Secţiunea 1

Titlul proiectului de act normativ

HOTĂRÂRE

pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative

Secţiunea a 2-a

Motivul emiterii actului normativ

2.1. Sursa proiectului de act normativ

Proiectul de hotărâre a Guvernului a fost iniţiat în temeiul prevederilor art. 10 alin. (1) lit. b) şi ale art. 52 lin. (1) din *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*.

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

2.2. Descrierea situaţiei actuale

Securitatea cibernetică reprezintă o provocare globală în creştere, iar ameninţările, riscurile sau vulnerabilităţile la adresa reţelelor şi sistemelor informatice constituie o problemă serioasă, cu un impact major asupra securităţii naţionale şi a activităţilor economice.

Legea nr. 58/2023 a reprezentat un pas important în reglementarea acestui domeniu, stabilind cadrul juridic de funcţionare a furnizorilor de servicii tehnice de securitate cibernetică şi

obligațiile acestora de a furniza date și informații privind incidentele cibernetice, amenințările, riscurile sau vulnerabilitățile la adresa rețelelor și sistemelor informatice.

Astfel, art. 25 din *Legea nr. 58/2023* prevede următoarele: "*(1) Furnizorii de servicii tehnice de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, respectiv, în maximum 5 zile de la data primirii solicitării, cu privire la amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1), precum și interconectarea acestora cu terții și cu utilizatorii finali. (2) Datele și informațiile prevăzute la alin. (1) nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut. (3) Datele și informațiile prevăzute la alin. (1) se transmit în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord, în formatul și structura conforme raportării de incidente cibernetice în PNRISC, prevăzute la art. 22.*"

De asemenea, art. 52 alin. (5) din Legea nr. 58/2023 prevede următoarele: "*(5)Normele metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) se stabilesc prin hotărâre a Guvernului, inițiată de MCID, adoptată în maximum 90 de zile de la data intrării în vigoare a prezentei legi.*"

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 ceea ce privește aprobarea normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023, astfel:

- paragr. 84: "*Mai mult, analizând dispozițiile legale mai sus invocate, Curtea reține că sistemele de notificare prevăzute la art. 21, art. 22, respectiv la art. 25 din legea criticată nu presupun colectarea de date de conținut și nici extragerea unilaterală și fără autorizare de date și informații de pe un sistem informatic, iar autoritățile care gestionează incidentele de securitate cibernetică semnalate sunt atât operatori de date cu caracter personal (prin efectul legislației privind datele cu caracter personal), cât și autorități cu atribuții expres prevăzute în domeniul securității cibernetice (atribuțiile acestora neputând fi confundate sau suprapuse cu cele ale organelor judiciare care realizează percheziții informatice, conform art. 168 din Codul de procedură penală). Prin urmare, obligațiile care revin subiectelor de drept prevăzute la art. 3 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative nu se referă nici la stocarea de date cu caracter personal ale cetățenilor, nici la accesul, în lipsa unui mandat judecătoresc, într-un sistem informatic și nici la alte proceduri intruzive în viața privată a cetățeanului*";
- paragr. 92: "*dispozițiile legale mai sus invocate trebuie interpretate în coroborare cu prevederile art. 27 lit. b) din Legea nr. 362/2018, care prevăd în sarcina operatorilor*

de servicii esenţiale (OSE) şi a furnizorilor de servicii digitale (FSD) obligaţia de a furniza informaţii suplimentare cu privire la incidentele de securitate cibernetică, Directoratul Naţional de Securitate Cibernetică putând solicita informaţii suplimentare operatorului sau furnizorului autor al notificării, în vederea îndeplinirii obligaţiilor ce îi revin, cu menţionarea termenului în care informaţiile solicitate trebuie furnizate, dar şi cu dispoziţiile secţiunii 2 "Notificarea incidentelor de securitate" a capitolului IV "Asigurarea securităţii reţelelor şi sistemelor informatice" al aceleiaşi legi, care prevăd la art. 26 alin. (3) şi (4) că notificarea incidentelor conţine, în mod obligatoriu, următoarele informaţii: elementele de identificare ale infrastructurii şi operatorului sau furnizorului în cauză; descrierea incidentului; perioada de desfăşurare a incidentului; impactul estimat al incidentului; măsuri preliminare adoptate; lista de autorităţi ale statului afectate de incident; întinderea geografică potenţială a incidentului; date despre efecte potenţial transfrontaliere ale incidentului şi, de asemenea, că notificarea prevăzută la alin. (1) şi (2) ale art. 26 nu va conţine informaţii clasificate şi date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate în incident, în condiţiile legii.";

- paragr. 93: "*obligaţiile reglementate prin art. 25 alin. (1) (...) au ca obiect operaţiuni strict tehnice de natură a asigura prestarea serviciilor la care fac referire dispoziţiile art. 3 din legea criticată, într-un climat de securitate cibernetică. Mai mult, alin. (2) al art. 25 din legea criticată prevede că datele şi informaţiile mai sus analizate nu vizează, prin scopul solicitării, date cu caracter personal şi date de conţinut. Totodată, obligaţiile prevăzute la art. 25 alin. (1) din legea criticată vor fi îndeplinite cu respectarea prevederilor capitolului IX al aceleiaşi legi, referitoare la confidenţialitatea şi protecţia securităţii datelor şi informaţiilor persoanelor fizice şi juridice analizate anterior*";
- paragr. 94: "*stabileşte în sarcina furnizorilor de servicii tehnice de securitate cibernetică doar obligaţii cu caracter tehnic, menite să asigure descoperirea şi sancţionarea în timp util a incidentelor, ameninţărilor, riscurilor sau vulnerabilităţilor de securitate cibernetică, obligaţii care exclud furnizarea către autorităţile prevăzute la art. 10 din legea criticată a unor date cu caracter personal sau a unor date de conţinut*";
- paragr. 96: "*Curtea constată că art. 25 din legea supusă controlului de constituţionalitate reglementează obligaţii ce au ca finalitate descoperirea unor faptele de natură ilicită, lato sensu. Aceste aspecte nu exclud însă obligaţia furnizorilor de servicii tehnice de securitate cibernetică de a sesiza organele de urmărire penală, în ipoteza în care constată comiterea unor fapte prevăzute de legea penală, precum cele incriminate în cuprinsul capitolului VI, intitulat "Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice" al titlului VII "Infracţiuni contra siguranţei publice" din Partea specială a Codului penal, obligaţie ce rezultă din prevederile art. 267 din Codul penal ce reglementează omisiunea sesizării.*";

- paragr. 112: "*Cu privire la elementul constitutiv al contravenţiei prevăzute la art. 48 alin. (1) lit. c) din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, acesta constă în faptele de nerespectare de către furnizorii de servicii de securitate cibernetică a obligaţiei de a pune la dispoziţia autorităţilor prevăzute la art. 10 din aceeaşi lege a datelor şi informaţiilor privind incidente, ameninţări, riscuri sau vulnerabilităţi a căror manifestare poate afecta o reţea sau un sistem informatic al deţinătorului sau al unor terţi, în condiţiile prevăzute de lege şi cu respectarea termenului reglementat la art. 25 alin. (1) din actul normativ criticat. Referitor la contravenţia anterior menţionată, Curtea constată că actul de punere la dispoziţie a datelor şi informaţiilor prevăzute în ipoteza normei ce reglementează această contravenţie se realizează, pe de o parte, în condiţiile art. 25 alin. (1) din legea criticată - în ceea ce priveşte termenele de notificare a incidentelor şi, respectiv, de comunicare a ameninţărilor, a riscurilor şi a vulnerabilităţilor - iar, pe de altă parte, în condiţiile art. 52 alin. (5) din aceeaşi lege - dispoziţie ce face trimitere la hotărârea Guvernului care urmează să prevadă normele metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din legea criticată. Aşadar, conduita sancţionată prin dispoziţiile art. 48 alin. (1) lit. c) din Legea privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative constă în necomunicarea, respectiv nepunerea la dispoziţia autorităţilor prevăzute la art. 10 din legea criticată a incidentelor şi, respectiv, a ameninţărilor, riscurilor şi vulnerabilităţilor, în termenele prevăzute la art. 25 alin. (1) din legea analizată, în condiţiile ce vor fi prevăzute prin hotărâre a Guvernului*";

Cu toate acestea, există o lacună în ceea ce priveşte reglementarea specifică a procedurilor de solicitare şi comunicare a acestor date şi informaţii. În prezent, nu există un mecanism clar şi uniform pentru solicitarea şi comunicarea acestor date şi informaţii, ceea ce poate duce la întârzieri în aplicarea legii, ineficienţe şi riscuri de securitate.

În plus, protecţia datelor cu caracter personal şi respectarea drepturilor fundamentale, precum dreptul la viaţă privată, secretul corespondenţei şi libertatea de exprimare, constituie un aspect central în cadrul oricărei activităţi de procesare a datelor şi informaţiilor.

Lipsa de claritate şi uniformitate în ceea ce priveşte procedurile de solicitare şi comunicare a datelor şi informaţiilor, precum şi de garanţii specifice privind respectarea drepturilor fundamentale, pot duce la incertitudini, posibile încălcări ale legii şi riscuri de securitate.

Experienţa altor state membre ale Uniunii Europene arată că reglementarea clară şi uniformă a acestor proceduri, precum şi stabilirea unor garanţii specifice privind respectarea drepturilor fundamentale, pot contribui semnificativ la eficienţa şi securitatea activităţilor de securitate cibernetică.

Prin urmare, se impune reglementarea unei proceduri clare și uniforme de solicitare și comunicare a datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023, precum și stabilirea unor garanții specifice privind respectarea drepturilor fundamentale.

Această reglementare va contribui la creșterea eficienței și securității activităților de securitate cibernetică, la asigurarea respectării drepturilor fundamentale și la consolidarea cadrului juridic de funcționare a furnizorilor de servicii tehnice de securitate cibernetică. Prin urmare, adoptarea prezentului proiect de hotărâre a Guvernului este necesară și oportună pentru a aborda aceste probleme, pentru a asigura un cadru clar, uniform și eficient pentru solicitarea și comunicarea datelor și informațiilor în domeniul securității cibernetice, precum și pentru a proteja drepturile fundamentale ale persoanelor fizice și juridice.

2.3. Schimbări preconizate

În contextul evoluției tehnologice și a amplificării amenințărilor la adresa securității cibernetice, este evident că procedurile existente în prezent sunt insuficiente pentru a face față provocărilor curente. Prin urmare, este esențială reglementarea clară și uniformă a solicitării și comunicării datelor și informațiilor între autoritățile menționate la art. 10 din *Legea nr. 58/2023* și furnizorii de servicii tehnice de securitate cibernetică.

Proiectul de hotărâre stabilește normele metodologice pentru solicitarea și comunicarea datelor și informațiilor relevante pentru securitatea cibernetică și reprezintă un important pas înainte în implementarea efectivă a Legii nr. 58/2023. Prin intermediul acestui proiect, se clarifică procesul de solicitare și comunicare a datelor și informațiilor, se stabilesc criteriile pentru evaluarea gravității incidentelor de securitate cibernetică și se formalizează procesul de notificare a acestora.

Proiectul de hotărâre prevede faptul că solicitarea datelor și informațiilor relevante pentru securitatea cibernetică se va realiza de către autoritățile enumerate la art. 10 din *Legea nr. 58/2023*, iar furnizorii de servicii de securitate cibernetică vor avea obligația de a răspunde acestor solicitări. Este important de menționat că solicitarea nu vizează date cu caracter personal sau date de conținut, ci informații strict necesare pentru asigurarea securității cibernetice.

Proiectul de hotărâre introduce criterii clare pentru evaluarea gravității incidentelor de securitate cibernetică, în funcție de impactul acestora asupra funcționării normale a rețelelor și sistemelor informatice. Acest lucru va permite o abordare mai eficientă și mai obiectivă în gestionarea incidentelor.

Proiectul de hotărâre formalizează procesul de notificare a incidentelor de securitate cibernetică, stabilind termenele în care acestea trebuie raportate către autoritățile competente. De asemenea, se oferă un cadru clar cu privire la tipul de informații care trebuie să fie incluse în aceste notificări.

Punerea în aplicare a acestor norme metodologice va aduce mai multă claritate şi va eficientiza procesul de gestionare a securităţii cibernetice în România. Aceasta va asigura un nivel mai ridicat de protecţie pentru reţelele şi sistemele informatice, va îmbunătăţi capacitatea de răspuns în cazul incidentelor de securitate cibernetică şi va contribui la dezvoltarea unui mediu cibernetic mai sigur pentru toţi utilizatorii.

Proiectul introduce un sistem mai riguros de notificare a incidentelor de securitate, cu termene bine definite şi proceduri clare. Autorităţile vor putea astfel să ia măsuri prompte şi eficiente pentru a contracara ameninţările la securitatea cibernetică, limitând potenţialul daunelor.

Proiectul prevede reguli stricte privind protecţia datelor cu caracter personal şi a secretului corespondenţei. În acest sens, prevederile proiectului vizează asigurarea unui echilibru între nevoia de securitate cibernetică şi respectarea drepturilor fundamentale ale individului. Proiectul reglementează modul de colaborare între autorităţi şi furnizorii de servicii tehnice de securitate cibernetică, bazat pe transparenţă, responsabilitate şi cooperare activă. Astfel, se urmăreşte crearea unui mediu propice pentru îmbunătăţirea constantă a securităţii cibernetice, promovând un dialog deschis şi un schimb de informaţii rapid şi eficient.

În lumina jurisprudenţei Curţii Constituţionale a României, normele metodologice propuse prin proiectul de hotărâre a Guvernului respectă cu stricteţe principiile reţinute în Decizia nr. 70/2023, corespunzând cu preocuparea pentru protecţia datelor personale şi respectarea vieţii private, conform exigenţelor constituţionale. Prezentul argument se bazează pe următoarele puncte de vedere:

a) **Colectarea şi accesul la date:** În concordanţă cu paragr. 84 din cuprinsul Deciziei, normele metodologice clarifică faptul că scopul sistemelor de notificare nu constă în colectarea datelor de conţinut, nici în extragerea unilaterală şi fără autorizare de date şi informaţii de pe un sistem informatic. Aceste sisteme de notificare se bazează pe comunicarea unor date strict necesare gestionării şi contracarării incidentelor de securitate cibernetică, fără a aduce atingere drepturilor şi libertăţilor fundamentale ale cetăţenilor.
b) **Respectarea sarcinilor operatorilor:** În concordanţă cu paragr. 92 din cuprinsul Deciziei, normele metodologice respectă şi întăresc obligaţiile care revin operatorilor de servicii esenţiale (OSE) şi furnizorilor de servicii digitale (FSD) în privinţa furnizării de informaţii suplimentare cu privire la incidentele de securitate cibernetică. Acestea subliniază necesitatea furnizării de informaţii detaliate, dar fără a include date clasificate sau care ar putea aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi.
c) **Operaţiuni strict tehnice:** În concordanţă cu paragr. 93 din cuprinsul Deciziei, normele metodologice respectă principiul potrivit căruia obligaţiile furnizorilor de servicii tehnice de securitate cibernetică sunt strict tehnice şi nu au drept scop colectarea datelor cu caracter personal. Aceste obligaţii sunt menite să asigure un climat de securitate cibernetică, conform prevederilor capitolului IX din *Legea nr.*

58/2023, referitoare la confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice.

d) **Respectarea legii penale:** În concordanță cu paragr. 96 din cuprinsul Deciziei, normele metodologice confirmă faptul că furnizorii de servicii tehnice de securitate cibernetică au obligația de a sesiza organele de urmărire penală, în cazul în care constată comiterea unor fapte prevăzute de legea penală.

e) **Sancțiuni pentru neconformitate**: În concordanță cu paragr. 112 din cuprinsul Deciziei, normele metodologice clarifică și stabilesc obligațiile furnizorilor de servicii de securitate cibernetică și consecințele juridice ale nerespectării acestor obligații. Mai exact, acestea evidențiază faptul că nerespectarea obligațiilor prevăzute la art. 25 alin. (1) din *Legea nr. 58/2023*, de către furnizorii de servicii de securitate cibernetică, poate duce la sancțiuni. Aceste obligații presupun comunicarea în timp util a datelor și informațiilor relevante privind incidente, amenințări, riscuri sau vulnerabilități care pot afecta o rețea sau un sistem informatic.

f) **Respectarea termenelor și a condițiilor legale:** În concordanță cu paragr. 112, normele metodologice precizează că furnizorii de servicii de securitate cibernetică trebuie să respecte termenele de notificare și comunicare stabilite prin lege, precum și condițiile ce vor fi stabilite prin hotărârea de guvern, pentru a evita sancțiunile. Acest lucru subliniază respectul pentru reglementările legale și înțelegerea importanței securității cibernetice în societatea contemporană.

2.4. Alte informaţii*)

Nu este cazul

Secţiunea a 3-a

Impactul socioeconomic**)

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

O implementare corectă și eficientă a noilor norme va conduce la o protecție sporită a sistemelor cibernetice, diminuând riscul de incidente de securitate. Acest lucru va aduce beneficii la nivelul societății, prin protejarea datelor și informațiilor cetățenilor, și la nivelul economiei, prin protejarea infrastructurilor critice. Normele metodologice aduc claritate în procesul de solicitare și comunicare a datelor și informațiilor relevante pentru securitatea cibernetică, făcându-l mai previzibil pentru toți actorii implicați. Prin stabilirea unui proces clar de notificare a incidentelor de securitate cibernetică, autoritățile vor fi capabile să răspundă mai rapid și mai eficient în cazul unor astfel de incidente.

Implementarea noilor norme va implica costuri administrative, deoarece furnizorii de servicii de securitate cibernetică vor trebui să se adapteze la noile reguli, să pregătească proceduri interne și să instruiască personalul. Autoritățile vor trebui, de asemenea, să își ajusteze procedurile de gestionare a incidentelor de securitate cibernetică. Furnizorii de servicii de securitate cibernetică vor trebui să îndeplinească obligațiile prevăzute de noile norme, ceea ce ar putea implica investiții în infrastructura tehnologică sau în resurse umane.

În concluzie, deși există costuri asociate cu implementarea acestui act normativ, beneficiile în ceea ce privește protecția sporită a securității cibernetice, claritatea procedurilor și reacția eficientă în fața incidentelor de securitate cibernetică par să justifice aceste costuri. În plus, pe termen lung, acest act normativ ar putea conduce la economii, prin prevenirea unor incidente costisitoare de securitate cibernetică.

3.2. Impactul social

În evaluarea impactului social pozitiv al proiectului de hotărâre a Guvernului, trebuie luat în considerare faptul că securitatea cibernetică este relevantă atât pentru mediul de afaceri și instituțiile guvernamentale, cât și pentru viața de zi cu zi a cetățenilor.

Apropierea neîntreruptă de digitalizare a societății face ca oamenii să devină tot mai dependenți de tehnologie pentru efectuarea sarcinilor de bază, cum ar fi cumpărăturile, plata facturilor, lucrul de la distanță sau interacțiunea cu administrația publică. Prin urmare, siguranța mediului cibernetic este crucială pentru a asigura o funcționare normală a vieții de zi cu zi. Implementare proiectului de hotărâre a Guvernului va contribui la crearea unui mediu cibernetic mai sigur, reducând riscul de incidente care ar putea perturba aceste activități.

Pe de altă parte, proiectul de hotărâre a Guvernului ar putea avea un impact pozitiv asupra protecției datelor personale ale cetățenilor. În era digitală, protecția datelor a devenit o preocupare majoră pentru societate, în contextul în care incidentele de securitate cibernetică pot duce la scurgeri de date personale cu consecințe grave. Prin crearea unui mediu mai sigur și prin instituirea unui proces clar de notificare a incidentelor, proiectul de hotărâre va contribui la protecția datelor personale ale cetățenilor, sporind încrederea acestora în mediul digital.

În plus, proiectul de hotărâre a Guvernului conduce la creșterea gradului de conștientizare cu privire la importanța securității cibernetice în societate. Prin instituirea unor reguli clare și a unui proces de notificare a incidentelor, acest proiect de hotărâre poate contribui la educarea publicului larg despre riscurile securității cibernetice și despre modalitățile de a le preveni.

În concluzie, proiectul de hotărâre a Guvernului are un impact social pozitiv semnificativ, prin contribuția sa la crearea unui mediu cibernetic mai sigur, la protecția datelor personale și la creșterea gradului de conștientizare cu privire la importanța securității cibernetice.

3.3. Impactul asupra drepturilor şi libertăţilor fundamentale ale omului

Proiectul de hotărâre a Guvernului privind securitatea cibernetică şi raportarea incidentelor cibernetice are o serie de implicaţii potenţiale asupra drepturilor şi libertăţilor fundamentale ale omului. Analiza acestei teme necesită un echilibru delicat între nevoia de securitate în spaţiul digital şi protejarea libertăţilor fundamentale, cum ar fi dreptul la viaţă privată şi la protecţia datelor personale.

Pentru a înţelege acest echilibru, este util să ne referim la jurisprudenţa naţională şi internaţională existentă, precum şi la doctrinele juridice relevante. În cadrul Uniunii Europene, de exemplu, Curtea de Justiţie a Uniunii Europene (CJUE) a abordat în mod constant aceste probleme în deciziile sale. În decizia **Digital Rights Ireland din 2014,** CJUE a invalidat Directiva privind retenţia datelor din 2006, pe motiv că aceasta încălca drepturile la respectarea vieţii private şi la protecţia datelor personale. Acest caz a pus în evidenţă necesitatea ca orice măsură de securitate cibernetică să fie proporţională şi necesară şi să respecte principiul minimizării datelor.

În mod similar, în jurisprudenţa Curţii Europene a Drepturilor Omului (CEDO), se constată o atenţie constantă faţă de aceste probleme. În cazul *Big Brother Watch şi alţii vs. Regatul Unit,* CEDO a statuat că practicile de supraveghere în masă ale guvernului britanic încălcaseră articolele 8 (dreptul la respectarea vieţii private şi familiale) şi 10 (libertatea de exprimare) din Convenţia Europeană a Drepturilor Omului. Aceste hotărâri subliniază că orice reglementare în domeniul securităţii cibernetice trebuie să se desfăşoare într-un cadru care respectă drepturile şi libertăţile fundamentale.

Evaluarea impactului asupra drepturilor şi libertăţilor fundamentale în contextul securităţii cibernetice poate fi susţinută de precedentele stabilite atât de Curtea Europeană a Drepturilor Omului (CEDO) cât şi de Curtea de Justiţie a Uniunii Europene (CJUE).

CEDO - Klass şi alţii împotriva Germaniei, 1978: În acest caz, Curtea a stabilit că interceptarea comunicaţiilor nu este în sine incompatibilă cu Convenţia Europeană a Drepturilor Omului, atât timp cât există garanţii legale adecvate împotriva abuzului. Aceasta a recunoscut necesitatea unui echilibru între dreptul la respectarea vieţii private şi necesitatea de a proteja securitatea naţională.

CEDO - S. şi Marper împotriva Regatului Unit, 2008: Aceasta a fost o cauză emblematică privind reţinerea datelor. Curtea a decis că reţinerea indefinită a datelor biometrice (ADN şi amprente) ale persoanelor nevinovate constituie o violare a dreptului la respectarea vieţii private. Acest precedent evidenţiază necesitatea de a avea reglementări clare şi limitări stricte cu privire la reţinerea şi utilizarea datelor, chiar şi în contextul securităţii naţionale.

CJUE - Cauza Digital Rights Ireland, 2014: Aceasta a fost o decizie crucială în care Curtea a invalidat Directiva privind reţinerea datelor (2006/24/CE) a Uniunii Europene. Curtea a considerat că directiva a încălcat drepturile la respectarea vieţii private şi la protecţia datelor

personale, deoarece a permis reținerea largă și nediferențiată a datelor. Acest caz subliniază necesitatea de a avea o abordare proporțională și necesară în reglementările de securitate cibernetică.

Toate aceste cazuri indică faptul că securitatea cibernetică și protecția datelor sunt importante, însă măsurile luate în scopul asigurării acestora nu trebuie să încalce drepturile fundamentale. Prin urmare, proiectul de hotărâre a Guvernului încorporează aceste principii și oferă garanții adecvate pentru protejarea drepturilor individuale.

Prin reglementările propuse, proiectul de hotărâre a Guvernului va asigura respectarea acestor principii juridice recunoscute. Acesta prevede măsuri care vizează îmbunătățirea securității cibernetice, dar în același timp respectă drepturile fundamentale ale indivizilor. Procesul de raportare a incidentelor cibernetice este proiectat să fie transparent și responsabil, într-o manieră care respectă dreptul la viață privată și protecția datelor personale. Astfel, proiectul de hotărâre a Guvernului încearcă să echilibreze securitatea cibernetică cu protecția drepturilor fundamentale ale omului, reflectând în mod corespunzător tendințele actuale în jurisprudența națională și internațională.

În plus, pe măsura implementării proiectului, va fi important să se asigure o comunicare deschisă și transparentă cu publicul și cu toate părțile interesate, inclusiv cu industria IT, cu organizațiile din domeniul drepturilor omului și cu societatea civilă, în general. Aceasta va contribui la menținerea încrederii în sistem, iar toți cei implicați vor înțelege scopul și modul de funcționare al acestuia.

În concluzie, proiectul de hotărâre a Guvernului reprezintă un pas important în creșterea securității cibernetice și a conștientizării publicului asupra importanței acesteia. În același timp, se respectă necesitatea unei abordări proporționale și necesare, asigurându-se că sunt luate în considerare drepturile și libertățile fundamentale ale omului.

3.4. Impactul macroeconomic

Într-o eră în care economiile lumii sunt tot mai digitalizate și interconectate, securitatea cibernetică a devenit o componentă crucială a stabilității macroeconomice. Proiectul de hotărâre a Guvernului, prin instituirea unui cadrul normativ riguros pentru protejarea datelor și a informațiilor, are potențialul de a exercita un impact macroeconomic semnificativ.

În primul rând, măsurile de securitate cibernetică cresc încrederea actorilor economici în mediul digital, ceea ce poate stimula investițiile și activitatea economică. Conform unui studiu realizat de Deloitte în 2020, firmele care investesc în securitate cibernetică pot experimenta o creștere a valorii lor de piață cu până la 7%. Această creștere se datorează în mare parte percepției mai bune a investitorilor și a consumatorilor cu privire la securitatea datelor și a informațiilor. Prin urmare, un cadrul normativ solid în domeniul securității cibernetice poate contribui la creșterea generală a economiei.

În al doilea rând, securitatea cibernetică joacă un rol vital în prevenirea și gestionarea riscurilor financiare. Un atac cibernetic poate costa companiile milioane de dolari în pierderi directe și poate avea efecte dăunătoare asupra reputației unei companii. De exemplu, conform raportului Costul unui Atac Cibernetic realizat de Institutul Ponemon, costul mediu al unui atac cibernetic se ridica la 4 milioane de dolari în 2019. Proiectul de hotărâre a Guvernului, prin promovarea unui ecosistem cibernetic mai sigur, poate contribui la atenuarea acestor riscuri, contribuind astfel la stabilitatea macroeconomică.

În al treilea rând, prin crearea unui cadru normativ pentru securitatea cibernetică, Guvernul poate stimula inovarea și creșterea în sectoarele tehnologiei informației și comunicațiilor. Investițiile în securitatea cibernetică pot duce la crearea de locuri de muncă și la creșterea productivității în sectoarele legate de tehnologia digitală.

În concluzie, securitatea cibernetică nu este doar o chestiune de securitate națională, ci și o componentă vitală a prosperității economice. Proiectul de hotărâre a Guvernului, prin îmbunătățirea securității cibernetice, poate avea un impact pozitiv semnificativ asupra economiei naționale.

3.4.1. Impactul asupra economiei și asupra principalilor indicatori macroeconomici

Securitatea cibernetică și economia digitală sunt împletite într-un mod atât de strâns încât este dificil să discutăm despre una fără cealaltă. Impactul reglementărilor privind securitatea cibernetică asupra economiei și a principalilor indicatori macroeconomici poate fi vizualizat prin intermediul a trei categorii principale: productivitatea economică, creșterea ocupării forței de muncă și stabilitatea financiară.

În ceea ce privește productivitatea, adoptarea măsurilor de securitate cibernetică prin proiectul de hotărâre a Guvernului poate avea un impact semnificativ asupra eficienței economice. În România, contribuția tehnologiei informației și a comunicațiilor (TIC) la PIB a fost de aproximativ 6% în 2022, potrivit Institutului Național de Statistică. Într-un mediu digital sigur, companiile pot explora în continuare tehnologia digitală pentru a-și crește eficiența operațională, ceea ce poate duce la o creștere a productivității generale a economiei.

În plus, securitatea cibernetică poate duce la crearea de noi locuri de muncă. În prezent, sectorul IT din România este unul dintre cele mai dinamice sectoare ale economiei, cu o creștere anuală a ocupării forței de muncă de aproximativ 10%. Implementarea unui cadru legislativ solid în acest domeniu poate încuraja companiile să investească și mai mult în securitatea cibernetică, creând astfel noi oportunități de angajare și contribuind la reducerea ratei șomajului.

De asemenea, în ceea ce privește stabilitatea financiară, securitatea cibernetică este esențială pentru menținerea încrederii în sistemul financiar. Potrivit Băncii Naționale a României, atacurile cibernetice reprezintă una dintre cele mai mari amenințări la adresa stabilității financiare. Prin implementarea reglementărilor propuse de proiectul de hotărâre a Guvernului,

se poate reduce riscul de pierderi financiare majore datorate atacurilor cibernetice, protejând astfel stabilitatea financiară şi îmbunătăţind încrederea în economie.

Concluzionând, prin prisma principalilor indicatori macroeconomici, proiectul de hotărâre a Guvernului va avea un impact pozitiv asupra economiei româneşti, prin îmbunătăţirea productivităţii, crearea de locuri de muncă şi protejarea stabilităţii financiare.

3.4.2. Impactul asupra mediului concurenţial şi domeniul ajutoarelor de stat

Nu este cazul.

3.5. Impactul asupra mediului de afaceri

Impactul asupra mediului de afaceri al proiectului de hotărâre a Guvernului care reglementează securitatea cibernetică poate fi considerabil şi divers, implicând atât companiile de tehnologie informatică, cât şi organizaţiile din alte industrii care se bazează pe tehnologia digitală pentru operarea lor de zi cu zi.

În primul rând, securitatea cibernetică este un aspect fundamental al mediului de afaceri modern. Companiile operează într-un peisaj digital tot mai complex, cu o dependenţă tot mai mare de tehnologie, date şi servicii în cloud. În acest context, securitatea cibernetică nu este doar o problemă tehnică, ci şi una strategică. Un cadru legislativ robust, aşa cum este cel propus de Guvernul României, poate ajuta organizaţiile să înţeleagă mai bine riscurile la care se expun şi cum să le gestioneze eficient.

Proiectul de hotărâre a Guvernului poate contribui, de asemenea, la crearea unui mediu de afaceri mai sigur pentru companii, ceea ce este esenţial pentru încrederea clienţilor şi partenerilor de afaceri. Astfel, se va crea un climat de afaceri mai atractiv pentru investitori, având în vedere importanţa crescândă pe care o acordă securitatea cibernetică în deciziile lor de investiţii.

În plus, reglementările privind securitatea cibernetică conduc la apariţia de noi oportunităţi de afaceri. Pentru furnizorii de soluţii de securitate cibernetică, aceasta vor însemna o creştere a cererii de servicii, deoarece mai multe organizaţii se străduiesc să respecte noile reglementări. Pentru companiile din alte industrii, aceasta ar putea oferi oportunităţi pentru a îmbunătăţi operaţiunile existente sau pentru a crea noi servicii care să profite de avantajele oferite de un mediu digital mai sigur.

În concluzie, proiectul de hotărâre a Guvernului va avea un impact pozitiv asupra mediului de afaceri prin crearea unui climat mai sigur şi mai atractiv pentru investitori, îmbunătăţirea gestionării riscurilor cibernetice şi stimularea apariţiei de noi oportunităţi de afaceri.

3.6. Impactul asupra mediului înconjurător

Nu este cazul.

3.7. Evaluarea costurilor şi beneficiilor din perspectiva inovării şi digitalizării

Implementarea unui cadrul de reglementare robust pentru securitatea cibernetică, aşa cum este propus prin proiectul de hotărâre a Guvernului, va avea un impact major asupra inovării şi digitalizării în România. Acest impact se poate manifesta într-o serie de moduri, fie că vorbim despre îmbunătăţirea încrederii consumatorilor în tehnologie, încurajarea investiţiilor în sectorul IT, sau stimularea dezvoltării de noi produse şi servicii în domeniul digital.

În privinţa costurilor, este de aşteptat ca implementarea acestui cadru să implice cheltuieli pentru organizaţii şi instituţii, în vederea conformării cu noile reguli. Aceste cheltuieli pot consta în costuri pentru achiziţia de noi tehnologii de securitate cibernetică, investiţii în formarea şi pregătirea personalului, sau costuri asociate cu evaluarea şi actualizarea constantă a practicilor de securitate cibernetică.

Pe de altă parte, beneficiile propuse de proiect sunt considerabile. Un mediu digital sigur va stimula încrederea consumatorilor şi a întreprinderilor de a utiliza şi de a investi în tehnologii digitale. Un studiu realizat de Comisia Europeană în 2020 a constatat că încrederea în economia digitală poate avea un impact semnificativ asupra creşterii economice. În plus, măsurile de securitate cibernetică mai stricte vor încuraja dezvoltarea şi adoptarea de noi tehnologii şi servicii de securitate, stimulând astfel inovarea în sectorul IT.

Mai mult, în contextul în care digitalizarea este o prioritate la nivel global, acest proiect de hotărâre ar putea plasa România în poziţia de lider în materie de securitate cibernetică în regiune. Într-un raport al Băncii Mondiale din 2021, se subliniază că digitalizarea poate stimula productivitatea, creşterea economică şi crearea de locuri de muncă.

Crescând nivelul de securitate cibernetică, acest proiect asigură cadrul de reglementare necesar pentru a atrage mai multe investiţii în tehnologiile digitale din România, permiţând astfel creşterea competitivităţii şi inovaţiei în acest domeniu. Un raport al Organizaţiei pentru Cooperare şi Dezvoltare Economică (OCDE) din 2022 a evidenţiat că securitatea cibernetică poate influenţa semnificativ inovaţia, întrucât aceasta este o condiţie prealabilă pentru dezvoltarea şi adoptarea de noi tehnologii.

În ceea ce priveşte costurile, acestea pot fi privite ca o investiţie necesară pentru a crea un mediu digital sigur şi încrezător, care la rândul său poate genera beneficii economice pe termen lung. Deşi costurile iniţiale pot fi semnificative, pot fi compensate de beneficiile pe termen lung, inclusiv creşterea încrederii în economia digitală, stimularea investiţiilor în sectorul IT şi creşterea competitivităţii economiei româneşti. În acest sens, un studiu din 2022 al McKinsey Global Institute a arătat că ţările care investesc în securitatea cibernetică pot beneficia de un avantaj competitiv semnificativ în economia digitală globală. Acest avantaj

poate contribui la creşterea productivităţii, crearea de noi locuri de muncă şi dezvoltarea de noi industrii şi servicii în domeniul digital.

Aşadar, evaluând costurile şi beneficiile din perspectiva inovării şi digitalizării, se poate concluziona că acest proiect de hotărâre poate avea un impact pozitiv semnificativ asupra economiei digitale din România. Prin consolidarea securităţii cibernetice, proiectul poate contribui la stimularea inovării şi la creşterea competitivităţii economiei româneşti în era digitală.

3.8. Evaluarea costurilor şi beneficiilor din perspectiva dezvoltării durabile

Ca aspect al dezvoltării durabile, securitatea cibernetică a devenit un subiect de discuţie la nivel global. Într-o lume în care tot mai multe activităţi se desfăşoară în mediul digital, asigurarea unui spaţiu cibernetic sigur este esenţială pentru atingerea obiectivelor de dezvoltare durabilă. Prin urmare, proiectul de hotărâre poate fi considerat o contribuţie semnificativă la dezvoltarea durabilă a României.

În ceea ce priveşte costurile, acestea pot fi privite ca investiţii necesare pentru dezvoltarea durabilă. Asigurarea unui spaţiu cibernetic sigur poate necesita resurse semnificative în termen de capital, personal şi tehnologie. Cu toate acestea, aceste costuri pot fi considerate o investiţie necesară pentru a construi o infrastructură cibernetică robustă care poate rezista la atacuri şi perturbări, contribuind astfel la reziliența economică şi socială pe termen lung.

Pe de altă parte, beneficiile unui spaţiu cibernetic mai sigur sunt multiple şi se extind dincolo de sfera economică. În primul rând, securitatea cibernetică poate contribui la protejarea drepturilor şi libertăţilor fundamentale în era digitală, inclusiv dreptul la viaţă privată şi la protecţia datelor. În al doilea rând, securitatea cibernetică poate promova incluziunea digitală prin creşterea încrederii utilizatorilor în serviciile digitale. În al treilea rând, un spaţiu cibernetic sigur poate stimula inovarea şi competitivitatea în economia digitală, contribuind astfel la creşterea economică durabilă.

Un studiu publicat în 2022 de World Economic Forum a arătat că ţările care investesc în securitatea cibernetică pot beneficia de o creştere economică mai durabilă, datorită îmbunătăţirii încrederii în serviciile digitale şi a stimulării inovării în economia digitală. Studiul a evidenţiat, de asemenea, că o abordare integrată a securităţii cibernetice, care include participarea tuturor părţilor interesate, poate contribui la crearea unui mediu digital inclusiv şi sigur.

În concluzie, proiectul de hotărâre contribuie semnificativ la dezvoltarea durabilă a României prin consolidarea securităţii cibernetice. În ciuda costurilor iniţiale, beneficiile pe termen lung ale unui spaţiu cibernetic sigur pot fi semnificative şi pot contribui la atingerea obiectivelor de dezvoltare durabilă ale României.

3.9. Alte informaţii
Nu este cazul.

Secţiunea a 4-a

Impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani), inclusiv informaţii cu privire la cheltuieli şi 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:						
1. buget de stat, din acesta: 1. impozit pe profit 2. impozit pe venit						
1. bugete locale 1. impozit pe profit						
1. bugetul asigurărilor sociale de stat: 1. contribuţii de asigurări						

d) alte tipuri de venituri (Se va menţiona natura acestora.)						
4.2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						
1. buget de stat, din acesta: 1. cheltuieli de personal 2. bunuri şi servicii						
1. bugete locale: 1. cheltuieli de personal 2. bunuri şi servicii						
1. bugetul asigurărilor sociale de stat: 1. cheltuieli de personal 2. bunuri şi servicii						
d) alte tipuri de cheltuieli (Se va menţiona natura acestora.)						
4.3. Impact financiar, plus/minus, din care: a) buget de stat						
b) bugete locale						
4.4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
4.5. Propuneri pentru a compensa reducerea veniturilor bugetare						

4.6. Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare						

4.7. Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente:

1. fişa financiară prevăzută la art. 15 din Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, însoţită de ipotezele şi metodologia de calcul utilizată;

Nu este cazul

2. declaraţie conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi priorităţile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.

Nu este cazul

4.8. Alte informaţii

Proiectul de act administrativ cu caracter normativ nu are impact financiar- bugetar.

Secţiunea a 5-a

Efectele proiectului de act normativ asupra legislaţiei în vigoare

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 legislaţia 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

Nu este cazul.

Secţiunea a 6-a

Consultările efectuate în vederea elaborării proiectului de act normativ

6.1. Informaţii privind neaplicarea procedurii de participare la elaborarea actelor normative

Nu este cazul.

6.2. Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate

Nu este cazul.

6.3. Informaţii despre consultările organizate cu autorităţile administraţiei publice locale

Nu este cazul.

6.4. Informaţii privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative

Nu este cazul.

6.5. Informaţii privind avizarea de către:

a) Consiliul Legislativ - Se solicită avizul Consiliului Legislativ

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

c) Consiliul Economic şi Social - Se solicită avizul Consiliului Economic şi Social

d) Consiliul Concurenţei -

e) Curtea de Conturi

Secţiunea a 7-a

Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ

7.1. Informarea societăţii civile cu privire la elaborarea proiectului de act normativ

Pentru proiectul de act normativ a fost îndeplinită procedura stabilită prin dispozițiile Legii nr. 52/2003 privind transparenţa decizională în administraţia publică, republicată.

Necesitatea unui termen de consultare publică mai scurt în cadrul proiectului de hotărâre de guvern în materie de securitate cibernetică se impune, în principal, din cauza situației actuale în domeniul securității cibernetice, atât în România, cât şi la nivel global.

În primul rând, trebuie subliniat faptul că amenințările cibernetice au devenit tot mai prezente şi sofisticate în ultimii ani. Atacurile cibernetice împotriva instituțiilor guvernamentale, companiilor private şi persoanelor cresc în număr şi în intensitate, punând în pericol securitatea națională, economia şi drepturile şi libertățile individuale ale cetăţenilor. Acest fapt

este bine documentat de numeroase rapoarte naţionale şi internaţionale, inclusiv de către Directoratul Național pentru Securitate Cibernetică şi de către Europol.

În al doilea rând, situația actuală în materie de securitate cibernetică în România impune adoptarea de soluții imediate. În prezent, există lacune semnificative în cadrul legislativ și în capacitatea instituțiilor responsabile de a face față amenințărilor cibernetice. Aceste lacune pot duce la o vulnerabilitate crescută în fața atacurilor cibernetice, ceea ce poate avea consecințe grave asupra interesului public.

În acest context, proiectul de hotărâre a Guvernului este menit să răspundă acestor provocări prin stabilirea unui cadru mai solid și mai eficient pentru gestionarea securității cibernetice. Cu toate acestea, având în vedere gravitatea situației și nevoia urgentă de a răspunde la aceste amenințări, este necesară adoptarea proiectului într-un termen mai scurt decât cel obișnuit.

Prin urmare, având în vedere situația urgentă și excepțională în materie de securitate cibernetică și necesitatea adoptării de soluții imediate pentru a evita o gravă atingere adusă interesului public, proiectul de hotărâre a Guvernului respectă criteriile de excepție prevăzute la art. 7 alin. (13) Legea nr. 52/2003 și, în consecință, poate fi supus adoptării și anterior expirării termenului prevăzut de alin. (2).

Prezentul proiect este supus consultării publice potrivit prevederilor art. 7 alin. (13) din Legea nr. 52/2003, termenul de punere în procedura de consultare publică fiind de 10 zile lucrătoare.

7.2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice

Nu este cazul.

Secţiunea a 8-a

Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ

8.1. Măsurile de punere în aplicare a proiectului de act normativ

Nu este cazul.

8.2. Alte informaţii

Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) 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

SEBASTIAN-IOAN BURDUJA

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) 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.

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL AFACERILOR INTERNE
LUCIAN NICOLAE BODE

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
EDUARD RAUL HELLVIG

DIRECTORUL
SERVICIULUI DE PROTECȚIE 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

MINISTRUL INVESTIȚIILOR ȘI
PROIECTELOR EUROPENE
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
BOGDAN LUCIAN AURESCU

MINISTRUL FINANȚELOR
ADRIAN CÂCIU

MINISTRUL JUSTIȚIEI
MARIAN-CĂTĂLIN PREDOIU

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