NOTĂ DE FUNDAMENTARE

Secțiunea 1 Titlul proiectului de act normativ Hotărâre a Guvernului privind aprobarea Strategiei de Securitate Cibernetică a României și a Planului de Acțiune 2021-2026	
Secțiunea a 2-a **Motivul emiterii actului normativ**	
1. Descrierea situației actuale	Creșterea gradului de digitalizare și conectivitate atât la nivelul României, al Uniunii Europene, dar și la nivel global, duce la o serie de beneficii majore dar și la o agravare a riscurilor de securitate cibernetică, societatea și economia devenind astfel mai vulnerabile la amenințările cibernetice. Se amplifică amenințările cibernetice persistente orchestrate de actori statali și non-statali ce vizează instituții ale statului, operatori economici și infrastructuri cibernetice naționale din transport, sănătate, energie, sectorul financiar-bancar, apă potabilă, servicii poștale și de curierat, termoficare, infrastructurile digitale, industria chimică și farmaceutică, administrația publică centrală și locală, cât și persoane private, riscând, prin toate acestea, să pună în pericol buna funcționare a societății românești în ansamblul său, precum și din perspectiva apartenenței României la structurile Uniunii Europene. La nivel național, amenințarea cibernetică se situează în prezent pe un trend ascendent și susținut, principala provocare la adresa securității cibernetice fiind reprezentată de atacurile cibernetice derulate de entități asociate unor actori statali, de grupări de criminalitate cibernetică, precum și de grupări de hackeri cu motivație ideologică, politică sau extremist-teroristă. Amploarea, frecvența, complexitatea și impactul incidentelor de securitate cibernetică sunt într-o creștere constantă și reprezintă o amenințare gravă pentru funcționarea infrastructurilor, a rețelelor și a sistemelor informatice, atât la nivelul României cât și la nivelul Uniunii Europene, cu impact major la adresa securității naționale, societății și economiei. Toate aceste amenințări de natură cibernetică necesită un răspuns determinat, decisiv, coordonat și coerent la nivelul instituțiilor competente ale statului român. Mai mult, în ultima perioadă, numărul și amploarea incidentelor de securitate cibernetică observate la nivelul țării au crescut continuu, iar situația de criză generată de răspândirea virusului SARS-COV-2 a scos în evidență și mai mult acest lucru. Consecințele atacurilor și incidentelor cibernetice se reflectă asupra tuturor sectoarelor importante pentru statul român și pot genera pierderi majore ori chiar pot conduce la materializarea unor riscuri severe la adresa securității naționale. În aceste condiții, securitatea și reziliența infrastructurilor, a rețelelor și a sistemelor informatice trebuie incluse în prioritățile statului român,

	inclusiv prin eforturi determinate de actualizare şi dezvoltare permanentă a cadrului normativ şi instituţional pe componenta gestionării riscurilor şi a contracarării ameninţărilor şi atacurilor cibernetice, precum şi a asigurării securităţii cibernetice a României. De asemenea, se impune luarea în considerare a dinamicii evoluţiilor în domeniul societăţii digitale, precum şi a cerinţelor ridicate şi a necesităţilor Pieţei Unice Digitale la nivel european. Acestea necesită o abordare inovativă şi proactivă în ceea ce priveşte măsurile de securitate cibernetică în totalitatea lor, normativ şi tehnic, pentru a asigura încrederea, funcţionalitatea, reziliența şi eficienţa acestora. Decizia din decembrie 2020 a UE de găzduire la Bucureşti a Centrului de competenţe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică este un element suplimentar ce solicită o nouă viziune şi abordare la nivel naţional în ceea ce priveşte strategia, obiectivele majore, prioritățile şi rolul României în domeniul securităţii cibernetice, al digitalizării, al cercetării şi inovării. Centrul va derula investiţiile viitoare ale Uniunii Europene şi va fi un catalizator al inovării, cercetării si colaborării din domeniul securităţii cibernetice şi va contribui decisiv la dezvoltarea ecosistemului în domeniu atât la nivel naţional, cât şi european. România urmăreşte o dezvoltare susţinută a unei societăţi si economii digitalizate, bazată pe interoperabilitate şi servicii specifice societăţii informaţionale, pe asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor, a datelor personale dar şi a intereselor de securitate naţională, într-un cadru legal adecvat. În contextul actual în continuă schimbare, România trebuie să aibă o strategie de securitate cibernetică flexibilă şi dinamică pentru a face faţă cu succes noilor provocări şi ameninţări. Hotărârea de Guvern nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului Naţional de Securitate Cibernetică a devenit depăşită în raport cu evoluţiile internaţionale în domeniul securităţii cibernetice în special în ceea ce priveşte viziunea, obiectivele, mecanismele de acţiune, colaborare şi cooperare, evoluţiile rapide din domeniu, precum şi în raport cu instituţiile create la nivelul UE sau cu obligaţiile şi responsabilităţile ce revin ţării noastre in raport cu UE, statele membre sau statele aliate on partenere. Strategia naţională în materie de securitate cibernetică este o caracteristică politică esenţială, aliniată pe deplin cu Strategia Naţională de Apărare a Ţării, ce stabileşte o serie de obiective şi priorităţi naţionale trebuie atinse într-un interval de timp pentru a îmbunătăţi, în ansamblu, securitatea cibernetică la nivelul României, ca parte a securităţii naţionale. Pe acest fond, Guvernul României consideră că este necesară actualizarea şi adoptarea unei noi Strategiei de Securitate Cibernetică a României care să permită o abordare adecvată şi adoptarea unei viziuni coerente şi moderne la nivel naţional, pentru a poziţiona ferm România la nivelul celor mai avansate state membre ale Uniunii Europene în domeniul securităţii cibernetice. Grupul de lucru inter-instituţional desemnat pentru pregătirea propunerii noii Strategii de Securitate Cibernetică şi a Planului de Acţiune 2021-2026 s-a constituit şi şi-a

	început activitatea efectiv la 16 octombrie 2020.
2. Schimbări preconizate	Prin propunerea de act normativ se urmăreşte aprobarea Strategiei de Securitate Cibernetică a României şi definirea, în vederea adoptării, a Planului de Acţiune 2021-2026 pentru atingerea obiectivelor strategice prin implementarea efectivă şi eficace a măsurilor şi principalelor acţiuni definite de către o serie de instituţii participante, vine în contextul unor măsuri şi decizii luate recent la nivel european. Printre acestea pot fi enumerate: noua strategie a de securitate cibernetică UE pentru decada digitală, propunerile de adoptare a Directivei NIS 2.0 şi a Directivei pentru reziliența entităților critice, ce evidenţiază atât preocupările intense şi interesul major manifestate de factorii de decizie strategici din UE faţă de complexitatea problematicii securităţii cibernetice, dar şi responsabilităţile crescute ce revin statelor membre, inclusiv României. Prezentul proiect de Strategie de Securitate Cibernetică a României este gândit a reprezenta documentul de bază pentru planificarea acţiunilor subsumate securităţii cibernetice a României, în acord cu documentele de natură strategică asumate până în prezent, îndeosebi cu Strategia Naţională de Apărare a Ţării. Strategia de Securitate Cibernetică este menită să consolideze deopotrivă securitatea cibernetică naţională, rolul României în plan regional, european şi internaţional şi să sprijine dezvoltarea un ecosistem digital performant, ca şi componentă cheie a societăţii şi economiei. Ea răspunde nevoilor de definire a unui cadru naţional de cooperare şi colaborare precum şi a obligaţiilor ce revin României din noua strategie europeană de securitate cibernetică pentru decada digitală. Principiile fundamentale reflectate în strategie sunt următoarele: 1. Securitatea cibernetică, parte integrantă a securităţii naţionale, este responsabilitatea tuturor actorilor implicaţi: entităţi publice, private şi cetăţeni. 2. Securitatea cibernetică sprijină funcţionarea statului şi a societăţii, creşterea competitivităţii economiei naţionale, dezvoltarea capabilităţilor naţionale de cercetare-dezvoltare şi inovare. 3. Securitatea cibernetică se bazează pe stabilirea unui cadru normativ adecvat. 4. Securitatea cibernetică este consolidată printr-o cooperare pragmatică la nivel internaţional. 5. În asigurarea securităţii cibernetice este garantată respectarea drepturilor şi libertăţilor fundamentale ale cetăţenilor, precum şi protejarea libertăţilor individuale şi a datelor cu caracter personal. În acest sens, sunt identificate cinci obiective majore de securitate cibernetică de o importanţă naţională pentru perioada 2021-2026, a căror implementare va fi posibila printr-un efort comun, printr-o coordonare şi cooperare adecvată între instituţiile publice cu responsabilităţi în domeniu, sectorul privat, mediul academic şi cetăţeni: 1. Reţele şi sisteme informatice sigure şi reziliente. 2. Cadru normativ şi instituţional consolidat în domeniul securităţii cibernetice.

	3. Parteneriat public-privat pragmatic. 4. Reziliență prin abordare pro-activă. 5. România - actor relevant în arhitectura internațională de cooperare în domeniul securității cibernetice. Măsurile concrete ce trebuie întreprinse pentru atingerea obiectivelor sunt cuprinse în Planul de Acțiune pentru 2021-2026 şi reprezintă o responsabilitate comună a tuturor actorilor implicați. Noua viziune proiectată de către Strategia de Securitate Cibernetică prevede atât măsuri şi acțiuni reactive cât şi abordări pro-active, pentru detectarea amenințărilor şi atacurilor cibernetice înainte de a impacta infrastructurile, rețelele şi sistemele informatice din România, precum şi dezvoltarea unor mecanisme adecvate de răspuns în acord cu respectarea dreptului internațional. Abordarea se regăseşte în strategiile actuale ale mai multor state membre ale UE, precum şi alte țări partenere şi conferă un cadru flexibil de acțiune care să contribuie la reducerea riscurilor, prevenirea şi descurajarea amenințărilor, precum şi la asigurarea apărării şi securității cibernetice a României.
3. Alte informații	Strategia de Securitate Cibernetică a României prezintă o viziune politică națională ce identifică elementele fundamentale ale interesului național, principiile şi obiectivele strategice, actorii cheie implicați precum şi cadrul național de cooperare şi colaborare aferent. Evaluarea progresului implementării strategiei precum şi al îndeplinirii obligațiilor ce revin actorilor instituționali în implementarea strategiei naționale de securitate cibernetică va trebui efectuată periodic, în vederea adaptării continue la provocările şi oportunitățile generate de un mediu de securitate în permanentă schimbare şi la evoluțiile înregistrate în dezvoltarea tehnologiilor informaționale pe plan mondial.
Secțiunea a 3-a Impactul socioeconomic al proiectului de act normativ	
1. Impactul macroeconomic	Proiectul de act normativ va contribui în mod direct la sprijinirea creşterii economice şi a stabilității sociale prin consolidarea cooperării, colaborării şi parteneriatelor între instituțiile statului şi societatea civilă, respectiv mediul privat, precum şi a formatelor internaționale din domeniul securității cibernetice. Strategia de Securitate Cibernetică a României este un element politic cheie pentru susținerea încrederii, stabilității, rezilienței şi securității în contextul transformării digitale şi al adoptării noilor tehnologii, cu efecte benefice asupra unei dezvoltări economice echilibrate şi sustenabile la nivel național. Strategia va sprijini competitivitatea pe ansamblu a economiei naționale, prin transformarea securității cibernetice într-un avantaj competitiv pentru Romania. Implementarea strategiei va sprijini la nivel național masurile şi acțiunile pentru valorificarea şi capacitarea resursei umane din domeniu pentru atragerea şi păstrarea specialiştilor romani, încurajarea şi susținerea sistemului de învățământ românesc astfel încât securitatea cibernetică să capete o pondere importantă în structura economiei naționale şi PIB.
1[1].Impactul asupra	

mediului concurențial și domeniului ajutoarelor de stat	
2. Impactul asupra mediului de afaceri	Proiectul de act normativ va contribui stimularea parteneriatului public-privat în domeniul securității cibernetice, precum și la creșterea accelerată a domeniului produselor și serviciilor de securitate cibernetice în România. Va crea premisele creșterii ratei de absorbție a fondurilor europene pentru care România este eligibilă, în domeniul securității cibernetice, în special în noul context determinat de proximitatea Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, găzduit de București și a adoptării Planul Național de Redresare și Reziliență (PNRR).
3. Impactul social	Proiectul de act normativ nu se refera la acest subiect.
4. Impactul asupra mediului (***)	Proiectul de act normativ nu se refera la acest subiect.

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)

- mii lei -

Indicatori	Anul curent	Următorii 4 ani				Media pe 5 ani
1	2	3	4	5	6	7
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						
2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
b) bugete locale:						

(i) cheltuieli de personal						
(ii) bunuri şi servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri şi servicii						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor si/sau cheltuielilor bugetare						
7. Alte informaţii	Nu au fost identificate.					

Secţiunea a 5-a Efectele proiectului de act normativ asupra legislaţiei în vigoare	
1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii.	Se abrogă Hotărârea Guvernului nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică. Adoptarea unei Ordonanţe de Urgenţă privind înfiinţarea Directoratului Naţional pentru Securitate Cibernetică (DNSC). Consolidarea rolului şi responsabilităţilor COSC. Adoptarea Legii privind Securitatea şi Apărarea Cibernetică.
2. Conformitatea proiectului de act normativ cu legislaţia comunitară în cazul proiectelor ce transpun prevederi comunitare	Articolele aplicabile din **Directiva (UE) 2016/1148** a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune: • **Articolul 1** Obiect şi domeniu de aplicare *(2) În acest scop, prezenta directivă: (a) stabileşte pentru toate statele membre obligaţia de a adopta o strategie naţională privind securitatea reţelelor şi a sistemelor*

	informatice. • **Articolul 7** Strategia națională privind securitatea rețelelor și a sistemelor informatice *(1) Fiecare stat membru adoptă o strategie națională privind securitatea rețelelor și a sistemelor informatice care definește obiectivele strategice și măsurile politice și de reglementare adecvate, în vederea obținerii și menținerii unui nivel ridicat de securitate a rețelelor și a sistemelor informatice, și care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III. Strategia națională privind securitatea rețelelor și a sistemelor informatice se referă, în special, la următoarele aspecte: (a) obiectivele și prioritățile strategiei naționale privind securitatea rețelelor și a sistemelor informatice; (b) un cadru de guvernanță pentru realizarea obiectivelor și a priorităților strategiei naționale privind securitatea rețelelor și a sistemelor informatice, care să includă rolurile și responsabilitățile organismelor guvernamentale și ale altor actori relevanți; (c) identificarea măsurilor referitoare la gradul de pregătire, răspuns și redresare, inclusiv cooperarea dintre sectorul public și cel privat; (d) indicarea programelor de instruire, sensibilizare și formare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice; (e) indicarea planurilor de cercetare și dezvoltare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice; (f) un plan de evaluare a riscurilor pentru identificarea riscurilor; (g) o listă a diferiților actori implicați în punerea în aplicare a strategiei naționale privind securitatea rețelelor și a sistemelor informatice.* Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică). Strategia de Securitate Cibernetică a Uniunii Europene (UE) din 16 decembrie 2020.
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se refera la acest subiect
4. Hotărâri ale Curții de Justiție a Uniunii Europene	Proiectul de act normativ nu se refera la acest subiect
5. Alte acte normative și/sau documente internaționale din care decurg angajamente	Proiectul de act normativ nu se refera la acest subiect
6. Alte informații	Nu au fost identificate
Secțiunea a 6-a Consultările efectuate în vederea elaborării proiectului de act normativ	

1. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate	Elaborarea prezentului act normativ nu a necesitat astfel de consultări.
2. Fundamentarea alegerii organizațiilor cu care a avut loc consultarea, precum și a modului în care activitatea acestor organizații este legată de obiectul proiectului de act normativ	Elaborarea prezentului act normativ nu a necesitat astfel de consultări.
3. Consultările organizate cu autoritățile administrației publice locale, în situația în care proiectul de act normativ are ca obiect activități ale acestor autorități, în condițiile Hotărârii Guvernului nr.521/2005 privind procedura de consultare a structurilor asociative ale autorităților administrației publice locale la elaborarea proiectelor de acte normative	Elaborarea prezentului act normativ nu a necesitat astfel de consultări.
4. Consultările desfășurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr.750/2005 privind constituirea consiliilor interministeriale permanente	Elaborarea prezentului act normativ nu a necesitat astfel de consultări.
5. Informații privind avizarea de către: **a) Consiliul Legislativ** **b) Consiliul Suprem de Apărare a Țării** **c) Consiliul Economic și Social** **d) Consiliul Concurenței** **e) Curtea de Conturi**	Prezentul proiect necesită avizul: Consiliului Suprem de Apărare a Țării, Consiliului Legislativ
6. Alte informații	Nu au fost identificate.
Secțiunea a 7-a Activități de informare publică privind elaborarea și implementarea proiectului de act normativ	
1. Informarea societății civile cu privire la necesitatea elaborării proiectului de act normativ	Au fost respectate dispozițiile legii 52/2003 privind transparența decizionala în administrația publică, republicată. Proiectul de act normativ va fi supus procedurii de consultare publică, inclusiv prin afișarea pe pagina de internet a Ministerului Cercetării, Inovării și Digitalizării.
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	Proiectul de act normativ nu se referă la acest subiect.
3. Alte informații	

Secțiunea a 8-a Măsuri de implementare	
1. Măsurile de punere în aplicare a proiectului de act normativ de către autoritățile administrației publice centrale și/sau locale - înființarea unor noi organisme sau extinderea competentelor instituțiilor existente	Înființarea Directoratului Național pentru Securitate Cibernetică (DNSC) prin ordonanță de urgență.
2. Alte informații	Nu au fost identificate.

Față de cele prezentate, a fost elaborat proiectul de Hotărâre a Guvernului privind aprobarea Strategiei de Securitate Cibernetică a României și a Planului de Acțiune 2021-2026, pe care îl supunem Guvernului spre adoptare.

Ministrul Cercetării, Inovării și Digitalizării
Ciprian TELEMAN

AVIZĂM FAVORABIL:

SECRETARUL GENERAL AL GUVERNULUI
Tiberiu Horațiu GORUN

MINISTRUL APĂRĂRII NAȚIONALE
Nicolae-Ionel CIUCĂ

MINISTRUL AFACERILOR EXTERNE
Bogdan Lucian AURESCU

MINISTRUL MUNCII ȘI PROTECȚIEI SOCIALE
Raluca TURCAN

MINISTERUL AFACERILOR INTERNE
Lucian Nicolae BODE

MINISTERUL JUSTIȚIEI
Stelian-Cristian ION

MINISTRUL INTERIMAR AL FINANȚELOR
Florin-Vasile CÎȚU

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
Cristian GHINEA

MINISTRUL EDUCAȚIEI
Sorin-Mihai CÎMPEANU

MINISTRUL ECONOMIEI, ANTREPRENORIATULUI ȘI TURISMULUI
Claudiu-Iulius-Gavril NĂSUI

DIRECTORUL SERVICIULUI ROMÂN DE INFORMAȚII

Eduard Raul HELLVIG

DIRECTORUL SERVICIULUI DE INFORMAȚII EXTERNE

Gabriel VLASE

DIRECTORUL SERVICIULUI DE TELECOMUNICAȚII SPECIALE

General-locotenent ing. Ionel-Sorin BĂLAN

DIRECTORUL SERVICIULUI DE PROTECȚIE ȘI PAZĂ

General doctor Lucian-Silvan PAHONȚU

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

Marius PETRESCU

PREȘEDINTELE AUTORITĂȚII PENTRU DIGITALIZAREA ROMÂNIEI

Octavian OPREA

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII

Vlad STOICA

DIRECTORUL GENERAL AL CENTRULUI NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ

Dan CÎMPEAN