Biroul permanent al Senatului
L...828.../...21.12.2022.....

Parlamentul României
Senat

Comisia pentru apărare, ordine publică și siguranță națională

Nr. XXV/599/20.12.2022

Comisia pentru comunicații, tehnologia informației și inteligență artificială

Nr. LXIX/456/20.12.2022

RAPORT COMUN
asupra proiectului de Lege privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative (L828/2022)

În conformitate cu prevederile art. 70 din Regulamentul Senatului, republicat, cu modificările ulterioare, **Comisia pentru apărare, ordine publică și siguranță națională și Comisia pentru comunicații, tehnologia informației și inteligență artificială**, prin adresa nr. L828/2022, au fost sesizate de către Biroul permanent al Senatului în vederea dezbaterii şi elaborării raportului comun asupra **proiectului de Lege privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative**, în procedură de urgență, având ca inițiator Guvernul României.

Proiectul de lege are ca **obiect de reglementare** instituirea cadrului juridic şi instituţional referitor la organizarea şi desfăşurarea activităţilor din domeniile securitate cibernetică şi apărare cibernetică, a mecanismelor de cooperare şi a responsabilităţilor instituţiilor cu atribuţii în domeniile menţionate. Potrivit expunerii de motive, obiectivele proiectului sunt: crearea de reţele şi sisteme informatice sigure şi reziliente, elaborarea şi adoptarea unui cadru normativ şi instituţional consolidat, consolidarea unui parteneriat public-privat, pragmatic, pe linia securităţii cibernetice, asigurarea rezilienţei prin abordare proactivă şi descurajare, transformarea României într-un actor relevant în arhitectura internaţională de cooperare în domeniul securităţii cibernetice. Totodată, proiectul stabileşte un cadru armonizat de acţiune a autorităţilor şi instituţiilor publice cu responsabilităţi şi capabilităţi specifice prevenirii şi contracarării ameninţărilor, vulnerabilităţilor şi riscurilor cibernetice, instituind, la nivel naţional, un cadru normativ care va permite crearea instrumentelor instituţionale şi a mecanismelor de acţiune integrată şi cooperare interinstituţională în domeniile securitate şi apărare cibernetică. Astfel, prin intermediul arhitecturii de cooperare interinstituţională se asigură o coerenţă crescută în ceea ce priveşte răspunsul la incidente sau atacuri cibernetice, precum şi responsabilităţi clare şi predictibilitate în ceea ce priveşte tipul de

acţiuni desfăşurate de fiecare instituţie din domeniile apărării, ordinii publice şi securităţii naţionale.

Proiectul de lege a fost adoptat de Camera Deputaților la data de 19.12.2022.

La întocmirea prezentului raport s-au avut în vedere:

- **avizul favorabil,** cu observații și propuneri, al **Consiliului Legislativ** transmis cu nr. 1352/07.12.2022;
- **avizul favorabil,** cu observații al **Consiliului Economic și Social** transmis cu nr. 7717/07.12.2022;
- **avizul favorabil** al **Consiliului Suprem de Apărare a Țării**, conform Hotărârii nr. 206/07.12.2022.

La dezbaterea proiectului de lege au participat în calitate de **invitați**, în conformitate cu prevederile art. 63 din Regulamentul Senatului, republicat, cu modificările ulterioare, reprezentanți ai Ministerului Cercetării, Inovării și Digitalizării, Ministerului Apărării Naționale, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, Autorității Naționale pentru Administrare și Reglementare în Comunicații și Directoratului Național de Securitate Cibernetică.

În **ședința din data de 20.12.2022**, membrii celor două comisii au dezbătut proiectul de lege, au analizat avizele și propunerile de amendamente primite, precum și punctele de vedere exprimate și au hotărât, cu majoritate de voturi, să adopte un raport comun de admitere cu amendamente admise și respinse.

La lucrările ședinței comune a celor două comisii senatorii au fost prezenți conform listelor de prezență.

În consecință, Comisia pentru apărare, ordine publică și siguranță națională și Comisia pentru comunicații, tehnologia informației și inteligență artificială supun spre dezbatere și adoptare Plenului Senatului prezentul **raport comun de admitere cu amendamente admise și respinse,** care se regăsesc în anexa parte integrantă a prezentului raport **și proiectul de lege**.

În raport cu obiectul de reglementare, proiectul de lege face parte din categoria legilor organice şi urmează a fi adoptat în conformitate cu prevederile art.76 alin. (1) din Constituţie.

Potrivit art. 75 alin.(l) din Constituţia României, republicată, şi ale art.92 alin.(8) pct. 2 din Regulamentul Senatului, republicat, cu modificările ulterioare, **Senatul** este **Cameră decizională.**

Președinte,
Senator Nicoleta Pauliuc

Secretar,
Senator Gheorghiță Mîndruță

Președinte,
Senator Marius Humelnicu

Secretar,
Senator Adrian Hatos

Anexă la raportul
nr. XXV/559/20.12.2022
nr. LXIX/1556/20.12.2022

AMENDAMENTE ADMISE
la proiectul de Lege privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative
(L828/2022)

Nr. crt.	Forma adoptată de Camera Deputaților	Amendamente	Motivare admitere
1.	**Art. 3.** - (1) În domeniul securității cibernetice prezenta lege se aplică următoarelor: ---------- c) 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 **desfășoară activități cu scop lucrativ și nelucrativ, de cercetare, dezvoltare, inovare și producție în domeniul tehnologia informației și a comunicațiilor, sau** furnizează servicii publice ori de interes public, altele decât cele de la lit. b).	**La articolul 3 alineatul (1), litera c) se modifică și va avea următorul cuprins:** "c) 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)." **Autori:** **Membrii PSD și PNL ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	În forma actuală, litera c) prevede o categorie prea largă de persoane fizice și juridice cărora li se adresează soluția legislativă (startup TIC, PFA, multinaționale programare și cercetare-dezvoltare TIC pentru clienți din străinătate, ex. Microsoft, Oracle, Amazon). Această soluție poate duce la mutarea în alte state/pierderea de clienți a industriei românești TIC. De asemenea, textul are caracter ambiguu, deoarece nu se cunoaște destinatarul normei, rămânând la latitudinea arbitrară a celui care aplică norma dacă admite sau nu că o persoană fizică sau juridică este destinatară. Forma actuală are efect extrateritorial – aplicabil și entităților străine care au centre în România, ceea ce ridică probleme privind plenitudinea de competență.

			Pentru toate acestea, soluția legislativă poate duce la contestare la CCR de către persoanele juridice de drept privat. Pentru aceasta, se propune eliminarea sintagmei "*desfășoară activități cu scop lucrativ și nelucrativ, de cercetare, dezvoltare, inovare și producție în domeniul tehnologia informației și a comunicațiilor*".
2.	**Art. 23.** În domeniul managementului incidentelor de securitate cibernetică, autoritățile prevăzute la art. 10 alin. (1) lit. c) și d) au următoarele responsabilități: --- e) să păstreze pe o perioadă de 5 ani datele referitoare la incidentele de securitate cibernetică și rezultatele măsurilor de contracarare a acestora, fără a colecta **date conținut.**	**La articolul 23, litera e) se modifică și va avea următorul cuprins:** "e) să păstreze pe o perioadă de 5 ani datele referitoare la incidentele de securitate cibernetică și rezultatele măsurilor de contracarare a acestora, fără a colecta date **de** conținut." **Autori:** **Membrii PSD și PNL ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	Amendamentul corectează o eroare de redactare.
3.	**Art. 24. -** (1) Asigurarea rezilienței în spațiul cibernetic se realizează prin implementarea de măsuri proactive și reactive de către persoanele prevăzute la art. 3.	**La articolul 24, alineatul (1) se modifică și va avea următorul cuprins:** "(1) Asigurarea rezilienței în spațiul cibernetic se realizează prin implementarea de măsuri proactive și reactive de către **instituțiile și** persoanele prevăzute la art. 3." **Autori:** **Senator Nicoleta Pauliuc**	

4.	**Art. 25.** – (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, 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.	**La articolul 25, alineatul (1) se modifică și va avea următorul cuprins:** "(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,** 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." **Autori:** **Membrii PSD și PNL ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	Termenul de 48 de ore este unul scurt pentru notificarea privind vulnerabilitățile, riscurile și amenințările de securitate cibernetică, notificare ce presupune o analiză prealabilă din partea furnizorilor de servicii tehnice. De aceea, se dorește separarea incidentelor de securitate cibernetică care pot fi notificate în maximum 48 de ore, de notificarea amenințărilor, vulnerabilităților și riscurilor, pentru care se propune un termen de 5 zile de la data solicitării.
5.	**Art. 48.** --- (2) Prin derogare de la dispozițiile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, contravențiile prevăzute la alin. (1) se sancționează astfel: --- b) pentru operatorii economici cu o cifră de	**La articolul 48 alineatul (2), litera b) se modifică și va avea următorul cuprins:** "b) pentru operatorii economici cu o cifră de	

	afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la **5%** din cifra de afaceri netă, iar, în cazul săvârşirii unei noi contravenții, în termen de 6 luni, de la data săvârşirii primei contravenții, limita maximă a amenzii este de **10%** din cifra de afaceri netă.	afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la **1%** din cifra de afaceri netă, iar, în cazul săvârşirii unei noi contravenții, în termen de 6 luni, de la data săvârşirii primei contravenții, limita maximă a amenzii este de **3%** din cifra de afaceri netă." **Autori:** **Membrii PSD, PNL și USR ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	
6.	**Art. 51.** Ordonanţa de urgenţă a Guvernului nr.1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, publicată în Monitorul Oficial al României, Partea I, nr.22 din 21 ianuarie 1999, aprobată cu modificări şi completări prin Legea nr.453/2004, cu modificările şi completările ulterioare, se modifică după cum urmează: --- 3. Articolul 23 se modifică și va avea următorul cuprins: "Art.23.- (1) Ordonanţele militare se emit în limitele stabilite prin decretul de instituire a măsurii excepţionale, astfel: 1. pe durata stării de asediu: a) de ministrul apărării naţionale sau de şeful Statului Major **General**, când starea de asediu a fost instituită pe întregul teritoriu al ţării; b) de comandanţii de mari unităţi în raza teritorială pentru care au fost împuterniciţi de	**La articolul 51, punctul 3 se modifică și va avea următorul cuprins:** "3. Articolul 23 se modifică şi va avea următorul cuprins: Art.23.- (1) Ordonanţele militare se emit în limitele stabilite prin decretul de instituire a măsurii excepţionale, astfel: 1. pe durata stării de asediu: "a) de ministrul apărării naţionale sau de şeful Statului Major **al Apărării**, când starea de asediu a fost instituită pe întregul teritoriu al ţării; b) de comandanţii de mari unităţi în raza	Amendamentul corectează o eroare de redactare și armonizează conceptele din cuprinsul actelor normative incidente.

	şeful Statului Major **General**, când starea de asediu a fost instituită în anumite unităţi administrativ-teritoriale; 2. pe durata stării de urgenţă: a) de ministrul afacerilor interne sau de înlocuitorul de drept al acestuia, când starea de urgenţă a fost instituită pe întregul teritoriu al ţării; b) de ofiţerii împuterniciţi de ministrul afacerilor interne sau de înlocuitorii legali ai acestora, când starea de urgenţă a fost instituită în anumite unităţi administrativ-teritoriale. (2) În situaţia instituirii **stării** excepţionale pentru cauze ce privesc securitatea sau apărarea cibernetică în condiţiile art.2 şi art.3 lit. a), emitenţii ordonanţelor militare solicită avizul prealabil şi consultativ al Consiliului Operativ de Securitate Cibernetică."	teritorială pentru care au fost împuterniciţi de şeful Statului Major **al Apărării**, când starea de asediu a fost instituită în anumite unităţi administrativ-teritoriale; 2. pe durata stării de urgenţă: a) de ministrul afacerilor interne sau de înlocuitorul de drept al acestuia, când starea de urgenţă a fost instituită pe întregul teritoriu al ţării; b) de ofiţerii împuterniciţi de ministrul afacerilor interne sau de înlocuitorii legali ai acestora, când starea de urgenţă a fost instituită în anumite unităţi administrativ- teritoriale. (2) În situația instituirii **măsurii** excepționale pentru cauze ce privesc securitatea sau apărarea cibernetică în condițiile art.2 și art.3 lit.a), emitenții ordonanțelor militare solicită avizul prealabil și consultativ al Consiliului Operativ de Securitate Cibernetică." **Autori:** **Membrii PSD și PNL ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	
7.	**Art. 52.** --- (4) În vederea aplicării prevederilor art. 24, autorităţile prevăzute la art. 10 adoptă măsuri proprii de reziliență în spațiul cibernetic în maximum 120 de zile de la data intrării în vigoare a prezentei legi. (5) În vederea aplicării prevederilor art. 28 alin. (1), metodologia se emite prin ordin al	**La articolul 52, după alineatul (4), se introduce un nou alineat, alin. (4^1), cu următorul cuprins:** "(4^1) 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."	Pentru a asigura textului de la art. 25 alin. (1) claritate, previzibilitate și calitate, se propune ca întreaga procedură de solicitare, respectiv notificarea a datelor și informațiilor să fie reglementată prin hotărâre de Guvern. Astfel, se asigură respectarea prevederilor art. 1 alin. (5) și ale art. 135 alin. (1) din Constituția României.

	directorului DNSC în maximum 6 luni de la data intrării în vigoare a prezentei ----------	**Autori:** **Membrii PSD și PNL ai Comisiei pentru apărare, ordine publică și siguranță națională și ai Comisiei pentru comunicații, tehnologia informației și inteligență artificială**	

AMENDAMENTE RESPINSE
la proiectul de Lege privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative
(L828/2022)

Nr. crt.	Forma adoptată de Camera Deputaților	Amendamente	Motivare amendament
1.	**Art. 16.** STS este autoritate competentă în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele, serviciile **proprii** și spectrul de frecvențe radio **proprii, precum și cele reglementate prin legi speciale**.	**Articolul 16 se modifică și va avea următorul cuprins:** "Art. 16. STS este autoritate competentă **la nivel național** în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele, **serviciile și spectrul de frecvențe radio aflate în domeniul de competență.**" **Autori:** **Senator Nicoleta Pauliuc** **Senator Marius Humelnicu**	Amendamentul propus vine în sprijinul asigurării clarității și cursivității conținutului textului proiectului de lege, prin eliminarea sintagmei „*proprii*", precum și uniformizarea conținutului art. 16 cu art. 11-15 și 17 din proiectul de lege, prin înlăturarea sintagmei „*precum și cele reglementate prin legi speciale*". Totodată, amendamentul asigură punerea în concordanță a proiectului de lege cu dispozițiile Legii nr. 92/1996 privind organizarea și funcționarea Serviciului de Telecomunicații Speciale, cu modificările și completările ulterioare, din următoarele considerente: 1. Sintagma „*proprii*", din cuprinsul art. 16 din proiectul de lege, creează confuzia că responsabilitatea asigurării de către STS a securității cibernetice se referă doar la sistemele și aplicațiile informatice interne ale STS, fapt ce contravine dispozițiilor art. 1 și ale lit. C. din Anexa

			nr. 2 din Legea nr. 92/1996, potrivit cărora STS furnizează "*pentru beneficiarii prevăzuți în Anexa nr. 1 la lege, rețele, infrastructuri, sisteme, servicii și aplicații în diferite tehnologii informatice și de comunicații, cu soluții de securitate asociate.*" Prin efectul Legii nr. 92/1996, STS are obligația de a asigura securitatea cibernetică inclusiv pentru sistemele și aplicațiile informatice furnizate beneficiarilor legali. Astfel, menținerea sintagmei „*proprii*" în cuprinsul art. 16, a cărei interpretare poate fi subiectivă și neclară, poate conduce la imposibilitatea îndeplinirii obligațiilor legale ale STS și contravine principiului personalității, menționat la art. 5 lit. a) din proiectul de lege, conform căruia "*responsabilitatea asigurării securității cibernetice și/sau apărării cibernetice a unui sistem, rețea și/sau serviciu informatic revine persoanei fizice sau juridice care le deține în proprietate, le organizează, administrează și/sau utilizează, după caz.*" Un argument în plus pentru eliminarea sintagmei „*proprii*" din conținutul art. 16 este și faptul că, potrivit prevederilor art. 11 lit. b) și c) din Legea nr. 92/1996, STS gestionează spectrul de frecvențe radio cu utilizare guvernamentală și ține evidența și monitorizează, pe teritoriul

			național, în scopul protecției, spectrul de frecvențe radio aflat în gestiunea sa și al organismelor ce fac parte din sistemul național de apărare, ordine publică și securitate națională. Astfel, conform Legii nr. 92/1996, competențele de asigurare a securității și protecției de către STS acoperă, în prezent, și serviciile de comunicații utilizate de aparatul guvernamental și de instituțiile din sistemul național de apărare, ordine publică și securitate națională, ceea ce nu s-ar mai putea realiza în situația în care art. 16 din proiectul de lege ar intra în vigoare în forma propusă de inițiator. Mai mult, progresul tehnologic înregistrat în domeniul comunicațiilor și tehnologiei informațiilor obligă STS, în calitate de dezvoltator și administrator tehnic, de a furniza către beneficiarii legali servicii și aplicații informatice care se bucură încă de la momentul conceperii de soluții de securitate cibernetică, fapt ce asigură menținerea permanentă a unui climat de securitate ridicat pentru datele și informațiile vehiculate în sistemele și aplicațiile informatice în cauză, pe toată durata operaționalizării acestora de către beneficiari, fără a fi necesară implicarea sau alocarea de resurse umane, financiare și tehnologice de către aceștia, pentru a asigura securitatea cibernetică.

			De cele mai multe ori, beneficiarii legali prevăzuți în Anexa nr. 1 din Legea nr. 92/1996 nu pot implementa, într-un interval de timp optim, măsurile tehnice necesare asigurării securității cibernetice a sistemelor și aplicațiilor informatice pe care le utilizează în desfășurarea activității. 2. Totodată, raportat la eliminarea sintagmei „*precum și cele reglementate prin legi speciale*", precizăm faptul că formularea propusă exclude din domeniul de competență al STS sistemele și aplicațiile informatice care au fost dezvoltate, administrate și securizate, din punct de vedere cibernetic, de către STS, în baza prevederilor hotărârilor de Guvern, a ordinelor emise de către conducătorii instituțiilor beneficiare, precum și în baza acordurilor de colaborare între STS și beneficiari. Considerăm, așadar, că, în forma propusă, norma este lipsită de predictibilitate, iar aplicarea ei ar conduce la imposibilitatea asigurării securității cibernetice a sistemelor și aplicațiilor informatice sus-menționate, pe o perioadă însemnată de timp. Așadar, dintr-o eroare materială a inițiatorului, formularea actuală a art. 16 din proiectul de lege conduce la scoaterea din sfera de competență a STS a serviciilor informatice și aplicațiilor

			reglementate și operaționalizate prin acte normative care nu au putere de lege. În exemplificare menționăm Sistemul Informatic Integrat „Programare-vaccinare-ROVACCINARE", reglementat prin HG nr. 1031/2020 și Sistemul Informatic Integrat SUMAL 2.0, reglementat prin HG nr. 497/2020, ambele sisteme informatice având o importanță deosebită la nivel național. În aceeași situație se află și sistemul informatic IMM-INVEST, dezvoltat, administrat și securizat în baza Acordului de colaborare cu Ministerul Finanțelor. Sistemele și aplicațiile informatice sus-menționate se află, în prezent, în exploatarea beneficiarilor, fiind utilizate de către cetățeni, iar asigurarea securității cibernetice a acestora este în responsabilitatea directă a STS.
2	**Art. 3 alin.(1)** **[...]** c) 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 desfășoară activități cu scop lucrativ și nelucrativ, de cercetare, dezvoltare, inovare și producție în domeniul tehnologia informației și a comunicațiilor, sau furnizează servicii publice ori de interes	**La articolul 3, alineatul (1) litera c) se modifică și va avea următorul cuprins:** **„c) 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)."** **La articolul 3, alineatul (1), după litera c), se adaugă literele d) și e), cu următorul cuprins:** **„d) rețelele și sistemele informatice deținute**	Includerea rețelelor și sistemelor informatice ale persoanelor juridice care furnizează servicii publice ori de interes public (fără a defini acești termeni în cuprinsul acestui act normativ) face ca spectrul de aplicare să fie exagerat de larg. Obligațiile prevăzute sunt imposibil de îndeplinit pentru oricare din următoarele: - un *site* cu 3 utilizatori, administrat de un PFA la ONG, care oferă un serviciu online (care este public prin definiție),

	public, altele decât cele de la lit. b).	**sau administrate de persoane juridice, altele decât cele de la lit. b), care deservesc servicii esențiale sau importante, cu obligațiile specifice în conformitate cu legea 362/2018.** **e) rețelele și sistemele informatice deținute sau administrate de persoane juridice, prin care sunt prelucrate date cu caracter personal, cu obligațiile specifice în conformitate cu Regulamentul UE 679/2016."** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	- un site care aparține unei publicații mici mass-media, serviciu gratuit sau plătit, - un mic magazin *offline* (care și el are un serviciu public) dotat cu casă de marcat electronică (deci un sistem informatic). În plus, articolul actual nu respectă par. 69 al Deciziei CCR 17/2015, potrivit cu care: *„Or, dispozițiile legale în forma supusă controlului de constituționalitate prezintă un grad mare de generalitate, obligațiile vizând totalitatea deținătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice, indiferent de importanța acestora care poată viza interesul național sau doar un interes de grup ori chiar particular. Pentru a evita impunerea unei sarcini disproporționate asupra micilor operatori, cerințele trebuie să fie proporționale cu riscurile la care sunt expuse rețeaua sau sistemul informatic în cauză și nu trebuie aplicat deținătorilor de infrastructuri cibernetice cu importanță nesemnificativă din punctul de vedere al interesului general."* Trebuie avut în vedere faptul că *Internetul* este un spațiu ubicuu - deci nu doar infrastructura informatică din România poate cauza probleme sistemelor informatice din România.

			Deci a impune astfel de obligații la nivel național nu rezolvă problema de fond a asigurării securității, ci doar împovărează orice deținător din România. Chiar și directivele NIS1 (în vigoare) si NIS2 exceptează în mod explicit IMM-urile de la obligațiile din domeniul securității informatice - în acest sens a se vedea și comentariul de la art. 22 cu privire la limitele pentru IMM-uri.
3	**Art. 21** **(1)** Persoanele prevăzute la art. 3 alin. (1) lit. b) și lit. c), au 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. **[...]**	La art. 21, alineatul (1) se modifică și va avea următorul cuprins: **„Autoritățile prevăzute la art. 3 lit. c), ca și persoanele juridice prevăzute la art. 3 lit.e) pot notifica incidentele de securitate cibernetică prin intermediul PNRISC, în mod voluntar, fără a aduce atingere normelor legale aplicabile în materie de raportare, confidențialitate, protecția datelor personale și secret profesional, în cazurile în care estimează că acel incident poate fi relevant pentru asigurarea securității cibernetice la nivel național."** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	Persoanele juridice prevazute la lit d) deja au aceasta obligatie prin Legea 362/2018. Persoanele juridice prevăzute la lit. b) au deja această obligație similară prin Legea 198/2022. Persoanele juridice prevăzute la lit. e) au o obligație similară de raportare conform GDPR către ANSPDCP, dacă incidentul afectează datele personale. În consecință, pentru celelalte categorii, raportarea incidentelor de securitate trebuie sa fie voluntare, limitat la situația când raportarea nu aduce atingere drepturilor altora si cand raportarea ar fi utilă pentru asigurarea securității cibernetice la nivel național.
4	**Art. 22** Incidentele de securitate cibernetică sunt notificate în PNRISC în condițiile secțiunii a 2-a din Capitolul IV al Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor	**Articolul 22 se elimină.** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	Dacă nu se modifică art. 20 practic avem de-a face cu o extindere a Legii 362/2018 (care implementează corect Directiva NIS), de la cateva sectoare critice si aproximativ 100-200 de firme si autoritati mici si mari la probabil cateva

	informatice.		sute de mii de persoane juridice, aspect care este considerat excesiv de legislația UE. Aceasta ar fi o incalcare a acquis-ului comunitar: - considerentului 53 din directiva NIS - https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32016L1148 *Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra operatorilor de servicii esențiale și a furnizorilor de servicii digitale, cerințele ar trebui să fie proporționale cu riscurile la care este expusă rețeaua și sistemul informatic în cauză, ținând seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. În cazul furnizorilor de servicii digitale, aceste cerințe nu ar trebui să se aplice microîntreprinderilor și întreprinderilor mici.*
5.	**Art. 25.** (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, 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	**La art.25, alineatul (1) se modifică și va avea următorul cuprins:** **„(1) În măsura în care informațiile deținute ar fi utile pentru asigurarea securității cibernetice a altor rețele și în special pentru securitatea națională a României, furnizorii de servicii tehnice de securitate cibernetică au dreptul de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în funcție de domeniul de competență adecvat, date și informații privind incidente, amenințări, riscuri sau**	Scopul unui furnizor de servicii de securitate este acela de a proteja și de a rezolva problemele clientului său. De obicei, furnizorii de servicii de securitate cibernetică sunt niște profesioniști tehnici care au obligații contractuale de confidențialitate extrem de stricte față de clienții lor (din România sau străinătate). O parte din informațiile la care au access, sau pe care le descoperă, sunt legate de incidente, amenințări, riscuri sau vulnerabilități.

	utilizatorii finali. **[...]**	**vulnerabilități a căror manifestare poate afecta alte rețele sau sisteme informatice prevăzute la art. 3 alin. 1."** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	Conform proiectului de lege privind securitatea cibernetică a României, acești furnizori sunt obligați ca, la orice întrebare de la una din instituțiile din art. 10, să-și reclame/denunțe proprii clienți. Fără mandat judecătoresc, fără autorizație precisă, acești furnizori sunt obligați să dea informații despre starea securității unui client, sau, mai rău, a unei întregi infrastructuri (ceea ce poate include informații personale și secrete ale mai multor clienți, fie ei direct afectați de o posibilă vulnerabilitate sau nu). O asemenea obligație - care a făcut parte și din legea cu același obiect declarată neconstituțională prin decizia CCR 17/2015 - ar fi asemănătoare obligației unui auditor sau contabil ca în primul rând să pârască la ANAF și nu să își sfatuiasca clientul ce trebuie să facă pentru a fi în legalitate. Scopul conform declaratiilor publce ale MCID : *„Fiecare autoritate publică cu atribuții în domeniul securității cibernetice, pentru a-și putea exercita atribuțiile legale de protejare a rețelelor și sistemelor informatice, are nevoie de o colaborare loială cu furnizorii de servicii de securitate cibernetică. Această colaborare presupune inclusiv protejarea rețelelor și a sistemelor informatice ale acelor furnizori, care deservesc unor scopuri publice sau private. "*

6.	**Art. 25** **[...]** **(3)** Datele și informațiile prevăzute la alin.(1) se transmit în scris, prin mijloace electornice sau prin orice altă modalitate stabilită de comun acord, în formatul și structura conforme raportării de incidente cibernetice în PNRISC, menționate la art. 22.	La articolul 25, după alineatul (3) se introduce un nou alineat. alineatul (4), cu următorul cuprins: **„(3) In măsura în care informațiile deținute ar fi utile pentru asigurarea securității cibernetice a altor rețele și în special pentru securitatea națională a României, autoritățile prevăzute la art. 10, au dreptul de a pune la dispoziția furnizorii de servicii de securitate cibernetică, date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta alte rețele sau sisteme informatice, dacă:** **- datele și informațiile nu conțin date cu caracter personal; si** **- dezvăluirea datelor și informațiilor nu pot aduce atingere intereselor deținătorului rețelei sau sistemului informatic afectate, stabilite la nivel legal sau contractual."** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	Pentru obligații corelative din partea autorităților publice către sectorul privat.
7.	**Art. 41.** (1) Persoanele prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare, conform metodologiei menționate la art. 52 alin. (1)	**La articolul 41, alineatul (1) se modifică și va avea următorul cuprins:** **„(1) Persoanele prevăzute la art. 3 alin.(1) a-d) implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare, conform metodologiei menționate la art. 52 alin. (1)".** **Autori:** **Raoul-Adrian TRIFAN, senator USR**	Acest proces de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare sunt aspecte complexe de securitate cibernetica care trebuie sa fie implementate doar de autoritati publice si firme mari, conform acquis-ului comunitar existent (vezi directiva NIS 1 si NIS 2 menționate mai sus).

		Eugen-Remus, NEGOI, senator USR **Silvia DINICĂ, senatoare USR**	
8.	**Art. 50.** La articolul 3 din Legea nr. 51/1991 privind securitatea națională a României, republicată în Monitorul Oficial, Partea I, nr. 190 din 18 martie 2014, cu modificările și completările ulterioare, după litera m), se introduc trei noi litere, literele n), o) și p), care vor avea următorul cuprins: "n) amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național; o) acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului în raport cu riscurile și amenințările de tip hibrid; p) acțiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea Constituțională."	**Articolul 50 se elimină.** **Autori:** **Raoul-Adrian TRIFAN, senator USR** **Eugen-Remus, NEGOI, senator USR** **Silvia DINICĂ, senatoare USR**	Extinderea domeniilor de securitate națională trebuie sa se faca pe baza unei analize exhaustive si cu un text extrem de clar si nu vag - vezi în acest sens deciziile 91/2018 si 802/2018 ale CCR. În măsura în care nu sunt definite ce înseamnă „infrastructurilor informatice și de comunicații de interes național" sau „a unor campanii de propagandă sau dezinformare" sau „reziliența statului" sau „riscurile și amenințările de tip hibrid", ele practic pot sa însemne orice dorește SRI, ceea ce contrazice deciizile CCR: - par.83 din Decizia CCR nr.91: „Astfel, din modul de reglementare a sintagmei analizate, rezultă că se poate circumscrie unei amenințări la adresa securității naționale orice faptă/acțiune cu sau fără conotație penală care afectează un drept sau o libertate fundamentală. Cu alte cuvinte, sfera de aplicare a dispoziției criticate este atât de largă, încât față de orice persoană se poate reține exercitarea unei acțiuni care constituie amenințare la adresa securității naționale." - par. 80 din Decizia nr.802/2018: „Caracterul deschis al sintagmei criticate determină posibilitatea introducerii sau excluderii de elemente în/din această

			categorie, acțiune care se răsfrânge și asupra limitelor de aplicare a dispoziției de lege criticate. În acest mod, limitele de aplicare a dispoziției de lege criticate nu mai pot fi cunoscute de destinatarii normei, care, astfel, nu își pot corecta conduita și nu pot fi capabili să prevadă, într-o măsură rezonabilă, consecințele care pot apărea dintr-un act determinat."