aliniat adițional, după alin. 4, conform recit. 45 din Directiva NIS 2.0, cu următorul text: "*Prin urmare, autoritatea competentă ar trebui să poată face schimb de informații, inclusiv de date cu caracter personal, în țări terțe conform alin. 4 de mai sus, în condițiile prevăzute de capitolul 7 din Legea privind protecţia datelor cu caracter personal pentru transferurile de date cu caracter personal către țări terțe*."	**Nu se acceptă.** Proiectul de lege cuprinde deja prevederi suficiente pentru asigurarea temeiului juridic pentru autoritatea competentă de a face schimb de informații, precum și interconexiunile necesare cu legislația privind protecția datelor cu caracter personal.
		17)	**13**.La art. 17, ar fi util de inlocuit sintagma *"amenintare grava"* si *"perturbare grava"* cu termenul *"amenintare cibernetica semnificativa*", care este definit in lege.	**Se acceptă.** Alin. (3) a fost revizuit, rezultând următoarea redacție: *„(3) Pentru contracararea unei amenințări cibernetice semnificative imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea sau atenuarea consecințelor unui incident cibernetic semnificativ, autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții:...".*
		18)	**14.**Totodată se propune excluderea prevederilor art. 17 alin. (3) din proiectul Legii privind securitatea cibernetică, or posibilitatea acordată autorității competente de a restricționa	**Nu se acceptă.**

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			utilizarea sau accesul la un sistem informatic reprezintă o ingerință în activitatea furnizorilor de rețele și/sau servicii de comunicaţii electronice, astfel această prevedere ar acționa în detrimentul furnizorilor.	Această măsură este una care urmează a fi aplicată doar în anumite situații pentru a împiedica răspândirea consecințelor unui incident cu impact semnificativ. Autoritatea competentă trebui să dispună de pârghiile necesare pentru a asigura respectarea interesului public. Lăsarea doar la latitudinea furnizorilor de servicii acest aspect, ar putea periclita interesul public în detrimentul intereselor private ale furnizorului de servicii.
		19)	**15**.La art. 18 alin. (3), este necesar de precizat daca accesul la informatii al autoritatii competente nu presupune și acces liber la datele cu caracter personal, în special date protejate prin secretul comunicaţiilor.	**Nu se acceptă.** O astfel de precizare este de prisos. Autoritatea competentă în exercitarea prerogativelor de putere publică poate și trebuie să aibă acces la date, art. 20 alin.(1) din proiectul de lege este elocvent în acest sens.
		20)	**16.**La art. 18 alin. (4), se propune de a complete cu sintagma "și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi". Simpla sesizare din partea unui terţ nu trebuie să servească temei pentru control, mai ales dacă aceasta nu conţine nicio probă care ar justificva o bănuială rezonabilă că ar exista o încălcare.	**Precizare.** Proiectul de lege anume aceasta și prevede la lit. b) alin.(4) art. 19 din proiectul de lege.
		21)	**17**.La art. 18 alin. (5), nu este clar dacă procedura de control va înlocui sau completa procedura generala stabilită de Legea nr. 131/2012.	**Se acceptă.** Art. 18 alin. (1) a fost completat cu o normă generală de trimitere la Legea nr. 131/2012 privind controlul de stat a activității de întreprinzător. Prin urmare, în exercitarea funcției sale de control, discreția autorității competente urmează să fie limitată de normele legii respective. De asemenea, cadrul normativ guvernamental, care urmează să fie aprobat în temeiul alin. (3) al art. 18 din proiectul de lege, trebuie să detalieze procedura de control însă bineînțeles în limitele stabilite de normale juridice cuprinse în Legea nr. 131/2012.
		22)	**18.**La art. 19 se propune de adăugat următorul aliniat, conform art. 35, alin. 2 din Directiva NIS 2.0, cu textul: "În cazul în care	**Se acceptă parțial.**

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			Centrului Național pentru Protecția Datelor cu Caracter Personal aplică o amendă administrativă, autoritatea competenta nu aplică o amendă administrativă pentru o încălcare menționată la aliniatul (1) din prezentul articol rezultată în urma aceluiași comportament care a făcut obiectul amenzii administrative. Cu toate acestea, autoritatea competenta poate aplica măsurile de asigurare a respectării prezentei legi." **a.** Tot aici se propune de adăugat un aliniat, conform recit. 14 și art. 2, alin. 14 din Directiva NIS 2.0, cu următorul text: "Dreptul privind protecția datelor și dreptul privind protejarea confidențialității se aplică oricărei forme de prelucrare a datelor cu caracter personal în temeiul prezentei legi. În special, prezenta lege nu aduce atingere Legii privind protecţia datelor cu caracter personal și Legii nr. 241 din 15.11.2007 privind comunicaţiilor electronice. Prin urmare, prezenta lege nu aduce atingere, printre altele, sarcinilor și competențelor Centrului Naţional pentru Protecţia Datelor cu Caracter Personal și Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei. Furnizorii de servicii, autoritatea competenta, Centrul guvernamental de răspuns la incidentele de securitate cibernetică prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentei legi și în conformitate cu legea privind protecţia datelor cu caracter personal; în special această prelucrare se bazează pe articolul 5 din respectiva lege. Prelucrarea datelor cu caracter personal în temeiul prezentei legi de către furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului se efectuează în conformitate cu legea."	Articolul 19, devenit articolul 20, a fost completat cu alineatul (1) cu următorul cuprins: „(1) În exercitarea competenței cu care este învestită prin prezenta lege autoritatea competentă prelucrează date cu caracter personal în condițiile stabilite de legislația în acest domeniu." Celelalte propuneri nu pot fi acceptate deoarece vor dubla prevederile legislației privind protecția datelor cu caracter personal. De asemenea propunerile respective vor avea ca efect încălcarea principiilor activității de legiferare, stabilite de Legea nr. 100/2017 privind actele normative, precum și a normelor de tehnică legislativă
		23)	**b.** Tot aici se propune de adăugat un aliniat, conform recit. 136 din Directiva NIS 2.0, cu următorul text: "Prezenta lege ar trebui să stabilească norme de cooperare între autoritatea	**Nu se acceptă.** Proiectul deja prevede la art. 7 alin. (1) lit. d) interacțiunea în domeniul securității cibernetice cu autoritățile și

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			competenta și autoritatea de supraveghere în conformitate cu legea privind protecția datelor cu caracter personal pentru tratarea cazurilor de încălcare a prezentei legi în materie de date cu caracter personal.”	instituțiile publice naționale și cu furnizorii de servicii, inclusiv autoritatea de supraveghere în conformitate cu legea privind protecția datelor cu caracter personal
		24)	**19.** La art. 20 alin. (3), personalul furnizorilor de servicii care interacționează cu autoritatea competentă în condițiile prezentei legi, nu ar trebui să poarte răspundere personală, în conformitate cu legislația, pentru neîndeplinirea atribuțiilor funcționale stabilite de actele normative. Această răspundere o poartă furnizorii de servicii, în baza alin. (3).	**Se acceptă.** Alineatul a fost exclus.
		25)	**20**.La art. 21 alin. 1, se propune extinderea termenului de aplicare, nu peste 1 an, ci 21 de luni de la intrarea în vigoare, conform Directivei NIS 2.0.	**Se acceptă.** Termenul de intrare al legii a fost modificat în 1 ianuarie 2025.
		26)	**21**.Se propune operarea modificărilor și completarea proiectului de lege cu prevederi legale ce țin de: - Desemnarea delimitată a unei autorități competente responsabile de securitatea cibernetică ce va avea sarcini de supraveghere a respectării legislației în domeniul securității cibernetice. - Instituirea aparte a unui punct punct național unic de contact. - Și desemnarea sau instituirea aparte a unei echipe de răspuns la incidentele cibernetice de nivel național. - Introducerea în conținutul proiectului de lege a articolelor ce vor conține prevederi privind activitatea și atribuțiile aparte a fiecărei autorități, punct sau echipe de răspuns desemnate.	**Nu se acceptă.** Prevederile proiectului de lege care abordează cadrul instituțional în domeniul securității cibernetice este reprezentat în principal de articolele 6 și 7. Potrivit art. 7 alin. (1) Guvernului i se deleagă atribuția de a desemna o autoritate competentă în domeniul securității cibernetice și să stabilească modul de organizare și funcționare a acesteia. Din perspectivă instituțională, conceptul propus în proiect, ca Guvernul să decidă desemnarea autorității competente în domeniul securității cibernetice se înscrie în spectrul exercitării de către Guvern a prerogativelor sale în stabilirea modului de organizare și funcționare a persoanelor juridice de drept public din structura guvernamentală. Astfel, potrivit prevederilor art. 6 literele b), d) și e) din Legea nr. 136/2017 cu privire la Guvern, Guvernul este împuternicit să constituie în structura sa atât autorități administrative centrale, cât și structuri organizaționale în sfera de competență a acestora și cea a ministerelor, precum

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				și să le reglementeze modul de organizare și funcționare. Bineînțeles această marjă discreționară acordată de către Parlament Guvernului este limitată, pe de o parte de obiectivele strategice ce urmează a fi realizate și de necesitatea asigurării eficienței și eficacității activității administrative, iar pe de alta de normele legale primare care reglementează administrația publică centrală de specialitate. Modul de organizare și funcționare a persoanelor juridice de drept public în structura Guvernului este stabilit de Legea nr. 98/2014 privind administrația publică centrală de specialitate. Conform proiectului autoritatea competentă în domeniul securității cibernetice, de rând cu funcțiile de echipă de răspuns la incidentele cibernetice la nivel național și de punct național unic de contact urmează să exercite și funcția de supraveghere și control a modului de realizare a obligațiilor stabilite de lege de către furnizorii de servicii, precum și alte atribuții care vizează implementarea politicii statului în domeniul securității cibernetice. Prevederile respective ale proiectului de lege în coroborare cu prevederile art. 4 pct. 1) lit. b), ale art. 14 alin. (5) și ale art. 25 alin. (2) lit. c) ne permit să identificăm forma juridică de organizare a viitoarei autorități competente și anume de autoritate administrativă subordonată unui minister sau unei autorități administrative centrale. Această opțiune specifică în exercitarea de către Guvern a acestei prerogative ar putea fi revăzută la discreția Guvernului, în limitele expuse mai sus, în funcție de evoluția situației atât la nivelul activității administrative guvernamentale, cât și la nivelul sectorului specific asigurării securității cibernetice.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				Din perspectiva delimitării funcțiilor în interiorul structurii unui minister menționăm că un minister (o autoritate administrativă centrală) nu trebuie confundat cu aparatul central al acestuia care, potrivit prevederilor art.30 din Legea nr. 98/2012 este responsabil de elaborarea, elaborarea, monitorizarea și evaluarea politicilor publice în domeniile de activitate ale acestuia, pe când realizarea celorlalte funcții prevăzute de art. 25 din Legea nr. 98/2014 (supraveghere și control, prestare de servicii publice, alte funcții de implementare), în vederea respectării unui principiu fundamental în organizarea și funcționarea administrației publice delimitarea funcțiilor de elaborare a politicilor de cele de implementare, urmează a fi atribuite unor autorități administrative subordonate ministerului responsabil de realizarea politicii respective. Aceste autorități administrative sunt prin excelență instrumente instituționale ale unui minister în procesul de implementare a politicii de stat. Actualmente realizarea politicii de stat în domeniul securității cibernetice este prerogativa Ministerului Dezvoltării Economice și Digitalizării. Prin urmare, în temeiul cadrului normativ enunțat mai sus în coroborare cu conceptul funcțional pentru CSIRT-urile naționale, oferit de Directiva NIS2 (care de altfel este transpusă parțial în proiectul de lege), ne permite identificarea cu precizie înaltă locul și forma de organizare juridică a viitoarei autorități competente și anume de autoritate administrativă subordonată ministerului responsabil de realizarea politicii statului în domeniul securității cibernetice (actualmente Ministerul Dezvoltării Economice și Digitalizării). O opțiune alternativă ar fi crearea unei autorități administrative centrale. Acestea însă, prin prisma prevederilor legii menționate, sunt cvasi-ministere care

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				urmează să se supună acelorași reguli de delimitare a funcțiilor. În consecință această opțiune ar presupune crearea a cel puțin 2 entități: - unei autorități administrative centrale care va elabora monitoriza și evalua implementarea politicilor în domeniul securității cibernetice, și - în subordinea acesteia a unei autorități administrative (ex. agenție) care va exercita în principal funcțiile de supraveghere și control și de CSIRT național. Având în vedere doar cheltuielile pentru realizarea funcțiilor de suport și cele de conducere examinarea unei astfel de opțiuni se prezintă a fi lipsită de utilitate. În concluzie, atât în proiectul de lege, cât și în documentele de suport al acestuia, în mod special în analiza de impact, s-a propus un model centralizat de configurare a cadrului instituțional în domeniul securității cibernetice, în locul unui descentralizat. Alegerea acestei opțiuni s-a bazat pe recomandările raportului de evaluare privind modelul de guvernanță în domeniul securității cibernetice în Republica Moldova, întocmit de experți europeni în cadrul Proiectului „Asistență rapidă Republicii Moldova în domeniul securității cibernetice”. Modelele centralizate se caracterizează în principal printr-o singură autoritate competentă dedicată tuturor sectoarelor și o legislație cadru cuprinzătoare, iar cel descentralizat prin subsidiaritate, adică autorități competente dedicate fiecărui sector, cooperare din acestea și legislație sectorială specifică. Referitor la funcția de punct unic de contact, menționăm că atribuirea acesteia autorității competente se bazează pe prevederile art. 8 alin. (3) din Directiva NIS2, conform căruia în cazul în care un stat membru desemnează sau instituie o singură autoritate competentă), autoritatea

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
				competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.
		27)	**22**. Se propune completarea art. 5 cu următoarele principii: *Principiul confidențialității*- în procesul de asigurare a securității cibernetice, persoanele responsabile urmează a se conduce și de prevederile legale ce țin de protecția datelor cu caracter personal și secret comercial.	**Nu se acceptă.** Aceste principii nu intră în obiectul de reglementare al proiectului de lege sunt principii generale caracteristice unor alte ramuri sau legi sectoriale, cum ar fi legislația contravențională, fiscală, privind controlul de stat al activității de întreprinzător, etc.
		28)	**23**. Având în vedere faptul că, de către Guvern va fi constituită sau desemnată o singură autoritate competentă ce va exercita funcții de punct național unic de contact și echipă de răspuns la incidentele la nivel național, considerăm oportun completarea proiectul de lege cu preveri legale referitore la delimitarea atribuțiilor autorității competente și anume cele de supraveghere și control, de atribuțiile de soluționare a incidentelor și acordarea asistenței necesare furnizorilor de servicii, persoanelor fizice sau juridice ce ar comunica careva vulnerabilități sau incidente cibernetice. În susținerea poziției expuse propunem ca art. 20 să fie completat cu un alineat nou: „autoritatea competentă urmează să acorde furnizorilor de servicii de comunicații electronice careva garanții ca în procesul divulgării incidentelor cibernetice sau a vulnerabilităților vor beneficia de asistența necesară și nu vor fi penalizați nemotivat, inițial din momentul divulgării, în conformitate cu principiul prezumției nevinovăției. ”	**Nu se acceptă.** Vedeți comentariul de la pct. 26) al prezentei sinteze
		29)	**24**. Reieșind din prevederile art. 20 din proiectul Legii privind securitatea cibernetică ce indică: „Autoritatea competentă constată contravențiile în domeniul securității cibernetice și întocmește procesele verbale corespunzătoare, examinează cauzele contravenționale și aplică sancțiunile contravenționale în conformitate cu prevederile Codului contravențional”,	**Se acceptă.** Art. 18 alin. (1) a fost revizuit corespunzător.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			considerăm oportun a completa proiectul legii cu referințe la Legea cu privire la controlul de stat asupra activității de întreprinzător și prevederi ce se referă la procesele-verbale întocmite de autoritatea competentă în domeniul securității cibernetice, conținutul acestora, cât și modul de contestare.	
		30)	Finalmente punctăm importanța finalizării pachetului final al proiectului de lege, care să includă cadrul legislativ aferent, oferind astfel vizibilitate asupra sectoarelor care cad sub incidența legii, detalii despre sancțiunile potențiale dar și alte obligații suplimentare pentru sectorul privat.	**Precizare**. Elaborarea proiectului de lege pentru modificarea unor acte normative urmează a fi demarată în cel mai scurt timp, după finalizarea definitivării pachetului de documente privind proiectului de lege privind securitatea cibernetică. De asemenea, în prealabil elaborării textului acestui proiect de lege urmează a fi realizată o identificare preliminară a furnizorilor de servicii, ceea ce va contribui la colectarea unor informații primare suplimentare necesare elaborării unor modificări și completări la legislația în vigoare strict necesare și suficiente pentru a putea pune în aplicare prevederile Legii privind securitatea cibernetică. În același context ținem să relevăm că adoptarea cadrului normativ de punere în aplicare a prevederilor proiectului de lege este doar una dintre măsurile de implementare ale acestuia. Odată cu publicarea Directivei NIS2 a fost publicată și Directiva CER (reziliența entităților critice). Aceste două acte sunt în interconexiune din perspectiva tangențelor domeniilor de aplicare ale acestora. La mod concret statele membre trebuie să se asigure, printre altele, că autoritățile lor competente în temeiul Directivei CER notifică autoritățile competente în temeiul NISD 2 cu privire la entitățile critice pe care le-au identificat. Ca regulă, pentru a asigura alinierea între cele două instrumente, toate entitățile critice identificate în temeiul Directivei privind reziliența entităților critice vor face obiectul obligațiilor de reziliență cibernetică în temeiul NIS2.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
5.	**Asociația Națională a Companiilor din sectorul TIC** nr. 553 din 01.02.2023	***31)***	1. completarea art. 5 cu următoarele principii: - *Principiul neadmiterii penalizării duble* - asigurarea unui șir de garanții pentru furnizorii serviciilor de comunicații electronice, în vederea evitării sancționării duble a acestora de către autorități diferite. În cazul concurenței normelor care prevăd diferite penalități, corect ar fi, să se aplice penalitatea cea mai mică. Or, ar putea apărea situații în care raportarea incidentelor cibernetice ar putea fi privită de diferite autorități și calificată drept încălcare a legislației, prin prisma diferitor legi. (spre exemplu raportarea aceluiași incident cibernetic atât în viziunea autorității competente de securitatea cibernetică, cât și a CNPDCP). - *Principiul evitării contrapunerii funcțiilor de control a mai multor autorități* – ce prevede modalitatea de delimitare a funcțiilor de control de către diferite autorități. Or, în cazul inițierii unui control de către o autoritate competentă asupra raportarii unui anumit incident cibernetic, să decadă automat necesitatea inițierii controlului asupra aceleiași raportări și aceluiași incident cibernetic de către o altă autoritate. - *Principiul caracterului consultativ al controlului* - prevenirea încălcării legislaţiei prin aspectul consultativ al controlului. Acest principiu, are drept scop aplicarea corectă a legislației în domeniul securității cibernetice, precum și executarea corectă a procedurii de raportare a incidentelor cibernetică. Astfel Autoritatea competentă în domeniul asigurării securității cibernetice ar avea obligația acordării suportului consultativ furnizorilor de servicii de comunicații electronice și în general întreprinderilor ce cad sub incidența Legii privind securitatea cibernetică.	**Se acceptă parțial.** Aceste principii nu intră în obiectul de reglementare al proiectului de lege sunt principii generale caracteristice unor alte ramuri sau legi sectoriale, cum ar fi legislația contravențională, fiscală, privind controlul de stat al activității de întreprinzător, etc. Totuși în art. dedicat controlul al proiectului de lege au fost înserată o normă de trimitere la Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. De asemenea în proiectul de lege privind modificarea unor acte normative care va avea ca scop aducerea legislației în concordanță cu prevederile proiectului, vor fi incluse norme care vor asigura interconexiunea cu prevederile proiectului de lege și vor asigura baza legală suficientă pentru exercitarea de către autoritatea competentă a atribuțiilor sale legale.
		32)	2. Se propune completarea art. 12 din proiectul Legii privind securitatea cibernetică cu prevederi legale ce țin de modalitatea notificării incidentelor cibernetice către autoritatea competentă și anume se propune introducerea modalității de raportare (notificare) electronică sau prin intermediul unui ghișeu unic de notificare a incidentelor cibernetice ce ar exclude necesitatea raportării multiple către diferite autorități ce au tangență directă	**Nu se acceptă.** Prevederile articolului respectiv stabilesc norme materiale și procedura privind obligațiile de notificare. Metodele și modalitățile de implementare sau de operare a subiecților legii în procesul realizării acestor obligațiuni urmează a constitui obiectul unor activități normative, tehnice și

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			cu monitorizarea incidentelor cibernetice și a altor situații ce derivă din aceste incidente cibernetice. Această modalitate de raportare prin intermediul unei căi unice ar constitui rezultatul bunei colaborări între mai multe autorități investite cu atribuții de control.	operaționale ulterioare, desfășurate de autoritatea competentă în comun cu furnizorii de servicii în procesul de realizare a obligațiunilor respective. În același context atragem atenția că proiectul de lege cuprinde prevederi care vizează chestiunea implementării în activitatea autorității competente, inclusiv în raport cu furnizorii de servicii. Astfel art. 10 stabilește expres necesitatea instituirii și implementării unui Registru de stat al incidentelor de securitate cibernetică și a sistemului informațional care îl formează. Conceptul acestui sistem a fost deja aprobat prin Hotărârea Guvernului nr. 388/2022. Bineînțeles, că acest concept urmează a fi analizat după publicarea proiectului de lege din perspectiva aducerii acestuia în concordanță cu prevederile legii. De asemenea, una din atribuțiile de bază ale autorității competente, stabilită de art. 7 alin. (4) punctul 9) constă în implementarea în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate.
		33)	3. Se propune completarea art. 18 alin. (1) lit. b), după cuvântul lege să fie completată cu cuvintele *„în calitate de măsuri excepționale în cazul ineficienței suportului consultativ oferit de către autoritatea competentă”*, iar la lit e), după cuvântul „controlului” să fie completat cu cuvintele *„și acordarea unui termen rezonabil în vederea remedierii încălcărilor constatate”* – această completare ar confirma caracterul prietenos al legislației, ce nu urmărește drept scop sancționarea sistematică și abuzivă a furnizorilor de servicii.	**Se acceptă parțial.** Articolul 18, devenit articolul 19, a fost revizuit. În mod special atragem atenția asupra faptului că potrivit revizuirilor controlul urmează a fi efectuat în conformitate cu prevederile Legii nr. 131/2012 cu privire la controlul de stat a activității de întreprinzător.
		34)	5.Se propune completarea art. 20 din proiectul legii cu un nou aliniat ce ar indica că, în cazul în care prin prisma prevederilor mai multor legi se prezumă aplicarea sancțiunilor diferite și în cuantum diferit, urmează a fi aplicată sancțiunea mai blândă, în vederea evitării înrăutățirii situației furnizorului de servicii ce a	**Nu se acceptă.** Completarea respectivă ar depăși obiectul de reglementare al proiectului de lege. Chestiunile invocate de autorul obiecției intră în sfera de reglementare a actelor normative

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			notificat incidentul cibernetic. Totodată, articolul respectiv urmează a fi completat cu prevederi ce țin de aplicarea principiului de clemență asupra furnizorilor de servicii fiind pasibili de răspundere, având în vedere faptul că, ultimii au contribuit activ la înlăturarea incidentului cibernetic.	care stabilesc norme materiale și procedurale privind categoriile corespunzătoare de răspunderi. Totodată pentru punerea în aplicare a prevederilor legii în speță, în cel mai scurt timp va fi inițiată elaborarea proiectului de lege pentru modificarea unor acte normative în vederea aducerii acestora în concordanță cu prevederile proiectului. În acest context, dacă va fi cazul va fi examinată și oportunitatea completării legislației cu propunerile respective.
		35)	5. Având în vedere că, art. 15 al proiectului de lege prevede un șir de obligații a furnizorului de servicii în procesul de notificare a incidentelor cibernetice, se propune completarea proiectului de lege cu un articol aparte ce ar prevedea un șir de drepturi pe care le-ar deține furnizorul de servicii pe parcursul procesului de notificare.	**Nu se acceptă.** Legea prevede obligațiile minime care trebuie îndeplinite de către furnizorii de servicii și de autoritatea competentă. Acestea însă nu anulează drepturile furnizorilor de servicii sau a autorității competente sau a altor autorități responsabile în procesul de implementare a legii, care le revin conform cadrului normativ.
		36)	Totodată, ar fi binevenită introducerea unui articol ce ar indica expres șirul de drepturi de care dispune autoritatea competentă în procesul de raportare și gestionare a incidentelor cibernetice. Aceste articole ar aduce o claritate și ar evidenția care este limita drepturilor pe care pe de o parte le deține autoritatea competentă, iar pe de altă parte furnizorii de servicii, acest fapt ar exclude posibilitatea apariției unor abuzuri în procesul raportării și gestionării incidentelor cibernetice, din partea oricărei părți vizate de incidente.	**Nu se acceptă.** Reglementarea competenței autorității competente în art. 7 este destul de vastă și nu necesită reiterarea unor drepturi separat cu riscul dublării prevederilor acestea, precum și a altor acte normative.
		37)	6. De adăugat la art.11, alin.2, lit. b) sintagma "având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile", iar în acest context la alin. 4 al aceluiași articol de adăugat la lit a) și lit. b) sintagma „și luând în considerare stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile."	**Nu se acceptă.** În principiu aceste măsuri sunt măsuri de securitate minime ce urmează a fi realizate de entități care furnizează servicii esențiale. Acestea sunt prevăzute de art. 21 alin. (2) din Directiva NIS2 și asigură o armonizare minimă a legislației naționale în conformitate cu art. 5 din această directivă.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			Argument: pentru a nu defini măsuri care ar presupune costuri exorbitante pentru furnizori, pe de o parte, și pentru a fi tehnologic neutru, pe de altă parte. Nici GDPR nu definește măsurile de securitate concrete, ci „adecvate" riscurilor. Trebuie să fie luate în considerare cu stadiul actual al tehnicii și costurile de implementare, precum și natura, domeniul de aplicare, contextul și scopul prelucrării informației. Adică, se reflectă atât abordarea bazată pe risc, cât și faptul că nu există o soluție de securitate a informațiilor „ one size fits all" (ce este „adecvat" pentru unii, ar putea să nu fie pentru alții, în dependență de propriile circumstanțe - în funcție de gradul de sofisticare al sistemelor, de utilizare și de expertiza tehnică a personalului, etc.).	
		38)	7. De completat cu următoarea sintagma "aderarea Furnizorului la un cod de conduită aprobat de autoritatea competenta, sau la un mecanism de certificare aprobat de autoritatea competenta, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la articolul 11", ceea ce ar minimiza interpretarea de neconformare a obligațiilor din articolul respectiv.	**Nu se acceptă.** Considerăm că indicarea unei modalități formale prin care să fie confirmată respectarea cerințelor nu asigură realizarea scopul normelor juridice respective și va avea efecte de neîndeplinire a acesteia în fapt.
		39)	8. La art. 12 înainte de termenul indicat în ore 24,72, de adăugat sintagma "dacă este posibil", căci nu în toate situațiile este posibil să detectezi, sau detaliile incidentului să nu fie întotdeauna disponibile în perioadă inițială și să raportezi în termen, luând în considerare și faptul că un furnizor trebuie să raporteze la mai multe entități. Eventual am putea adăuga și textul: "Atunci când notificarea nu se poate realiza în termenul stabilit, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere."	**Nu se acceptă.** Aceste prevederi transpun prevederi ale Directivei NIS2. Ținem să menționăm că aceste prevederi sunt o condiție esențială a procesului de gestionare a incidentelor la nivel național și asigură o transpunere minimă a prevederilor Directivei NIS2, în acord cu art. 5 al acesteia.
		40)	9. La art. 12, înainte de propunerea noastră prezentată anterior: „*Întru realizarea unei sinergii pozitive, funcționarii responsabili cu securitatea cibernetică au obligația de a coopera îndeaproape cu responsabilul cu protecția datelor desemnat în conformitate cu legea privind protecția datelor cu*	**Nu se acceptă.** Proiectul de lege conține suficiente și necesare prevederi care stabilesc obligația autorității competentă să coopereze atât cu autoritățile publice naționale, organizațiile

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			caracter personal atunci când se ocupă de activități care se suprapun”, făcând analogie la prevederile Legii nr. 133/2011, se propune completarea acestuia cu prevederi prin care atât furnizorii de servicii, cât și autoritățile publice să asigure desemnarea Funcției de responsabil de asigurare a securității cibernetice, acolo unde ar fi relevantă desemnarea acestuia.	internaționale și autoritățile statelor străine, cât și cu furnizorii de servicii, inclusiv cu cei privați.
6.	**S.A. „CET-Nord”** nr. 500-008/0104 din 26.01.2023		Lipsa de obiecții și propuneri.	
7.	**Ruslan Budeci** ruslanbudeci@gmail.com tel. 078300656	***41)***	Cu privire la discuția proiectului de Lege din domeniul securității cibernetice, în timpul ședinței au fost menționați și mai bine zis, confundați câțiva termeni cu care aș dori să ne clarificăm din start: Bug bounty - un program de recompense pentru descoperirea de vulnerabilități (cunoscute și sub denumirea de "bugs") - este un program prin care o organizație oferă recompense pentru descoperirea de vulnerabilități în software-ul sau sistemele sale. Acesta presupune că o companie încurajează și remunerează persoanele care descoperă vulnerabilități în software-ul sau sistemele sale. Divulgarea coordonată a vulnerabilităților – NU presupune neapărat că o companie oferă permisiunea de a sparge sistemele sale. Invers, ea permite companiei să lucreze împreună cu cercetătorii din securitate pentru a identifica și corecta vulnerabilitățile înainte ca acestea să fie folosite în mod necorespunzător sau să afecteze utilizatorii. Pe când la ședință, din păcate această noțiune, inclusiv utilizarea acestea, a fost puțin distorsionată. Aș vrea să menționez că divulgarea coordonată a vulnerabilităților nu este același proces ca și Bug Bounty.	**Precizare.** În cadrul ședinței dedicate consultării publice a proiectului de lege privind securitatea cibernetică, care a avut loc la data de 27 ianuarie curent, într-adevăr a fost abordată problematica mecanismelor existente și care ar putea fi aplicate și în țara noastră în ce privește descoperirea vulnerabilităților și întreprinderea măsurilor necesare pentru eliminarea sau cel puțin diminuarea potențialului de exploatare a acestora. Totuși, în cadrul sus numitei ședințe confuziile nu au vizat nemijlocit prevederile proiectului de lege, ci reieșind din discuțiile diferitor părți interesate participante, au vizat mai mult interpretarea prevederilor proiectului și aspecte ce vizează implementarea ulterioară a acestora, precum și unele practici implementate actualmente în context internațional. În mod special discuțiile s-au axat pe diferite tehnici existente și mecanisme de vizează divulgarea vulnerabilităților Procesul de divulgare coordonată a vulnerabilităților, în raport cu Directiva NIS este o instituție juridică abordată pentru prima dată în Directiva NIS2. Conform acesteia din urmă Statele membre ar trebui să ia măsuri pentru a înlesni divulgarea coordonată a vulnerabilităților prin stabilirea

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			Proiectul de Lege prevede divulgarea coordonată a vulnerabilităților, însă fără alte schimbări în cadrul legislativ actual, acest proces nu va fi eficient. Printre beneficiile finale, care necesită o abordare legislativă mai complexă, ar fi: - atragerea de hackeri neremunerați în scopuri benefice, pentru căutarea vulnerabilităților și lichidarea acestora înainte ca să fie identificate de atacatorii externi; - antrenarea tinerilor talente (de pe băncile școlii/colegiului/universității) ca să-și aplice cunoștințele și să-și testeze abilitățile din domeniul securității cibernetice în folosul comunității; - și bineînțeles identificarea tinerilor talente pentru recrutare timpurie. NOTĂ: Conform cercetării 'COORDINATED VULNERABILITY DISCLOSURE POLICIES IN THE EU' publicate de ENISA (European Union Agency for Cybersecurity) din aprilie 2022, ~85% din problemele pe partea de implementare revin barierelor legale și lipsei de cooperare dintre companii (documentul poate fi găsit aici: [https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu/@@download/fullReport] (https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu/@@download/fullReport)). De atras atenția că în documentul de mai sus se menționează și dificultățile prin care au trecut țările europene care au implementat astfel de proiecte, dar se menționează și anumite practici utile pentru a preveni aceste probleme. Deși pare neimportant, un astfel de proces poate aduce beneficii pentru comunitatea de cercetători din domeniul securității dacă este	unei politici naționale relevante. Ca parte a politicii lor naționale, statele membre ar trebui să își propună să facă față, în măsura posibilului, încercărilor cu care se confruntă cercetătorii în domeniul vulnerabilității, inclusiv expunerea potențială a acestora la răspunderea penală, în conformitate cu dreptul intern. Având în vedere faptul că persoanele fizice și juridice care cercetează vulnerabilități ar putea fi expuse, în unele state membre, răspunderii penale și civile, **statele membre sunt încurajate să adopte orientări în ceea ce privește neurmărirea penală a cercetătorilor în domeniul securității informațiilor** și exonerarea de răspundere civilă pentru activitățile desfășurate de aceștia. Echipele naționale CSIRT, în acest context trebuie să aibă rolul de coordonator al acestor procese. Acest rol ar trebui să includă identificarea și contactarea entităților în cauză, asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate, negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități. Anume aceste aspecte și au constituit obiectul examinărilor și includerii în proiectul de lege a reglementărilor corespunzătoare. În acest context, proiectul de lege vine să instituie baza juridico-normativă primară pentru crearea mecanismelor la nivel național capabile să utilizeze instrumentele cele mai eficiente în descoperirea vulnerabilităților. Pentru implementarea prevederilor din proiectul de lege cuprinse la art. 2 pct. 3) și art. 7 alin.(4) lit. i), Guvernul, în temeiul art. 7 alin. (4) lit. i) urmează să aprobe cadrul normativ care va detalia chestiunile ce vizează divulgarea coordonată a vulnerabilităților. Bineînțeles că în acest proces, de rând cu alte informații relevante, vor fi examinate și bunele practici europene și internaționale în acest domeniu, inclusiv cel al Letoniei.

Nr. d/o	Participantul la consultare publică		Conținutul obiecției/ propunerii (recomandării)	Argumentarea autorului proiectului
			implementat corect. În caz contrar, poate aduce consecințe grave asupra comunității, pană la lipsa totala de forță de muncă pe domeniul securității cibernetice care și până acum a avut de suferit prin ignoranță și lipsă de perspectivă în țara noastră. Ca și practici utile din domeniul legislativ, putem vedea exemplul Letoniei. Documentul privind proiectul de legi poate fi accesat aici: [https://www.sciencedirect.com/science/article/abs/pii/S0267364917303606#:~:text=In%202013%20the%20Netherlands%20launched,policy%20as%20a%20state%20policy] (https://www.sciencedirect.com/science/article/abs/pii/S0267364917303606#:~:text=In%202013%20the%20Netherlands%20launched,policy%20as%20a%20state%20policy) Un exemplu de divulgare coordonată a vulnerabilităților din Olanda poate fi accesat aici: [https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure] (https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure) Divulgarea coordonata a vulnerabilităților poate avea un impact cu mult mai mare asupra comunității de securitate din Moldova, decât am expus mai sus.	De asemenea , este important de menționat că procedeele, metodele și tehnicile utilizate în divulgarea vulnerabilităților au un caracter interdisciplinar și ar trebui să constituie obiectul unor examinări aprofundate ulterioare, inclusiv din perspectiva faptului că atinge domenii diverse care au tangență cu și legea penală și cea civilă. În acest context prevederile proiectului de lege sunt un imbold pentru inițierea procesului de implementarea a unor astfel de mecanisme.