

GUVERNUL ROMÂNIEI



HOTĂRÂRE

pentru aprobarea normelor metodologice 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

În temeiul art. 108 din Constituția României, republicată, precum și al art. 52 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative,

Guvernul României adoptă prezenta hotărâre.

Articol unic - Se aprobă normele metodologice 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, prevăzute în anexa care face parte integrantă din prezenta hotărâre.

PRIM-MINISTRU
Ion-Marcel CIOLACU

NORME METODOLOGICE

**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**

Art. 1. -

- (1) Prezentele norme metodologice 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, denumite în continuare norme metodologice, 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, denumite în continuare operatori de servicii publice esențiale, 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 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) din Legea 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;
 - d) în cazul producerii unui incident de securitate cibernetică care afectează rețelele și sistemele informatice proprii, furnizarea serviciului prestat este perturbată semnificativ.
- (2) Este considerată o perturbare semnificativă a furnizării serviciului public sau de interes public, în funcție de cel puțin unul dintre următoarele criterii:
- a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;
 - b) dependența altor furnizori de servicii publice sau de interes public, a unor operatori de servicii esențiale ori a unor infrastructuri critice naționale de serviciul furnizat de entitatea în cauză;
 - c) impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;
 - d) distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;
 - e) importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.
- (3) În termen de 60 de zile de la data intrării în vigoare a prezentei hotărâri, Directoratul Național pentru Securitate Cibernetică elaborează Normele tehnice privind valorile de prag, criteriile și metodele pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii publice esențiale, care se aprobă prin ordin al Directoratului Național pentru Securitate Cibernetică și se publică în Monitorul Oficial al României, Partea I.

Art. 2. -

Persoanele care se încadrează în lista cu categoriile prevăzute la art. 1 se înscriu, cu denumirea de operatori de servicii publice esențiale, în Registrul operatorilor de servicii esențiale, prevăzut la art.5 din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice cu modificările și completările ulterioare.

Art. 3. -

(1) În vederea asigurării unui nivel ridicat de securitate, operatorii de servicii publice esențiale se identifică și se înscriu în Registrul operatorilor de servicii publice esențiale care se înființează și se întreține de către Directoratul Național pentru Securitate Cibernetică.

(2) Identificarea operatorilor de servicii publice esențiale se realizează de către toate entitățile care îndeplinesc criteriile stabilite la art. 1.

Art. 4. -

(1) Operatorii de servicii publice esențiale care se încadrează în categoriile și criteriile prevăzute la art. 1 sunt înscriși din oficiu sau la cerere în Registrul operatorilor de servicii esențiale.

(2) Înscrierea operatorilor de servicii publice esențiale în Registrul operatorilor de servicii publice esențiale se realizează prin decizia directorului Directoratului Național pentru Securitate Cibernetică care se comunică operatorului de servicii publice esențiale.

(3) În termen de 60 de zile de la intrarea în vigoare a prezentei hotărâri, Directoratul Național pentru Securitate Cibernetică elaborează Normele metodologice privind înscrierea și radierea operatorilor de servicii publice esențiale și operaționalizarea Registrului operatorilor de servicii publice esențiale care se aprobă prin ordin al directorului Directoratului Național pentru Securitate Cibernetică, care se publică în Monitorul Oficial al României, Partea I.

Art. 5. -

Înregistrarea, modificarea și radierea operatorilor de servicii publice esențiale stabiliți în condițiile prezentei hotărâri se realizează în condițiile prevăzute la Capitolului II, Secțiunea 1 din Legea nr. 362/2018, cu modificările și completările ulterioare.

Art. 6. -

Operatorii de servicii publice esențiale pot solicita asistența Directoratului Național pentru Securitate Cibernetică în procesul de identificare și înscriere în Registrul operatorilor de servicii publice esențiale ori în procesul de radiere.

Secțiunea 1:
Titlul proiectului de act normativ
HOTĂRÂRE

pentru aprobarea normelor metodologice 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

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. 10 alin. (1) lit. b) și al art. 52 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

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 Anexei la OUG nr. 124/2021 coroborat cu Acordul de finanțare dintre MIPE 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 Ministerul Cercetării Inovării și Digitalizării, 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 și funcționarea Ministerului Cercetării, Inovării și 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 subiecte de drept cărora li se aplică prevederile acesteia, respectiv *”rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de 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)”*. 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.

Curtea Constituțională a României, în Decizia nr. 70/2023 referitoare la respingerea obiecțiilor de neconstituționalitate a dispozițiilor art. 3 alin. (1) lit. c), art. 21 alin. (1), art. 22, art. 25, art. 41, art. 48 și art. 50 din Legea privind securitatea și apărarea cibernetică a României, precum și

pentru modificarea și 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 constituționalitate și 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 și juridice de drept privat care prestează servicii publice sau de interes public cu un impact asupra securității naționale în spațiul 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 - subiecți 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 comunicații electronice pentru entități publice centrale sau locale) și 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 și securitatea națională. În consecință, prin hotărârea prevăzută la art. 52 alin. (1), Guvernul va organiza punerea în aplicare a prevederilor art. 3 alin. (1) lit. c), ținând cont de ansamblul normativ al întregii legi. Or, o hotărâre de Guvern care este prevăzută de legea însăși pentru punerea în aplicare a unui articol din respectiva lege nu poate fi adoptată cu ignorarea întregului ansamblu normativ. Principiul legalității 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 reține că dispozițiile art. 3 alin. (1) lit. c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative asigură și respectarea principiului securității raporturilor juridice, astfel cum acesta este reglementat prin dispozițiile art. 1 alin. (5) din Constituție, iar, la nivel infralegal, prin exigențele 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 Constituțională a reținut, în jurisprudența 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 și coordonarea legislației, precum și conținutul și forma juridică adecvate pentru fiecare act normativ. Astfel, respectarea acestor norme concură la asigurarea unei legislații care respectă principiul securității raporturilor juridice, având claritatea și 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 același sens, instanța de contencios constituțional a statuat că, pentru ca legea să satisfacă cerința de*

previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea și modalitățile de exercitare a puterii de apreciere a autorităților în domeniul respectiv, ținând cont de scopul legitim urmărit, pentru a oferi persoanei o protecție 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, și 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 reținut, prin aceeași jurisprudență, că o dispoziție legală trebuie să fie precisă, neechivocă, să instituie norme clare, previzibile și accesibile a căror aplicare să nu permită arbitrarul sau abuzul, precum și că norma juridică trebuie să reglementeze în mod unitar și uniform și să stabilească cerințe 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 reține că dispozițiile art. 3 alin. (1) lit. c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative sunt în acord cu exigențele constituționale anterior analizate”;

- paragr 74: ”Curtea constată că introducerea în domeniul de aplicare a legii criticate a categoriilor de persoane fizice și 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 divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform pentru a determina entitățile 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 entitățile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei sau depășesc plafoanele aferente întreprinderilor mijlocii prevăzute la alineatul (1) din respectivul articol și care își desfășoară activitatea în sectoarele și furnizează tipurile de servicii sau desfășoară activitățile reglementate de prezenta directivă intră în domeniul său de aplicare. Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici și microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) și (3) din respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esențial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive.” De altfel, și punctul 6 din același 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 și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. În special, prezenta directivă vizează depășirea deficiențelor legate de diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă, deoarece

nu reflectă importanța sectoarelor sau a serviciilor pentru activitățile societale și economice din cadrul pieței interne.”;

- paragr. 77: ”Având în vedere considerentele mai sus invocate, Curtea reține că prevederile art. 3 alin. (1) lit. c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, care includ în sfera destinatarilor legii inclusiv persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la alin. (1) lit. b) din cuprinsul aceluiași articol, extinzând, astfel, sfera persoanelor cărora le incumbă obligațiile prevăzute prin actul normativ criticat la întreprinderile mici și mijlocii, nu contravin dispozițiilor constituționale ale art. 148 alin. (2) și (4) referitoare la integrarea în Uniunea Europeană și nici prevederilor art. 11 din Legea fundamentală cu privire la dreptul internațional și dreptul intern”;
- paragr. 78: ”În ceea ce privește critica conform căreia dispozițiile art. 3 alin. (1) lit. c) și cele ale art. 21 alin. (1) și art. 22 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative încalcă dreptul la viața intimă, familială și privată, precum și libertatea de exprimare, a căror încălcare a constituit unul dintre temeiurile admiterii de către Curtea Constituțională, prin Decizia nr. 17 din 21 ianuarie 2015, a obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României (PL-x nr. 263/2014), Curtea constată că, prin legea care constituie obiectul prezentelor sesizări de neconstituționalitate, legiuitorul a legiferat garanții sporite necesare asigurării dreptului, respectiv a libertății fundamentale prevăzute la art. 26 și, respectiv, la art. 30 din Constituție”;
- paragr. 87: ”Cu privire la proporționalitatea obligațiilor ce revin subiecților de drept care au în proprietate, administrare, organizare și utilizare rețele și sisteme informatice de tipul celor prevăzute de art. 3 alin. (1) lit. c), potrivit actului normativ criticat, Curtea constată că aceste obligații sunt, de principiu, următoarele: obligația 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 și de autorii obiecțiilor]; obligația de asigurare a rezilienței în spațiul cibernetic, care se realizează prin implementarea de măsuri proactive și reactive [prevăzută la art. 24 alin. (1) din legea criticată]; obligația de a pune la dispoziția autorităților 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 și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1) din aceeași lege, precum și interconectarea acestora cu terții și cu utilizatorii finali [prevăzută la art. 25 alin. (1) criticat și de autorii obiecțiilor]; obligația de a elabora și de a pune în aplicare unele planuri proprii de acțiune pentru fiecare tip de alertă cibernetică [prevăzută la art. 29 alin. (1) și (2) din legea criticată]; obligația de asigurare, pentru personalul propriu, a formării profesionale, educației și instruirii în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminare, precum și alte tipuri de activități (prevăzută la art. 37 din legea criticată); obligația de a implementa procesele de

management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare (prevăzută la art. 41 criticat și de autorii obiecțiilor); obligația de a desemna persoane responsabile de securitatea cibernetică (prevăzută la art. 42 din legea criticată); obligația de a dispune măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanțului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor și programelor de instruire existente (prevăzută la art. 43 din legea criticată); obligația de a dezvolta capacități avansate de testare și evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităților cibernetică ale echipamentelor, produselor software sau pieselor componente achiziționate sau dezvoltate la nivel instituțional (prevăzută la art. 44 din legea criticată).”;

- paragr. 88: - *”Analizând conținutul obligațiilor mai sus enumerate sub aspectul proporționalității lor și prin raportare la scopul legii criticate, precum și argumentele prin care autorii își întemeiază critica potrivit căreia prevederile art. 21 alin. (1) instituie obligații disproporționate sub aspectul caracterului lor excesiv de oneros în sarcina persoanelor fizice și juridice prevăzute la art. 3 alin. (1) lit. c) din aceeași lege - cum sunt, cu titlu exemplificativ, obligațiile de a asigura personalului propriu formarea profesională, educația și instruirea în domeniul securității și apărării cibernetică, prin participarea la cursuri, la exerciții, la conferințe, la seminare, precum și la alte tipuri de activități - și fără să se prevadă acordarea unui ajutor financiar din partea statului, Curtea constată că evaluarea acestor categorii de costuri excedează competenței instanței de contencios constituțional care, conform art. 2 alin. (3) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale, ”se pronunță numai asupra constituționalității 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, și 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 și impredictibilitatea unei norme sau noțiuni juridice nu poate fi confundată cu sfera de întindere a respectivei noțiuni juridice. De altfel, autorul obiecției (Avocatul Poporului) precizează în sesizarea sa faptul că sfera de aplicare a dispoziției este atât de largă, încât față de orice persoană se poate reține exercitarea unei acțiuni care constituie amenințare la adresa securității naționale. Or, tocmai acest lucru denotă că, în realitate, sintagma criticată nu este neclară sau imprecisă, ci faptul că, în opinia autorului sesizării de neconstituționalitate, 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 subiecte de drept cărora li se aplica Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României. Legea, în forma sa actuală, face trimitere la aceste categorii în mod abstract și generic, fără a furniza o listă cuprinzătoare și clară a entităților care sunt considerate subiecte 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 subiectelor 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 subiectelor 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 de Guvern este esențială pentru a nevoia de individualizarea a subiectelor de drept, pe cale legislativă, pentru a îmbunătăți securitatea cibernetică a României.

2.3 Schimbări preconizate

Proiectul de Hotărâre a Guvernului propune adoptarea normelor metodologice pentru stabilirea categoriilor de persoane cărora li se aplică prevederile Legii nr. 58/2023, având potențialul de a introduce schimbări semnificative și benefice în cadrul legislativ 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 crearea unei liste detaliate a subiectelor 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 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)), care reprezintă unul dintre principalele instrumente juridice ale Uniunii Europene în domeniul securității cibernetică, stabilește în mod similar categorii specifice de entități care sunt supuse regulilor sale.

În plus, proiectul inițiat pune în evidență importanța securității cibernetică în asigurarea funcționării eficiente și sigure a serviciilor publice esențiale. Prin înscrierea acestor entități în Registrul operatorilor de servicii esențiale, se subliniază necesitatea de a păstra rețelele și sistemele informatice în stare de funcționare optimă și de a menține reziliența în fața potențialelor incidente sau atacuri cibernetică. Aceasta este o abordare care reflectă tendințele actuale în doctrina juridică și în practica juridică internațională în domeniul securității cibernetică.

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 cibernetică 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 norme metodologice privind stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023, denumite în continuare norme metodologice, 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, denumite în continuare operatori de servicii publice esențiale, 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 lit. a) și lit. b) din Legea 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;
- d) în cazul producerii unui incident de securitate cibernetică care afectează rețelele și sistemele informatice proprii, furnizarea serviciului prestat este perturbată semnificativ.

Este considerată o perturbare semnificativă a furnizării serviciului public sau de interes public, în funcție de cel puțin unul dintre următoarele criterii:

- a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;

- b) dependența altor furnizori de servicii publice sau de interes public, a unor operatori de servicii esențiale ori a unor infrastructuri critice naționale de serviciul furnizat de entitatea în cauză;
- c) impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;
- d) distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;
- e) importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

În termen de 60 de zile de la data intrării în vigoare a prezentei hotărâri de Guvern, Directoratul Național pentru Securitate Cibernetică elaborează Normele tehnice privind valorile de prag, criteriile și metodele pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii publice esențial, care se aprobă prin ordin al directorului Directoratului Național pentru Securitate Cibernetică și se publică în Monitorul Oficial al României, Partea I.

Proiectul de Hotărâre a Guvernului propus aduce o soluție necesară acestei probleme, furnizând o listă cuprinzătoare și detaliată a categoriilor de subiecte 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.

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.

În era digitală, protecția datelor și a vieții private a devenit o preocupare majoră. Prin asigurarea unui nivel ridicat de securitate cibernetică, proiectul contribuie la protecția drepturilor digitale ale cetățenilor, inclusiv dreptul la confidențialitate și protecția datelor personale.

Îmbunătățirea cadrului legislativ privind securitatea cibernetică poate contribui la sporirea rezilienței societății în fața atacurilor cibernetice, care pot afecta atât infrastructura critică, 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 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 critice și a sistemelor informatice 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 infrastructurii critice: Securitatea cibernetică a infrastructurii critice este esențială pentru funcționarea economiei unei națiuni. În cazul unui atac cibernetic,

infrastructura critică - cum ar fi rețelele de energie, transportul, comunicațiile și serviciile 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 infrastructurii critice de atacurile cibernetice ar fi o contribuție directă la stabilitatea macroeconomică a țării. Infrastructura critică, care include energie, transport, servicii de sănătate, comunicații 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 infrastructurii critice, 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 și 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 (subiectele 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 cadru 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 infrastructurii critice 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 și completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată; b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele și prioritățile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală și 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 Măsurile normative necesare pentru aplicarea prevederilor proiectului de act normativ Nu este cazul						
5.2 Impactul asupra legislației în 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 Măsurile normative necesare transpunerii directivelor UE Nu este cazul						
5.3.2 Măsurile 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 și/sau documente internaționale din care decurg angajamente asumate Nu este cazul
5.1. Măsurile normative necesare pentru aplicarea prevederilor proiectului de act normativ Nu este cazul 5.2. Impactul asupra legislației în 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. Măsurile normative necesare transpunerii directivelor UE Nu este cazul 5.3.2. Măsurile 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 și/sau documente internaționale din care decurg angajamente asumate Nu este cazul 5.6. Alte informații 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 subiectele 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 operatorii. 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 de subiecte 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 cibernetică.
10. **Noua Zeelandă:** Legea privind securitatea rețelor 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 rețelor 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 cibernetică 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 cibernetică 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

Se solicită punct de vedere de la Asociația Municipiilor din România, Asociația Orașelor din România, Asociația Comunelor din România și Uniunea Națională a Consiliilor Județene din România.

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 informații

Secțiunea a 7-a:

Activități de informare publică privind elaborarea și 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 de hotărâre a Guvernului privind stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1), lit. c) din Legea nr. 58/2023 intră sub incidența situațiilor excepționale care justifică reducerea termenului de consultare publică la 10 zile lucrătoare. Acest argument se bazează pe următoarele considerente:

Primul argument este contextul global de securitate cibernetică în care ne aflăm. În ultimii ani, amenințările cibernetice au crescut într-un ritm alarmant. Cyber criminalii au început să atace nu doar organizații mari sau guverne, ci și persoane fizice sau grupuri vulnerabile. Situația a devenit și mai gravă în contextul pandemiei COVID-19, care a accelerat digitalizarea în multe domenii și a crescut dependența de tehnologie, făcând astfel mai multe ținte disponibile pentru atacuri.

Al doilea argument este legat de necesitatea urgentă de a proteja persoanele vulnerabile de amenințările cibernetice. Proiectul de hotărâre a Guvernului își propune să definească aceste categorii de persoane în cadrul Legii nr. 58/2023, permițând astfel adoptarea unor măsuri specifice de protecție. Este esențial să stabilim cât mai repede aceste categorii pentru a preveni orice daune care ar putea surveni din cauza atacurilor cibernetice.

În al treilea rând, întârzierea în adoptarea acestui proiect de hotărâre a Guvernului ar putea aduce o gravă atingere interesului public. Într-o lume tot mai conectată, securitatea cibernetică nu este doar o chestiune de protecție a datelor personale, ci și de securitate națională. Dacă nu acționăm rapid pentru a proteja categoriile vulnerabile de persoane, acestea pot deveni ținte pentru atacuri cibernetice care pot avea consecințe grave la nivel individual și societal.

În al patrulea rând, proiectul de hotărâre a Guvernului a depășit termenul de adoptare impus de legiuitor, situație generată de complexitatea elaborării și analizării categoriilor de persoane, a doctrinei și jurisprudenței de specialitate. Reducerea termenului de consultare publică se impune pentru a garanta intrarea în vigoare cât mai rapidă a proiectului de act administrativ cu caracter normativ.

Din aceste considerente, se poate concluziona că proiectul de hotărâre a Guvernului privind stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1), lit. c) din Legea nr. 58/2023 îndeplinește criteriile de excepție prevăzute la art. 7 alin. (13) din Legea nr. 52/2003 și, prin urmare, poate fi supus consultării publice pentru un termen de 10 zile lucrătoare.

7.2 Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum și efectele asupra sănătății și securității cetățenilor sau diversității biologice.

Nu este cazul

7.2 .1 Alte 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

8.2 Alte informații

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea normelor metodologice 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, pe care îl supunem Guvernului pentru aprobare.

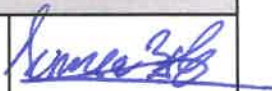
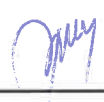
MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

FIȘĂ DE AVIZARE INTERNĂ

a proiectului de HOTĂRÂRE

pentru aprobarea normelor metodologice 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

FUNCȚIE PERSOANĂ AVIZATOARE	NUME ȘI PRENUME	DATA AVIZARE	OBSERVAȚII	SEMNĂTURĂ
Structuri avizatoare				
Secretar de Stat	Bogdan Mihai DUMEA	30.08.2023		
Secretar General	Victoria Ivonne SAGHIU	29.08.2023	—	
Șef Serviciu Serviciul Avizare Acte Normative și Relația cu Parlamentul	Mihaela SILE	28.08.2023	—	
Consilier	Pierrelle Boitard Profira	28.08.2023	—	
Consilier pentru afaceri europene Direcția Tehnologia Informației și Transformare Digitală	Raluca-Oana BONTEA	28.08.2023		

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea normelor metodologice 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, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

**VICEPRIM-MINISTRU
MARIAN NEACȘU**

**VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU**

**DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN**

**p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU**

**DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN SILVAN PAHONȚU**

**DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE**

**DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI
NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU**

**DIRECTORUL DIRECTORATULUI
NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN**

**PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU
ADMINISTRARE ȘI 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**