Secțiunea 1:
Titlul proiectului de act normativ

HOTĂRÂRE

pentru stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative

Secțiunea a 2-a:
Motivul emiterii actului normativ

2.1 Sursa proiectului de act normativ

Proiectul de hotărâre a Guvernului a fost inițiat în temeiul art. 3 alin. (1) lit. c) și al art. 52 alin. (1) din *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*.

Ministerul Cercetării Inovării și Digitalizării, denumit în continare MCID, a inițiat *Legea nr. 58/2023*, în calitate de coordonator de reformă pe Componenta C7 - Transformare digitală, din Programul Național de Redresare și Reziliență, conform prevederilor Anexei la *Ordonanța de Urgență a Guvernului nr. 124/2021 privind stabilirea cadrului instituţional şi financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare şi rezilienţă, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă, cu modificările și completările ulterioare,* coroborate cu Acordul de finanțare dintre Ministerul Investițiilor și Proiectelor Europene și MCID: Reforma 3 privind Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice, Jalonul 151 privind intrarea în vigoare a Legii privind apărarea și securitatea cibernetică a României.

De asemenea, proiectul de hotărâre a Guvernului este inițiat de MCID, în calitatea sa de autoritate de stat în domeniul securității cibernetice, conform prevederilor art. 1 alin. (3) și ale art. 4 alin. (1) din *Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării*, cu modificările și completările ulterioare.

2.2 Descrierea situației actuale

La art. 3 alin. (1) lit. c) din *Legea nr. 58/2023* sunt prevăzute generic categoriile de subiecți de drept cărora li se aplică prevederile acesteia, respectiv „*reţelele şi sistemele informatice deţinute, organizate, administrate sau utilizate de autorităţi şi instituţii ale administraţiei publice centrale şi locale, altele decât cele prevăzute la lit. a), precum şi de persoane fizice şi juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit. b)*”. În conformitate cu prevederile art. 52 alin. (1) din *Legea nr. 58/2023* categoriile de persoane care se încadrează în conținutul și limitele prevederilor art. 3 alin. (1) lit. c) se stabilesc prin hotărâre a Guvernului.

Totodată, din interpretarea coroborată a prevederilor art. 3 alin. (1) lit. c), teza I cu cele ale art. 10 lit. c) din Legea nr. 58/ 2023, rezultă că ANCOM este inclusă, în temeiul legii, în categoria de la art. 3 lit. c), prin urmare, deși Autoritatea nu va face obiectul identificării prin prezentul proiect de HG, în conformitate cu dispozițiile art. 52 alin. (1) din Legea nr. 58/2023, aceasta se supune cerințelor legale atunci când acestea vizează autoritățile de la art. 3, în ansamblu, sau de la art. 3 alin. (1), lit. c) din același act normativ (de ex. cele ale art. 21 alin. (1), art. 24, art. 25, etc).

Curtea Constituțională a României, în Decizia nr. 70/2023 referitoare la respingerea obiecţiilor de neconstituţionalitate a dispoziţiilor art. 3 alin. (1) lit. c), art. 21 alin. (1), art. 22, art. 25, art. 41, art. 48 şi art. 50 din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, a stabilit următoarele repere jurisprudențiale în identificarea și stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit c) din Lege:

- paragr. 68: „*Astfel, prin raportare la prevederile legii supuse controlului de constituţionalitate şi interpretând sistematic prevederile sale, Curtea constată faptul că sfera de întindere a persoanelor fizice sau juridice private care prestează servicii publice sau de interes public nu poate să vizeze decât acele persoane fizice şi juridice de drept privat care prestează servicii publice sau de interes public cu un impact asupra securităţii naţionale în spaţiul cibernetic, iar nu orice persoană fizică sau juridică de drept privat care prestează orice serviciu public sau de interes public*”;
- paragr. 70: „*categoriile de persoane - subiecţi de drept se pot stabili prin hotărâre de Guvern numai prin luarea în considerare a criteriului de clarificare stabilit expres în lege (dacă prestează servicii publice sau servicii de interes public), a criteriului de eliminare (altele decât persoanele fizice sau juridice care prestează servicii publice de comunicaţii electronice pentru entităţi publice centrale sau locale) şi a obiectivelor avute în vedere de legiuitor la art. 4, prin identificarea numai a acelor categorii de persoane fizice sau juridice care prestează servicii publice sau de interes public care pot afecta securitatea cibernetică, deci şi securitatea naţională. În consecinţă, prin hotărârea prevăzută la art. 52 alin. (1), Guvernul va organiza punerea în aplicare a prevederilor art. 3 alin. (1) lit. c), ţinând cont de ansamblul normativ al întregii legi. Or, o hotărâre de Guvern care este prevăzută de legea însăşi pentru punerea în aplicare a unui articol din respectiva lege nu poate fi adoptată cu ignorarea întregului ansamblu normativ. Principiul legalităţii presupune ca actul administrativ să respecte nu doar norma legală de trimitere, ci ansamblul normativ aplicabil în respectivul domeniu de reglementare*”;
- paragr. 71: „*Pentru aceste considerente, Curtea reţine că dispoziţiile art. 3 alin. (1) lit. c) din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative asigură şi respectarea principiului securităţii raporturilor juridice, astfel cum acesta este reglementat prin dispoziţiile art. 1 alin. (5) din Constituţie, iar, la nivel infralegal, prin exigenţele Legii nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată în Monitorul Oficial al României, Partea I, nr. 260 din 21 aprilie 2010. Referitor la acest principiu, Curtea Constituţională a reţinut, în jurisprudenţa sa, că prin reglementarea*

normelor de tehnică legislativă legiuitorul a impus o serie de criterii obligatorii pentru adoptarea oricărui act normativ, a căror respectare este necesară pentru a asigura sistematizarea, unificarea şi coordonarea legislaţiei, precum şi conţinutul şi forma juridică adecvate pentru fiecare act normativ. Astfel, respectarea acestor norme concură la asigurarea unei legislaţii care respectă principiul securităţii raporturilor juridice, având claritatea şi previzibilitatea necesară (a se vedea Decizia nr. 26 din 18 ianuarie 2012, publicată în Monitorul Oficial al României, Partea I, nr. 116 din 15 februarie 2012, Decizia nr. 17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 79 din 30 ianuarie 2015, paragraful 96). În acelaşi sens, instanţa de contencios constituţional a statuat că, pentru ca legea să satisfacă cerinţa de previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea şi modalităţile de exercitare a puterii de apreciere a autorităţilor în domeniul respectiv, ţinând cont de scopul legitim urmărit, pentru a oferi persoanei o protecţie adecvată împotriva arbitrarului (a se vedea Decizia nr. 348 din 17 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 529 din 16 iulie 2014, paragraful 17, şi Decizia nr. 302 din 4 mai 2017, publicată în Monitorul Oficial al României, Partea I, nr. 566 din 17 iulie 2017, paragraful 56). De asemenea, s-a reţinut, prin aceeaşi jurisprudenţă, că o dispoziţie legală trebuie să fie precisă, neechivocă, să instituie norme clare, previzibile şi accesibile a căror aplicare să nu permită arbitrarul sau abuzul, precum şi că norma juridică trebuie să reglementeze în mod unitar şi uniform şi să stabilească cerinţe minimale aplicabile tuturor destinatarilor săi (a se vedea Decizia nr. 637 din 13 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 906 din 8 decembrie 2015, paragraful 34). Or, având în vedere considerentele mai sus arătate, Curtea reţine că dispoziţiile art. 3 alin. (1) lit. c) din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative sunt în acord cu exigenţele constituţionale anterior analizate";

- paragr 74: „*Curtea constată că introducerea în domeniul de aplicare a legii criticate a categoriilor de persoane fizice şi juridice care furnizează servicii publice sau de interes public prevăzute la art. 3 alin. (1) lit. c) este în acord cu unul dintre scopurile Directivei (UE) 2022/2.555 (Directiva NIS 2), respectiv acela prevăzut la punctul 7 din preambulul directivei de "a elimina divergenţele mari dintre statele membre în această privinţă şi pentru a asigura securitatea juridică în ceea ce priveşte măsurile de gestionare a riscurilor în materie de securitate cibernetică şi obligaţiile de raportare pentru toate entităţile relevante, ar trebui stabilit un criteriu uniform pentru a determina entităţile care intră în domeniul de aplicare al prezentei directive. Criteriul respectiv ar trebui să constea în aplicarea unei norme de plafonare a dimensiunii, potrivit căreia toate entităţile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei sau depăşesc plafoanele aferente întreprinderilor mijlocii prevăzute la alineatul (1) din respectivul articol şi care îşi desfăşoară activitatea în sectoarele şi furnizează tipurile de servicii sau desfăşoară activităţile reglementate de prezenta directivă intră în domeniul său de aplicare. Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici şi microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) şi (3) din*

respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esenţial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive." De altfel, şi punctul 6 din acelaşi preambul prevede faptul că: "Odată cu abrogarea Directivei (UE) 2016/1.148, domeniul de aplicare pe sectoare ar trebui să fie extins la o parte mai mare a economiei pentru a oferi o acoperire cuprinzătoare a sectoarelor şi a serviciilor de importanţă vitală pentru activităţile societale şi economice esenţiale din cadrul pieţei interne. În special, prezenta directivă vizează depăşirea deficienţelor legate de diferenţierea dintre operatorii de servicii esenţiale şi furnizorii de servicii digitale, care s-a dovedit a fi caducă, deoarece nu reflectă importanţa sectoarelor sau a serviciilor pentru activităţile societale şi economice din cadrul pieţei interne.";

- paragr. 77: „*Având în vedere considerentele mai sus invocate, Curtea reţine că prevederile art. 3 alin. (1) lit. c) din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, care includ în sfera destinatarilor legii inclusiv persoane fizice şi juridice care furnizează servicii publice ori de interes public, altele decât cele de la alin. (1) lit. b) din cuprinsul aceluiaşi articol, extinzând, astfel, sfera persoanelor cărora le incumbă obligaţiile prevăzute prin actul normativ criticat la întreprinderile mici şi mijlocii, nu contravin dispoziţiilor constituţionale ale art. 148 alin. (2) şi (4) referitoare la integrarea în Uniunea Europeană şi nici prevederilor art. 11 din Legea fundamentală cu privire la dreptul internaţional şi dreptul intern*”;
- paragr. 78: „*În ceea ce priveşte critica conform căreia dispoziţiile art. 3 alin. (1) lit. c) şi cele ale art. 21 alin. (1) şi art. 22 din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative încalcă dreptul la viaţa intimă, familială şi privată, precum şi libertatea de exprimare, a căror încălcare a constituit unul dintre temeiurile admiterii de către Curtea Constituţională, prin Decizia nr. 17 din 21 ianuarie 2015, a obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României (PL-x nr. 263/2014), Curtea constată că, prin legea care constituie obiectul prezentelor sesizări de neconstituţionalitate, legiuitorul a legiferat garanţii sporite necesare asigurării dreptului, respectiv a libertăţii fundamentale prevăzute la art. 26 şi, respectiv, la art. 30 din Constituţie*”;
- paragr. 87: „*Cu privire la proporţionalitatea obligaţiilor ce revin subiecţilor de drept care au în proprietate, administrare, organizare şi utilizare reţele şi sisteme informatice de tipul celor prevăzute de art. 3 alin. (1) lit. c), potrivit actului normativ criticat, Curtea constată că aceste obligaţii sunt, de principiu, următoarele: obligaţia de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată, dar nu mai târziu de 48 de ore de la constatarea incidentului [prevăzută la art. 21 alin. (1) criticat şi de autorii obiecţiilor]; obligaţia de asigurare a rezilienţei în spaţiul cibernetic, care se realizează prin implementarea de măsuri proactive şi reactive [prevăzută la art. 24 alin. (1) din legea criticată]; obligaţia de a pune la dispoziţia autorităţilor prevăzute la art. 10 din legea ce face obiectul sesizării, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date şi informaţii privind incidente,*

ameninţări, riscuri sau vulnerabilităţi a căror manifestare poate afecta o reţea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1) din aceeaşi lege, precum şi interconectarea acestora cu terţii şi cu utilizatorii finali [prevăzută la art. 25 alin. (1) criticat şi de autorii obiecţiilor]; obligaţia de a elabora şi de a pune în aplicare unele planuri proprii de acţiune pentru fiecare tip de alertă cibernetică [prevăzută la art. 29 alin. (1) şi (2) din legea criticată]; obligaţia de asigurare, pentru personalul propriu, a formării profesionale, educaţiei şi instruirii în domeniul securităţii şi apărării cibernetice prin cursuri, exerciţii, conferinţe, seminare, precum şi alte tipuri de activităţi (prevăzută la art. 37 din legea criticată); obligaţia de a implementa procesele de management al riscurilor de securitate cibernetică specifice lanţului de aprovizionare (prevăzută la art. 41 criticat şi de autorii obiecţiilor); obligaţia de a desemna persoane responsabile de securitatea cibernetică (prevăzută la art. 42 din legea criticată); obligaţia de a dispune măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanţului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor şi programelor de instruire existente (prevăzută la art. 43 din legea criticată); obligaţia de a dezvolta capabilităţi avansate de testare şi evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităţilor cibernetice ale echipamentelor, produselor software sau pieselor componente achiziţionate sau dezvoltate la nivel instituţional (prevăzută la art. 44 din legea criticată).";

- paragr. 88: - „*Analizând conţinutul obligaţiilor mai sus enumerate sub aspectul proporţionalităţii lor şi prin raportare la scopul legii criticate, precum şi argumentele prin care autorii îşi întemeiază critica potrivit căreia prevederile art. 21 alin. (1) instituie obligaţii disproporţionate sub aspectul caracterului lor excesiv de oneros în sarcina persoanelor fizice şi juridice prevăzute la art. 3 alin. (1) lit. c) din aceeaşi lege - cum sunt, cu titlu exemplificativ, obligaţiile de a asigura personalului propriu formarea profesională, educaţia şi instruirea în domeniul securităţii şi apărării cibernetice, prin participarea la cursuri, la exerciţii, la conferinţe, la seminare, precum şi la alte tipuri de activităţi - şi fără să se prevadă acordarea unui ajutor financiar din partea statului, Curtea constată că evaluarea acestor categorii de costuri excedează competenţei instanţei de contencios constituţional care, conform art. 2 alin. (3) din Legea nr. 47/1992 privind organizarea şi funcţionarea Curţii Constituţionale, "se pronunţă numai asupra constituţionalităţii actelor cu privire la care a fost sesizată, fără a putea modifica sau completa prevederile supuse controlului*"";
- paragr. 125: „*La fel ca în cazul argumentelor aduse împotriva sintagmei reglementate de art. 3 alin. (1) lit. c) analizate anterior, şi în cazul acestor critici problema de drept invocată nu vizează de fapt imprecizia, neclaritatea sau impredictibilitatea normei, ci sfera prea largă de întindere a reglementării. Or, imprecizia, neclaritatea şi impredictibilitatea unei norme sau noţiuni juridice nu poate fi confundată cu sfera de întindere a respectivei noţiuni juridice. De altfel, autorul obiecţiei (Avocatul Poporului) precizează în sesizarea sa faptul că sfera de aplicare a dispoziţiei este atât de largă, încât faţă de orice persoană se poate reţine exercitarea unei acţiuni care constituie ameninţare la adresa securităţii naţionale. Or, tocmai acest lucru denotă că, în realitate,*

sintagma criticată nu este neclară sau imprecisă, ci faptul că, în opinia autorului sesizării de neconstituţionalitate, aceasta este prea largă".

În același sens exprimat de Curtea Constituțională, și *Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)* prevede, la Anexele 1 și 2, sectoare de importanță critică ridicată și medie, care se circumscriu și limitelor și conținutului dat de legiuitorul român, pentru persoane juridice, la art. 3 alin. (1) lit. c) din *Legea nr. 58/2023*.

În momentul de față, există o nevoie de reglementare semnificativă în ceea ce privește claritatea și precizia legii cu privire la categoriile de subiecți de drept cărora li se aplică *Legea nr. 58/2023*. Legea, în forma sa actuală, face trimitere la aceste categorii în mod abstract și generic, fără a detalia entitățile care sunt considerate subiecți de drept în sensul acesteia.

Această nevoie de reglementare poate fi observată prin contrast cu alte sisteme juridice care au abordat în mod direct și specific această problemă. De exemplu, Directiva NIS și Directiva NIS2 stabilesc în anexele lor o listă clară a categoriilor de operatori de servicii esențiale și de furnizori de servicii digitale cărora li se aplică prevederile acestora. La fel, în Statele Unite, Ordonanța Executivă 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" stabilește anumite categorii de entități cărora li se aplică ordonanță.

În doctrina juridică, există un consens larg cu privire la necesitatea unor definiții clare și precise ale subiecților de drept în legislația privind securitatea cibernetică (Von der Burchard, 2018; Schmitt, 2017). Fără o astfel de individualizare, eficiența și eficacitatea legii pot fi afectate, deoarece entitățile incerte cu privire la statutul lor juridic pot ezita să implementeze măsurile de securitate necesare, iar autoritățile de aplicare a legii pot întâmpina dificultăți în a stabili responsabilități și sancțiuni.

Din punct de vedere jurisprudențial, incertitudinile pot fi observate în deciziile instanțelor care au trebuit să interpreteze dispoziții similare din alte domenii juridice (vezi, de exemplu, cazul "Digital Rights Ireland", în care Curtea de Justiție a Uniunii Europene a trebuit să interpreteze dispozițiile Directivei privind retenția datelor datorită lipsei de claritate cu privire la categoriile de entități la care se aplica directiva). Prin urmare, această nevoie de stabilire a subiecților de drept, dacă nu este abordată, poate duce la o aplicare incoerentă și neuniformă a *Legii nr. 58/2023* și poate afecta negativ eforturile de a consolida securitatea cibernetică a României.

Astfel, în lumina jurisprudenței, a doctrinelor juridice și a dreptului comparat, adoptarea acestui proiect de Hotărâre a Guvernului este esențială pentru a nevoia de individualizarea a subiecților de drept, pe cale legislativă, pentru a îmbunătăți securitatea cibernetică a României.

Este de menționat faptul că, în contextul termenului prevăzut la art. 52 alin. (1) din Legea nr. 58/2023, Ministerul Cercetării, Inovării și Digitralizării a întreprins totate demersurile legale necesare în vederea promovării actului normativ însă, parcurgerea tuturor pașilor procedurali necesari adoptării unui act normativ de o asemenea importanță și în elaborarea căruia sunt implicate mai multe instituții și autorități centrale, a necesitat o perioadă mai lungă de timp pentru realizarea acestora.

2.3 Schimbări preconizate

Proiectul de Hotărâre a Guvernului propune adoptarea dispozițiilor pentru stabilirea categoriilor de persoane cărora li se aplică prevederile *Legii nr. 58/2023*, în completarea cadrului normativ existent.

Unul dintre principalele avantaje ale acestei reglementări constă în definirea explicită și cuprinzătoare a categoriilor de entități cărora li se aplică legea. Astfel, prin detalierea subiecților de drept, proiectul reduce ambiguitatea juridică și asigură o interpretare și aplicare mai uniformă și predictibilă a prevederilor *Legii nr. 58/2023*. Aceasta este o abordare comună în dreptul comparat și în cel al Uniunii Europene. De exemplu, Directiva (UE) 2022/2555 care reprezintă unul dintre principalele instrumente juridice ale Uniunii Europene în domeniul securității cibernetice, stabilește în mod similar categorii specifice de entități care sunt supuse regulilor sale.

Proiectul de Hotărâre a Guvernului propus poate fi considerat și ca o continuare a jurisprudenței relevante în domeniu. De exemplu, Curtea de Justiție a Uniunii Europene a recunoscut în mod constant importanța securității cibernetice și necesitatea unei reglementări clare și cuprinzătoare în acest domeniu. Prin oferirea unui cadru juridic mai robust și mai detaliat pentru aplicarea *Legii nr. 58/2023*, proiectul propus este în concordanță cu această jurisprudență.

Prezentele *dispoziții privind stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative,* stabilesc cadrul legal necesar asigurării și menținerii în parametri optimi a disponibilității, continuității și integrității, cât și asigurării rezilienței rețelelor și sistemelor informatice, îndeosebi a celor cu valențe critice pentru securitatea națională, deținute, organizate, administrate sau utilizate de autorități și instituții ale administrației publice centrale și locale, precum și de persoane fizice și juridice care furnizează servicii publice ori de interes public, în sensul *Legii 58/2023*, și care se încadrează într-una din următoarele categorii de persoane, care îndeplinesc cumulativ următoarele condiții:

a) sunt autorități și instituții ale administrației publice centrale și locale, potrivit prevederilor art. 2 și art. 3 din *Ordonanța de Urgență a Guvernului nr. 57/2019 privind Codul administrativ*, cu modificările și completările ulterioare, persoane juridice de drept privat care au statutul de instituție de utilitate publică, astfel cum sunt definite la art. 5 lit. aa), persoane fizice sau juridice cu capital privat care prestează servicii publice, astfel cum sunt definite la art. 5 lit. kk), sau servicii publice deconcentrate, astfel cum sunt definite la art. lit. ll) din același act normativ.
b) nu fac parte dintre autoritățile și instituțiile publice sau persoanele fizice sau juridice de drept privat prevăzute la art. 3 alin. (1) lit. a) și lit. b), precum și la art. 10 alin. (1) lit. c) din *Legea nr. 58/2023*;
c) serviciul furnizat de acestea depinde de infrastructuri informatice și de comunicații de interes național, astfel cum sunt definite la art. 2 lit. d) din *Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G*;

Proiectul de Hotărâre a Guvernului prevede de asemenea obligațiile subiecților de drept în cadrul procedurii de identificare și evaluare a serviciilor, rețelelor și sistemelor informatice, conform prevederilor art. 24 alin. (2) lit. h) din Legea nr. 58/2023, dar și conform prevederilor art. 42 din Legea nr. 58/2023,

În final, este prevăzut că, în aplicarea prevederilor ale art. 41 alin. (1) din Legea nr. 58/2023, DNSC elaborează, cu consultarea autorităților prevăzute la art. 10 din Legea nr. 58/2023, ghiduri în sprijinul implementării proceselor de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare.
Prin adoptarea acestui proiect, se va asigura o mai bună securitate juridică și se va oferi un cadru clar pentru implementarea eficientă a măsurilor de securitate cibernetică prevăzute de *Legea nr. 58/2023*. În plus, acest proiect va facilita cooperarea și coordonarea între diferitele entități implicate în apărarea cibernetică a României, deoarece toate părțile vor avea o înțelegere clară a rolurilor și responsabilităților lor.

Proiectul de Hotărâre a Guvernului propus asigură o descriere cuprinzătoare și detaliată a categoriilor de subiecți de drept cărora li se aplică legea. Prin adoptarea acestui proiect, se va asigura o mai bună securitate juridică și se va oferi un cadru clar pentru implementarea eficientă a măsurilor de securitate cibernetică prevăzute de Legea nr. 58/2023. În plus, acest proiect va facilita cooperarea și coordonarea între diferitele entități implicate în apărarea cibernetică a României, deoarece toate părțile vor avea o înțelegere clară a rolurilor și responsabilităților lor. Forma actuală a proiectului de act normativ a fost agreată, împreună cu reprezentanții Ministerului Justiției, în cadrul ședinței Grupului de Suport Tehnic ce a avut loc în data de 28 februarie 2024.

În plus, prezentul proiect, Legea nr. 58/2023 și cele două acte normative, *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, cu modificările și completările ulterioare și *Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Naţional de Securitate Cibernetică*, cu modificările şi completările ulterioare, formează un pachet legislativ coerent, corelat, care asigură facilitare în dezvoltare și eficiență în implementarea de măsuri și capabilități reale de securitate și apărare cibernetică. Este necesară sincronizarea și cooperarea în timp real pentru ca autoritățile statului să câștige lupta împotriva amenințărilor existente în spațiul cibernetic, care prin natura lor, au un grad ridicat de agilitate și complexitate. De altfel, este de menționat și faptul că în instrumentul de motivare al Legii nr. 58/2023 se prevăd următoarele: *,,prezenta lege nu intră în contradicție și nu dublează Legea 362/2018 și Ordonanța de urgență a Guvernului nr. 104/2021, ci le completează în vederea creării unei arhitecturi legislative cuprinzătoare și satisfăcătoare pentru domeniul securității și apărării cibernetice.''*
În instrumentul de motivare al Legii nr. 58/2023, la secțiunea a 5-a, efectele proiectului de act normativ asupra legislației în vigoare, punctul 1 *măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ* la lit. b*) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziții*, la punctul 1 se prevede: *,,categoriile de persoane prevăzute la art.3 alin. (1) lit. c) din proiectul de lege se stabilesc prin hotărâre de Guvern inițiată de MCID adoptată în maximum 60 de zile de la intrarea în vigoare.''*

În acest fel, legiuitorul a considerat necesar a sublinia faptul că aceste categorii de persoane vor fi stabilite ulterior prin legislație secundară, prin actul normativ stabilindu-se criteriile generale de identificare a destinatarilor legii, aceștia trebuind a fi ulterior identificați dintre categoriile trasate în conținutul actului normativ cu putere superioară, Legea nr. 58/2023.

În domeniul securității cibernetice, art. 3 alin. (1) lit. c) face referire la obiectul de aplicare al Legii nr. 58/2023. Obiectul de aplicare este limitat la domeniul securității cibernetice, fiind clar separat de cel al apărării cibernetice. Rezultă că lit. c) se referă la rețele și sisteme informatice, elemente pe care le definește ulterior.

În legătură cu aceste rețele și sisteme informatice, se dispune faptul că acestea trebuie fie să fie deținute, fie organizate, fie administrate, fie utilizate de un grup de entități. Astfel, vorbind despre posesorii elementelor care fac obiectul aplicării Legii nr. 58/2023, lit. c) prevede că aceștia pot face parte din două categorii de entități diferențiate în mod general prin caracteristici considerate a fi generale de către legiuitor în domeniul securității cibernetice, respectiv:
1) definite de interesul urmărit, anume interesul public, deoarece acesta promovează, protejează și realizează un scop general al societății;
2) persoane fizice și juridice care furnizează servicii publice ori de interes public. În legătură cu aceste din urmă calități ale persoanelor amintite CCR, în cadrul DCC nr. 70/2023 abordează întocmai această speță.

Dintre aceste categorii generale în care au fost împărțiți posesorii rețelelor și sistemelor informatice, legiuitorul exclude entitățile prevăzute la lit. a) și lit. b) ale aceluiași art. 3 alin. (1) din Legea nr. 58/2023, corespunzător.

Astfel, actul normativ oferă o încadrare clară a categoriilor de destinatari pentru care Legea nr. 58/2023 poate institui drepturi și aduce obligații. Însă, astfel cum se arată și în instrumentul de motivare al legii, această trasare a competenței actului normativ trebuie completată, în concordanță cu contextul reglementării, cu alte caractere, prin hotărâre de Guvern, în vederea identificării corespunzătoare a entităților ce dețin, organizează, administrează sau utilizează rețelele și sistemele informatice, conturându-se astfel relația de întreg – parte, cu următoarele semnificații: întreg, autorități și instituții ale administrației publice centrale și locale, altele decât cele prevăzute la lit. a), precum și de persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit. b) și parte, entitățile identificate conform proiectul de hotărâre propus.

Proiectul de act normativ respectă prevederile privitoare la activitatea de legiferare, anume conținutul și fundamentarea soluțiilor legislative, astfel încât acesta instituie reguli necesare, suficiente și posibile care să conducă la o cât mai mare stabilitate și eficiență legislativă. Soluțiile pe care le cuprinde trebuie să fie temeinic fundamentate, luându-se în considerare interesul social, politica legislativă a statului român și cerințele corelării cu ansamblul reglementărilor interne și ale armonizării legislației naționale cu legislația comunitară și cu tratatele internaționale la care România este parte, precum și cu jurisprudența Curții Europene a Drepturilor Omului. De asemenea, se integrează în ansamblul legislației corespunzătoare, prin respectarea cerințelor de:
a) proiectul de act normativ trebuie corelat cu prevederile actelor normative de nivel superior sau de același nivel, cu care se află în conexiune;
b) proiectul de act normativ, întocmit pe baza unui act de nivel superior, nu poate depăși limitele competenței instituite prin acel act și nici nu poate contraveni principiilor și dispozițiilor acestuia;
c) proiectul de act normativ trebuie să fie corelat cu reglementările comunitare și cu tratatele internaționale la care România este parte;
d) proiectul de act normativ trebuie să fie corelat cu dispozițiile Convenției europene a drepturilor omului și ale protocoalelor adiționale la aceasta, ratificate de România, precum și cu jurisprudența Curții Europene a Drepturilor Omului.

2.4 Alte informații *)
Nu este cazul.

Secțiunea a 3-a:
Impactul socioeconomic **)

3.1 Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ

Nu este cazul.

3.2 Impactul social

Prin stabilirea unor reguli clare și coerente pentru securitatea cibernetică și definirea entităților care trebuie să se conformeze acestor reguli, proiectul ajută la sporirea încrederii publicului în infrastructura digitală a României. Acesta crește, de asemenea, încrederea în tranzacțiile online și utilizarea serviciilor digitale, care au devenit esențiale în societatea modernă.

Îmbunătățirea cadrului legislativ privind securitatea cibernetică poate contribui la sporirea rezilienței societății în fața atacurilor cibernetice, care pot afecta atât infrastructurile și sistemele informatice cu relevanță pentru securitatea și apărarea cibernetică națională, cât și viața de zi cu zi a oamenilor. Acest lucru ajută la prevenirea perturbărilor majore și a potențialelor consecințe negative, pe plan economic și social. Un cadrul legislativ puternic poate contribui la dezvoltarea de capacități avansate de cyberintelligence în România, ceea ce poate ajuta la detectarea și prevenirea amenințărilor cibernetice și la protejarea securității naționale.

Proiectul stimulează promovarea practicilor bune de igienă cibernetică în rândul publicului larg și al organizațiilor, ceea ce poate ajuta la prevenirea incidentelor cibernetice și la sporirea securității cibernetice la nivelul întregii societăți.

3.3 Impactul asupra drepturilor și libertăților fundamentale ale omului

Proiectul de act administrativ cu caracter normativ, coroborat cu *Legea nr. 58/2023*, are un impact pozitiv asupra drepturilor și libertăților fundamentale ale omului, după cum urmează:

a) Protecția dreptului la viață privată: Consolidarea securității cibernetice poate reduce riscul de încălcări ale securității datelor, care ar putea compromite dreptul la viață privată. Implementarea unor măsuri de securitate cibernetică solide poate contribui la protejarea datelor personale și a informațiilor confidențiale împotriva accesului neautorizat sau a scurgerilor de date.
b) Libertatea de exprimare: O securitate cibernetică robustă poate proteja și libertatea de exprimare online, oferind utilizatorilor încrederea că pot împărtăși opinii și informații fără teama de represalii sau de a fi ținte ale atacurilor cibernetice.
c) Dreptul la informare: O componentă cheie a securității cibernetice este educația utilizatorilor în ceea ce privește practicile de navigare sigure pe internet și recunoașterea semnelor potențiale ale atacurilor cibernetice. Prin educarea publicului asupra acestor aspecte, proiectul poate contribui la promovarea dreptului la informare.
d) Accesul la servicii publice: Îmbunătățirea securității cibernetice a instituțiilor publice și a furnizorilor de servicii publice poate contribui la asigurarea unui acces continuu la servicii publice esențiale. Prin protejarea acestor sisteme împotriva atacurilor cibernetice, reglementările propuse prin proiectul de act administrativ cu caracter normativ pot contribui la protejarea dreptului cetățenilor de a avea acces la aceste servicii.

e) Dreptul la securitate: Într-o eră digitală, securitatea cibernetică a devenit o parte integrantă a dreptului la securitate. Prin protejarea infrastructurilor și a sistemelor informatice cu relevanță pentru securitatea și apărarea cibernetică națională împotriva atacurilor cibernetice, reglementările propuse prin proiectul de act administrativ cu caracter normativ contribuie la protejarea acestui drept fundamental.

3.4 Impactul macroeconomic

Proiectul de act administrativ cu caracter normativ va avea un impact pozitiv macroeconomic asupra României în după cum urmează:

a) **Protecția infrastructurilor și a sistemelor informatice cu relevanță pentru securitatea și apărarea cibernetică națională**: Securitatea cibernetică a infrastructurilor și sistemelor informatice este esențială pentru funcționarea economiei unei națiuni. În cazul unui atac cibernetic, infrastructura informatică aferentă rețelelor de energie, de transport, comunicații, servicii de sănătate și servicii financiare poate fi compromisă, având un impact negativ asupra economiei. Prin îmbunătățirea securității cibernetice a acestor sisteme, reglementările propuse prin proiectul de act administrativ cu caracter normativ pot contribui la protejarea economiei României;
b) **Creșterea încrederii în economia digitală**: Securitatea cibernetică solidă crește încrederea consumatorilor și a întreprinderilor în tranzacții online și servicii digitale. Acest lucru poate stimula utilizarea și dezvoltarea de noi tehnologii și servicii digitale, favorizând astfel creșterea economică.
c) **Reducerea costurilor asociate cu atacurile cibernetice**: Costurile asociate cu atacurile cibernetice - cum ar fi pierderile financiare directe, costurile de recuperare după un atac și costurile reputaționale - pot fi semnificative. Prin îmbunătățirea securității cibernetice, reglementările propuse prin proiectul de act administrativ cu caracter normativ pot contribui la reducerea acestor costuri.
d) **Atragerea de investiții**: O legislație solidă în domeniul securității cibernetice este un factor atractiv pentru investitori, care pot considera că o astfel de legislație reduce riscul asociat cu investițiile în tehnologia informației și în economia digitală a țării.
e) **Crearea de locuri de muncă**: Măsurile de securitate cibernetică avansate necesită o forță de muncă calificată. Prin urmare, reglementările propuse prin proiectul de act administrativ cu caracter normativ vor stimula crearea de locuri de muncă în sectorul securității cibernetice, contribuind astfel la ocuparea forței de muncă și la creșterea economică.

3.4.1 Impactul asupra economiei și asupra principalilor indicatori macroeconomici

Înțelegând importanța securității cibernetice în societatea contemporană, proiectul de act administrativ cu caracter normativ propus ar putea avea un impact semnificativ asupra economiei României și asupra principalilor indicatori macroeconomici.

În primul rând, protejarea infrastructurilor și a sistemelor informatice cu relevanță pentru securitatea și apărarea cibernetică națională de atacurile cibernetice ar fi o contribuție directă la stabilitatea macroeconomică a țării. Infrastructura informatică aferentă rețelelor de energie, de transport, comunicații, servicii de sănătate și servicii financiare, este esențială pentru funcționarea oricărei economii moderne. Atacurile cibernetice asupra acestor sectoare pot provoca perturbări semnificative, care ar putea avea un impact negativ asupra produsului intern brut (PIB) și asupra creșterii economice.

De asemenea, reglementările propuse prin proiectul de act administrativ cu caracter normativ pot consolida încrederea în economia digitală. Aceasta poate fi esențială pentru stimularea investițiilor în tehnologii noi și inovatoare, care la rândul lor, pot contribui la creșterea productivității. În plus, încrederea sporită poate stimula consumul de bunuri și servicii digitale, ceea ce ar putea avea un impact pozitiv asupra creșterii PIB.

De asemenea, securitatea cibernetică este un sector în creștere rapidă care poate contribui la crearea de noi locuri de muncă. Dezvoltarea capacităților de securitate cibernetică poate stimula cererea de specialiști în domeniu, ceea ce ar putea avea un impact pozitiv asupra ocupării forței de muncă și a ratei șomajului.

În ceea ce privește investițiile, o legislație solidă în domeniul securității cibernetice poate atrage investiții, atât locale, cât și străine, în tehnologia informației și în economia digitală a României. Aceste investiții pot contribui la creșterea economică și pot avea un impact pozitiv asupra balanței de plăți.

În final, implementarea acestui proiect de act administrativ cu caracter normativ poate ajuta la prevenirea costurilor asociate cu atacurile cibernetice, cum ar fi pierderile financiare directe, costurile de recuperare și costurile reputaționale. Reducerea acestor costuri ar putea avea un impact pozitiv asupra sănătății financiare a firmelor și a economiei în ansamblu.

Proiectul de act administrativ cu caracter normativ este în concordanță cu obligațiile internaționale și europene ale României și îmbunătățește poziția țării de actor responsabil în domeniul securității cibernetice. Acesta este un semnal pozitiv pentru investitori și pentru comunitatea internațională, care poate duce la creșterea încrederii în economia României. Un alt aspect juridic care poate avea impact asupra economiei într-un mod pozitiv este acela referitor la faptul că un cadru legal clar și cuprinzător în domeniul securității cibernetice poate reduce incertitudinea pentru companii. Companiile se pot baza pe un set clar de reguli și norme în gestionarea riscurilor de securitate cibernetică, ceea ce le poate permite să se concentreze pe inovație și creștere. În plus, acesta poate ajuta la crearea unui mediu mai competitiv în sectorul securității cibernetice, stimulând astfel dezvoltarea economică.

De asemenea, prin acest act administrativ cu caracter normativ, se recunoaște securitatea cibernetică ca o prioritate națională. Acest angajament poate atrage finanțări și investiții în acest domeniu, creând oportunități de dezvoltare economică.

În concluzie, proiectul de act administrativ cu caracter normativ în domeniul securității cibernetice are potențialul de a avea un impact pozitiv asupra economiei României și a principalilor indicatori macroeconomici. Acesta poate contribui la protecția și consolidarea infrastructurilor și a sistemelor informatice cu relevanță pentru securitatea și apărarea cibernetică națională, la consolidarea încrederii în economia digitală, la stimularea creșterii

economice și la crearea de noi locuri de muncă în sectorul securității cibernetice. În plus, acesta poate ajuta la atragerea de investiții și la prevenirea costurilor asociate cu atacurile cibernetice.

3.4.2 Impactul asupra mediului concurențial si domeniul ajutoarelor de stat
Nu este cazul.

3.5. Impactul asupra mediului de afaceri
Nu este cazul.

3.6 Impactul asupra mediului înconjurător
Nu este cazul.

3.7 Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării
Implementarea proiectului de act administrativ cu caracter normativ poate avea un impact semnificativ asupra evaluării costurilor și beneficiilor din perspectiva inovării și digitalizării în România.

Din punct de vedere juridic, introducerea unui astfel de cadru legal poate genera o serie de beneficii directe și indirecte în contextul digitalizării și inovării. Pe deoparte, va stimula încrederea în digitalizare prin furnizarea de garanții mai puternice de securitate pentru utilizatorii de servicii digitale. În același timp, va încuraja dezvoltarea și adoptarea de noi tehnologii și soluții inovatoare în domeniul securității cibernetice, datorită creșterii cererii de astfel de servicii într-un cadru legal bine definit.

Mai mult, este important să menționăm că există o interconectare puternică între securitatea cibernetică și inovație. Securitatea cibernetică poate acționa ca un facilitator al inovării, în sensul că poate crea un mediu de afaceri sigur în care companiile se pot simți confortabil, având posibilitatea să inoveze și să dezvolte noi produse și servicii. În acest sens, o reglementare solidă în domeniul securității cibernetice poate stimula inovația în întreaga economie.

În ceea ce privește costurile, este de așteptat ca implementarea acestui proiect de act administrativ cu caracter normativ să genereze o serie de costuri directe, cum ar fi costurile de conformare pentru entitățile reglementate (subiecților de drept cărora li se aplică prevederile *Legii nr. 58/2023*). Cu toate acestea, aceste costuri trebuie privite în contextul beneficiilor pe termen lung, care pot fi obținute prin protecția îmbunătățită împotriva amenințărilor cibernetice și prin stimularea inovării. De asemenea, un mediu de afaceri mai sigur poate reduce costurile asociate cu atacurile cibernetice, cum ar fi pierderile de date sau întreruperile operațiunilor.

În concluzie, este de așteptat ca acest proiect de act administrativ cu caracter normativ să aibă un impact pozitiv asupra evaluării costurilor și beneficiilor din perspectiva inovării și digitalizării în România. Beneficiile potențiale ale unui mediu de afaceri mai sigur și al unui cadru legal bine definit în domeniul securității cibernetice sunt susceptibile de a compensa costurile de conformare pe termen scurt.

3.8 Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile

Un proiect de act administrativ cu caracter normativ care vizează securitatea și apărarea cibernetică poate avea un impact important asupra evaluării costurilor și beneficiilor din perspectiva dezvoltării durabile.

Pe plan juridic, stabilirea unui cadrul legal în acest domeniu poate conduce la o serie de beneficii pentru dezvoltarea durabilă. Prin creșterea securității rețelelor și sistemelor informatice, proiectul poate contribui la promovarea unui mediu online sigur și de încredere în tehnologie, aspecte esențiale pentru a asigura o dezvoltare durabilă în era digitală. Protejarea infrastructurilor și a sistemelor informatice cu relevanță pentru securitatea și apărarea cibernetică națională de atacuri cibernetice ajută la menținerea funcționării eficiente a societății și la prevenirea potențialelor prejudicii economice și sociale pe termen lung.

Totodată, o securitate cibernetică puternică poate avea un rol esențial în protejarea datelor sensibile și a informațiilor, contribuind la respectarea drepturilor și libertăților individuale, o componentă cheie a dezvoltării durabile.

Referitor la costuri, punerea în aplicare a acestui proiect de act administrativ cu caracter normativ ar putea genera anumite costuri inițiale, cum ar fi cele asociate cu conformarea la noile reglementări. Însă, pe termen lung, se prefigurează economii substanțiale prin prevenirea atacurilor cibernetice costisitoare și prin creșterea eficienței și productivității în cadrul organizațiilor și instituțiilor care se conformează acestor reguli.

În concluzie, proiectul de act administrativ cu caracter normativ care abordează securitatea cibernetică poate avea un impact semnificativ asupra evaluării costurilor și beneficiilor din perspectiva dezvoltării durabile, oferind, atât protecție îmbunătățită împotriva amenințărilor cibernetice, cât și o bază solidă pentru inovație și creștere durabilă în era digitală.

3.9 Alte informații

Nu este cazul

Secțiunea a 4-a
Impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani), inclusiv informații cu privire la cheltuieli și venituri.*)**

- în mii lei (RON) -

Indicatori	Anul curent	Următorii patru ani				Media pe cinci ani
1	2	3	4	5	6	7
4.1 Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta: i. impozit pe profit ii. impozit pe venit						
b) bugete locale i. impozit pe profit						

c) bugetul asigurărilor sociale de stat: i. contribuții de asigurări						
d) alte tipuri de venituri (se va menționa natura acestora)						
4.2 Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta: i. cheltuieli de personal bunuri și servicii						
b) bugete locale: i. cheltuieli de personal ii. bunuri și servicii						
c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal bunuri și servicii						
d) alte tipuri de cheltuieli (se va menționa natura acestora)						
4.3 Impact financiar, plus/minus, din care: a) buget de stat						
4.3 Impact financiar, plus/minus, din care: a) buget de stat						
b) bugete locale						
4.4 Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare						
4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: a) fișa financiară prevăzută la art. 15 din *Legea nr. 500/2002 privind finanțele publice*, cu modificările şi completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată; b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi prioritățile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.						
4.8 Alte informații						
Secțiunea a 5-a:						

Efectele proiectului de act normativ asupra legislației în vigoare
5.1 Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ Nu este cazul
5.2 Impactul asupra legislației in domeniul achizițiilor publice Nu este cazul
5.3 Conformitatea proiectului de act normativ cu legislația UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE). Nu este cazul
5.3.1 Măsuri normative necesare transpunerii directivelor UE **Nu este cazul**
5.3.2 Măsuri normative necesare aplicării actelor legislative UE Nu este cazul
5.4 Hotărâri ale Curții de Justiție a Uniunii Europene Nu este cazul
5.5 Alte acte normative şi/sau documente internaționale din care decurg angajamente asumate Nu este cazul
5.1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ Nu este cazul **5.2. Impactul asupra legislaţiei în domeniul achiziţiilor publice** Nu este cazul **5.3. Conformitatea proiectului de act normativ cu legislația UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE)** Nu este cazul **5.3.1. Măsuri normative necesare transpunerii directivelor UE** Nu este cazul **5.3.2. Măsuri normative necesare aplicării actelor legislative UE** Nu este cazul

5.4. Hotărâri ale Curţii de Justiţie a Uniunii Europene

Nu este cazul

5.5. Alte acte normative şi/sau documente internaţionale din care decurg angajamente asumate

Nu este cazul

5.6. Alte informaţii

Există o serie de exemple notabile de state care au o legislație în domeniul securității cibernetice care, la fel ca în cazul României, prevede că subiecților de drept cărora li se aplică respectivele acte normative, sunt reglementate prin acte administrative cu caracter normativ distincte, astfel:

1. **Statele Unite ale Americii:** Statele Unite au un cadru legislativ extensiv privind securitatea cibernetică, inclusiv *Cybersecurity Information Sharing Act din 2015,* care permite împărtășirea de informații privind amenințările cibernetice între sectorul privat și guvern. Această lege se aplică unui număr mare de persoane juridice, inclusiv furnizorilor de servicii de internet, companiilor de software și hardware, băncilor și altor instituții financiare. în Statele Unite, Federal Information Security Management Act (FISMA) se aplică agențiilor guvernamentale federale și organizațiilor care prestează servicii în numele acestora. În plus, legi precum Health Insurance Portability and Accountability Act (HIPAA) se aplică în mod specific furnizorilor de servicii de sănătate.
2. **Regatul Unit al Marii Britanii și Irlandei de Nord**: Regatul Unit are mai multe legi privind securitatea cibernetică, inclusiv *Computer Misuse Act (1990), Data Protection Act (2018)* și *Network and Information Systems Regulations (2018)*, care implementează Directiva NIS a Uniunii Europene. Aceste legi se aplică unei game largi de persoane fizice și juridice, inclusiv operatorilor de servicii esențiale, furnizorilor de servicii digitale și persoanelor fizice care utilizează sisteme informatice. *Network and Information Systems (NIS) Regulations 2018* ale Regatului Unit identifică operatorii de servicii esențiale (OSE) în sectoare specifice, cum ar fi energia, transportul, sănătatea și infrastructura digitală, cărora li se aplică reglementările. De asemenea, sunt vizate anumite furnizoare de servicii digitale (DSP).
3. **Australia**: Australia are mai multe legi privind securitatea cibernetică, inclusiv *Privacy Act (1988), Spam Act (2003) și Cybercrime Act (2001).* Aceste legi se aplică unei game largi de persoane fizice și juridice și reglementează, printre altele, accesul neautorizat la sisteme informatice, atacurile de tip "*denial-of-service*" și fraudarea prin mijloace electronice. *Security of Critical Infrastructure Act (2018)* se aplică operatorilor de infrastructură critică din anumite sectoare, inclusiv energie, apă, transport și porturi.
4. **Uniunea Europeană:** Directivele NIS și NIS2 ale Uniunii Europene, care au fost transpuse în legislația națională de către statele membre, identifică de asemenea operator Germania: Germania a adoptat o serie de legi naționale de securitate cibernetică, inclusiv Legea privind securitatea IT (BSI Gesetz) și Legea privind controlul exporturilor de

software (Außenwirtschaftsgesetz). Aceste legi se aplică unei game largi subiecților de drept, inclusiv companiilor de IT, operatorilor de servicii esențiale și furnizorilor de servicii de telecomunicații.

5. **Canada***:* Legea privind protecția informațiilor personale și documentele electronice din Canada (PIPEDA) se aplică organizațiilor care colectează, folosesc sau dezvăluie informații personale în cursul activităților comerciale.
6. **Japonia**: Legea privind securitatea cibernetică din Japonia se aplică operatorilor de infrastructură critică, cum ar fi furnizorii de energie electrică, gaz și apă, operatorii de transport și de comunicații și instituțiile financiare. Aceștia sunt obligați să ia măsuri pentru a preveni amenințările cibernetice și să raporteze incidentele guvernului.
7. **India**: Legea IT din India *(Information Technology Act)* din 2000 se aplică persoanelor fizice, persoanelor juridice, agențiilor guvernamentale și organizațiilor care se ocupă cu orice formă de activitate digitală sau electronică ori de servicii esențiale și furnizori de servicii digitale.
8. **Singapore**: Legea privind securitatea cibernetică din Singapore, care a intrat în vigoare în 2018, se aplică operatorilor de infrastructură critică (CII) din diferite sectoare, inclusiv energia, serviciile bancare, transportul, guvernul, sănătatea, media și serviciile alimentare și de apă. Acești operatori sunt obligați să respecte un set de standarde de securitate cibernetică și să raporteze incidentele de securitate cibernetică.
9. **Africa de Sud**: Legea privind securitatea cibernetică din Africa de Sud, care a intrat în vigoare în 2020, se aplică o gamă largă de entități, inclusiv guvernul, sectorul privat și organizațiile fără scop lucrativ. Legea stabilește standardele minime de securitate cibernetică, obligația de a raporta incidentele de securitate cibernetică și impune pedepse pentru infracțiuni cibernetice.
10. **Noua Zeelandă**: Legea privind securitatea rețelelor și a sistemelor informatice (NIS) din Noua Zeelandă se aplică furnizorilor de servicii esențiale în sectoare precum sănătatea, energia, transportul și serviciile financiare. Acești furnizori sunt obligați să implementeze măsuri de securitate adecvate și să raporteze incidentele de securitate cibernetică.
11. **Brazilia**: Legea generală privind protecția datelor din Brazilia (LGPD) se aplică oricărei organizații, publice sau private, care procesează date personale în Brazilia. Aceasta include cerințe stricte pentru protejarea datelor și raportarea breșelor de securitate.
12. **Coreea de Sud**: Legea privind promovarea utilizării rețelelor de informații și protecția informațiilor (NIS Act) din Coreea de Sud se aplică furnizorilor de servicii de informații și operatorilor de infrastructură critică. Aceștia sunt obligați să implementeze măsuri de securitate adecvate și să raporteze incidentele de securitate cibernetică.

Este important de menționat că forța juridică a acestor legi variază în funcție de jurisdicția specifică și de natura amenințărilor cibernetice în cauză. De exemplu, în Statele Unite, *Cybersecurity Information Sharing Act* are o forță juridică substanțială și poate fi invocată pentru a facilita cooperarea între sectorul privat și guvern în cazul unor amenințări cibernetice serioase (complexe, de tip APT). În alte jurisdicții, precum Regatul Unit și Australia, legile

privind securitatea cibernetică pot fi invocate într-o gamă mai largă de circumstanțe, inclusiv în cazul încălcărilor de date și al atacurilor de tip "denial-of-service".

Secțiunea a 6-a:
Consultările efectuate în vederea elaborării proiectului de act normativ

6.1 Informații privind neaplicarea procedurii de participare la elaborarea actelor normative
Nu este cazul

6.2 Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate.
Nu este cazul

6.3 Informații despre consultările organizate cu autoritățile administrației publice locale
Au fost consultate structurile asociative, respectiv Asociația Municipiilor din România, Asociația Orașelor din România, Asociația Comunelor din România și Uniunea Naţională a Consiliilor Judeţene din România, iar ca urmare a acestor consultări nu au fost primite observații asupra proiectului de act normativ.

6.4 Informații privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative
Nu este cazul.

6.5 Informații privind avizarea de către:
a)**Consiliul Legislativ** - Se solicită avizul Consiliului Legislativ

b)**Consiliul Suprem de Apărare a Țării** - Se solicită avizul Consiliului Suprem de Apărare a Țării

c)**Consiliul Economic și Social** - Se solicită avizul Consiliului Economic și Social

d)**Consiliul Concurenței**

e)**Curtea de Conturi**

6.6 Alte informaţii

Secțiunea a 7-a:
Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ

7.1 Informarea societății civile cu privire la elaborarea proiectului de act normativ

Pentru proiectul de act administrativ cu caracter normativ a fost îndeplinită procedura stabilită prin dispozițiile *Legii nr. 52/2003 privind transparența decizională în administrația publică*, republicată. Proiectul a fost publicat pe pagina de internet a Ministerului Cercetării, Inovării și Digitalizării, în data de 04.03.2024.
7.2 **Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătății și securității cetățenilor sau diversității biologice.** Nu este cazul
7.2 .1Alte informații Nu este cazul
Secțiunea a 8-a: **Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ**
8.1 Măsurile de punere în aplicare a proiectului de act normativ Nu este cazul.
8.2 **Alte informații** Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative,* pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului* pentru stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAȚII
VALERIU-ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU