American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

16 noiembrie 2022

Observații ale Camerei de Comerț Americane în România (AmCham România) cu privire la *Proiectul de Lege privind securitatea și apărarea cibernetică a României*

1. CONSIDERAȚII GENERALE

- Fără a pune în discuție necesitatea în sine a unei asemenea reglementări, observăm existența în cuprinsul proiectului actual a **unor prevederi care sunt problematice din perspectiva sectorului privat**. Credem, astfel, că este important:

  (a) să nu se extindă aria de subiecți/sectoare față de NIS 2 – de exemplu, art 3 (c) actual este foarte larg „[...] *precum și de persoane juridice care desfășoară activități industriale, de cercetare științifică sau furnizează servicii publice ori de interes public, altele decât cele de la lit. b)*".

  Codurile CAEN potențial relevante, raportat la formularea de mai sus, sunt foarte numeroase și ar acoperi numeroase entități cu activități benigne și/sau cu risc redus pentru societate în caz de atac cibernetic. Menționăm și faptul că noțiunea de „serviciu de interes public" nu este consacrată legislativ, putând genera multă incertitudine juridică. De altfel, și formulările care privesc administrația publică sunt potențial foarte largi, cuprinzând potențial mii de primării mici și care ar trebui să facă investiții semnificative foarte rapid.

  Cu caracter mai general, o serie de formulări actuale (în special art. 3, 5 și 23) sunt, astfel, foarte largi și ar impune sarcini economice și incertitudini juridice potențial semnificative operatorilor economici din România, afectându-le competitivitatea față de concurenți din alte țări UE. Pentru domenii/subiecți în afara sferei directivei NIS2, s-ar putea avea în vedere posibilitatea unei certificări în acest sens pentru cei care ar îndeplini standardele respective în mod voluntar.

  (b) în orice caz, să se facă o distincție între grade de risc – direcție în care merge și legislația europeană, de exemplu, Proiectul de regulament cu privire la regulile în materie de inteligență artificială. Formulările actuale privesc, practic, în mod identic orice activitate industrială, orice activitate de cercetare etc - indiferent de obiect, grad de mărime, grad de conectare la alte rețele etc. De asemenea, nu se face o distincție între situații. De exemplu, un consorțiu de cercetare ar putea genera automat obligații oneroase pentru fiecare dintre membrii săi, deși s-ar folosi mai mult infrastructura liderului de consorțiu etc. De asemenea, pot apărea și alte situații excesive – orice solicitare din România (indiferent de obiect) pentru fonduri europene în domeniul cercetării, odată aprobată, arputea greva automat aplicanții raportat la forma actuală a proiectului de lege.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

(c) să nu fie impuse standarde de rezultat excesive – precum „protecția absolută" (și în contextul principiului personalității), în plus, cu obligații pentru subiecții legii de a verifica numeroase aspecte tehnice în afara competențelor lor obișnuite. Zona IT este una, prin definiție, destul de înalt specializată. Numeroase societăți comerciale achiziționează produse și servicii din zona respectivă tocmai pentru că nu au capabilitățile respective în intern. A muta răspunderea la ele(chiar cu drept de regres) riscă să fie atât excesiv, cât și contraproductiv pentru interesul general, fragilizând agenții economici din România. De asemenea, numeroase asigurări din piață ar și risca să fie inoperabile.

Poate apărea și o diferențiere potențială de standard între sectorul public și privat. Dacă apare un incident de securitate în rețelele de ordine publică, de exemplu, s-ar putea deduce că trebuie automat să răspundă, inclusiv pecuniar, cineva de la instituțiile respective pentru că nu s-a respectat principiul protecției absolute. În cazul sectorului privat, pare că simplul incident generează automat o răspundere pentru proprietarul/administratorul rețelei indiferent de modul cum s-a produs, de gradul de sofisticare de diligența medie de prevenire etc (dacă art. 5 respectiv rămâne în forma actuală). Este important să nu fie diferențe potențiale de tratament. Considerăm, de asemenea, necesar să fie clarificate diligențele (rezonabile) anterioare care protejează de răspundere în caz de incident.

(d) să existe diferențieri între intenție și culpă și între grade de culpă – e o consecință, apreciem,normală a celor de mai sus.

(e) să existe perioade de tranziție/adaptare rezonabile – România nu are numărul de experți necesari pentru a sprijini o conformare largă rapidă, dincolo de costurile ei economice și de infrastructura care ar trebui achiziționată. Perioadele foarte scurte de tranziție actuale privesc unele segmente din lege, dar nu privesc, de exemplu, aspectele de principii ale răspunderii, (oneros și extins formulate, după cum menționam și mai sus) – ceea ce poate genera consecințe juridice și economice semnificative rapid.

- Considerăm că forma finală a proiectului ar trebui, de asemenea, să aibă în vedere DECIZIA nr. 17 din 21 ianuarie 2015 asupra obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României. În acest sens, considerăm necesar de avut în vedere și faptul că dispozițiile prezentului proiect de lege creează obligații suplimentare de raportare în absența unor criterii clare sau a existenței unui mandat judecatoresc emis în acest sens, ceea ce poate duce la confuzie, până la încălcarea prevederilor constituționale, precum și încălcarea confidențialității datelor.
- Punerea în executare a legii este partajată între mai multe autorități publice, existând **riscul unei lipse de coordonare și de corelare** între ele, în special în procesul de adoptare a reglementărilor secundare. Apreciem, în acest sens, că orice reglementare secundară menită a asigura organizarea executării și punerea în executare a legii trebuie să îmbrace forma hotărârii de Guvern. Cu notă de recomandare, apreciem că desemnarea unei singure instituții pentru coordonarea activităților prevăzute de proiectul de lege, deși reprezintă, în esență, o chestiune funcțională care trebuie clarificată de autorități, este un element esențial de care va depinde buna aplicare a prevederilor viitoarei legi.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

- Legat de Directiva NIS 2, dincolo de aspectul de sferă de aplicabilitate menționat mai sus, considerăm important să se asigure **corelarea mai largă a prevederilor prezentului proiect de lege cu cele din Directiva NIS 2** (adoptată recent de către Parlamentul European)**, care urmează a fi transpusă în legislația națională**. În caz contrar, există riscul de a avea prevederi contradictorii sau care dublează în mod nejustificat obligațiile impuse în sarcina entităților private. Spre exemplu, în ceea ce privește intenția de reglementare privind securitatea lanțului de aprovizionare (Art. 40-43), Directiva NIS 2 conține o serie de prevederi în legătură cu evaluarea și managementul riscului de securitate cibernetică specifice lanțului de aprovizionare (a se vedea în acest sens recitalurile 59, 85, 90 și 91, precum și articolele 7 alineatul (2) litera a), 14 alineatul (4) litera i), 21 și 22). O serie de alte exemple sunt redate punctual în propunerile de amendamente din tabelul alăturat.

- Se impune clarificarea unor situații care se pot dovedi problematice, precum:
  - *Cum va fi gestionat un risc comercial?* Spre exemplu, dacă pe piață sunt două soluții – un consumator deține exclusivitatea utilizării uneia dintre ele, iar pe cealaltă o declară ca prezentând riscuri în ceea ce privește siguranța națională pentru a-i împiedica pe competitori să utilizeze o soluție similară. Cum va investiga DNSC, sau care va fi maniera de investigare a afirmațiilor din informările voluntare de risc?

2. PROPUNERI PUNCTUALE & OBSERVAȚII

Bold text nou
~~Strikethrough text eliminat~~

# ART.	FORMA ACTUALĂ	FORMA PROPUSĂ	MOTIVAȚIE / OBSERVAȚII
Art. 1 lit. u)	u) securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice sau private din spațiul cibernetic	u) securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice, ~~sau private~~ **precum și a resurselor sectorului privat**, din spațiul cibernetic.	Nu există o consacrare legală a termenului juridic de "serviciu privat".

AMERICAN CHAMBER OF COMMERCE IN ROMANIA

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

Art. 2 lit. k)	furnizor de servicii de găzduire electronică cu resurse IP - astfel cum e definit în art. 4 alin. (1), pct. 95 din OUG nr. 111/2011 privind comunicațiile electronice;	N/A	Deși proiectul de lege stabilește că furnizorul de servicii de găzduire electronică cu resurse IP are înțelesul stabilit prin Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, în cuprinsul proiectului nu se mai regăsesc referiri la acest tip de furnizor.
Art. 3	(1) În domeniul securității cibernetice prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru: a) rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat. b) rețelele și sistemele informatice deținute de persoanele juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale. c) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de	(1) În domeniul securității cibernetice prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru: a) rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat. b) rețelele și sistemele informatice deținute de persoanele juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale**, în vederea asigurării securității și apărării naționale și ordinii publice.**	Modificarea propusă are drept justificare existența unui cadru extensiv de reglementare de securitate informatică și în special cibernetică pentru furnizorii de servicii de comunicații electronice, stabilit între altele prin Ordonanța de Guvern nr. 111/2011 privind comunicațiile electronice, modificată pentru a transpune Codul european al comunicațiilor (Dir. (UE) 2018/1972). Prin urmare, noua Lege ar trebui să stabilească un cadru de reglementare numai pentru activitățile furnizorilor privați de comunicații electronice care se referă la chestiuni de securitate și apărare națională și ordine publică, care fac obiectul Legii propuse. În ceea ce privește prevederile aplicabile în cazul rețelelor de comunicații electronice nu este clar cum vor fi aceastea aplicate și interpretate în raport de prevederile articolelor 46 – 49[2] din OUG nr. 111/2011

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

	autorități și instituții ale administrației publice centrale și locale, altele decât cele prevăzute la lit. a), precum și de persoane juridice care desfășoară activități industriale, de cercetare științifică sau furnizează servicii publice ori de interes public, altele decât cele de la lit. b).	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 juridice care desfășoară activități industriale, de cercetare științifică sau furnizează servicii publice ~~ori de interes public~~, altele decât cele de la lit. b), în toate cazurile care privesc societăți comerciale în acest paragraf, în limita scopului și cu diferențierile prevăzute de Directiva NIS 2 care se vor aplica mutatis-mutandis . **În înțelesul Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, rețea și sistem informatic înseamnă:** **1. reţea de comunicaţii electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare;** **2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a**	care reglementează securitatea reţelelor şi serviciilor de comunicaţii electronice. În vreme ce pot exista persoane juridice de drept privat (altele decât cele prevăzute la art.3 alin.1 lit.b)) care furnizează servicii publice, iar termenul de ”serviciu public” are o definiție bine stabilită în art.5 lit. kk) din Codul administrativ, conceptul de ”serviciu de interes public”, mai ales, asociat unei persoane juridice de drept privat, nu are o definiție legală specifică și generează multă incertitudine juridică. Restrângerea sferei de aplicare are în vedere motivele descrise în partea introductivă. Pentru claritate, se impune clarificarea sintagmei ”rețea și sistem informatic”, în raport cu prevederile legale în vigoare (Legea 362/2018, OUG 111/2011). Draftul de lege ar trebui să excludă expres categoriile de subiecți de drept cărora nu li se aplică, precum, de exemplu, furnizorii de servicii de cloud ce oferă servicii de tipul SaaS.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

		datelor cu ajutorul unui program informatic; **3. datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la pct. 1 şi 2 în vederea funcţionării, utilizării, protejării şi întreţinerii lor;** **În înțelesul Ordonanței de urgență 111/2011 privind comunicaţiile electronice, prin rețea de comunicații electronice se înțeleg sistemele de transmisie, bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, şi, acolo unde este cazul, echipamentele de comutare sau rutare şi alte resurse, inclusiv elementele de reţea care nu sunt active, care permit transportul semnalelor prin cablu, prin unde radio, prin mijloace optice ori alte mijloace electromagnetice, incluzând reţelele de comunicaţii electronice prin satelit, reţelele terestre fixe, cu comutare de circuite şi cu comutare de pachete, inclusiv internet, şi mobile, reţelele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, reţelele utilizate pentru transmisia serviciilor media audiovizuale şi reţelele de**	

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

		televiziune prin cablu, indiferent de tipul de informaţie transmisă.	
Art. 3 alin. 3	N/A	**(3) Sfera categoriilor de persoane juridice menționate la alin.2 lit.c) teza a 2-a va fi stabilită prin hotărâre de Guvern, cu consultarea mediului privat, cu respectarea legislației aplicabile.**	Credem că în acest mod se poate evita crearea unei arii excesiv de largi de operatori economici privați supuși legii chiar la nivel de legislație primară și aloca mai mult timp discutării acestui aspect.
Art. 5	b) principiul protecției depline – entitatea responsabilă de securitatea și/sau apărarea cibernetică a unui sistem, rețea și/sau serviciu informatic răspunde de managementul riscurilor asociate acestora și conexiunilor acestora cu alte sisteme, rețele și/sau servicii informatice terțe, precum și implementarea măsurilor tehnice și organizaționale necesare protecției cibernetice;	b) principiul protecției depline – entitatea responsabilă de securitatea și/sau apărarea cibernetică a unui sistem, rețea și/sau serviciu informatic răspunde de managementul riscurilor asociate acestora și conexiunilor acestora cu alte sisteme, rețele și/sau servicii informatice terțe, precum și de implementarea măsurilor tehnice și organizaționale necesare protecției cibernetice **cu respectarea normelor contractuale, de drept civil și penal în privința proporționalității răspunderii**;	Formularea actuală lasă loc de interpretare în ceea ce privește răspunderea în toate formele ei. Astfel, deși incidentul poate să apară într-un lanț de distribuție, dacă avem de-a face cu culpa unui terț, din punct de vedere al răspunderii trebuie să avem în vedere proporționalitatea dispersării efectelor. Acești factori trebuie avuți în vedere și prin prisma dezvoltării pieței de asigurări pentru acoperirea daunelor produse de incidente cibernetice – dislocarea răspunderii având efecte și în cadrul răspunderii pecuniare.
Art. 17	Autoritățile prevăzute la art. 10 pot constitui și operaționaliza structure specializate în realizarea de audit de securitate cibernetică și structuri specializate de securitate cibernetică pentru gestionarea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate.	Autoritățile prevăzute la art. 10 pot constitui și operaționaliza/**opera** structuri specializate în realizarea de audit de securitate cibernetică și structuri specializate de securitate cibernetică pentru gestionarea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate. **Componenta de audit, împreună cu atribuțiile și capacitatea de**	Dreptul românesc asimilează dreptul contravențional (funcția de audit fiind inclusă în dreptul contravențional) dreptului penal. Astfel, dreptul discreționar de a crea structuri de audit echivalează cu dreptul discreționar de a crea parchete și curți specializate.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

		exercițiu fiind definite prin legislație ulterioară.	Totodată, apare un aspect al lipsei de previzibilitate a legii – deși legea trebuie să fie cunoscută în tot de către persoane, legea trebuie să își păstreze un aspect al previzibiliății, iar creare de organe de audit, fără ca acestea să fie definite, fără ca obligațiile organelor de audit să fie clare, duce la imprevizibilitatea demersului legislativ – în consecință, la imposibilitatea aplicării sale în forma actuală. Deși acest aspect a fost decis de către Curtea Europeană a Drepturilor Omului în privința subiecților naturali de drept, în cadrul legii se fac multiple referiri la persoane fizice ca fiind subiecți ai acestui demers legislativ.
Art. 18	Pentru rețelele şi sistemele informatice aflate în domeniul de competență, activitate sau responsabilitate, autoritatea prevăzută la art. 10 lit. c) are şi următoarele obligații specifice: a) să realizeze periodic audit de securitate cibernetică; b) să propună către DNSC politici de securitate cibernetică specifice; c) să asigure coordonarea și monitorizarea gestionării incidentelor de securitate cibernetică identificate.	N/A	Potrivit prevederilor articolului 49 alineatul (1) litera b) din OUG nr. 111/2011, ANCOM poate solicita furnizorilor de reţele publice de comunicaţii electronice să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent sau de o altă autoritate competentă şi să transmită ANCOM rezultatele auditului. În acest context, nu este clar care este scopul realizării unui audit de securitate cibernetic, atâta timp cât legislația specifică în domeniul telecom prevede deja posibilitatea realizării unui astfel de audit.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			De asemenea, Proiectul de lege nu stabilește ce înseamnă periodic, cine va realiza efectiv acest audit și cine va suporta costurile cu realizarea acestuia. Mai mult, și prevederile menționate la literele b) și c) par să se suprapună cu obligații și măsuri stabilite de prevederile articolelor 46 – 492 din OUG nr. 111/2011.
Art. 20	(1) Persoanele juridice care au în responsabilitate rețele și sisteme informatice 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 24 de ore de la constatarea incidentului. (2) Dacă informațiile prevăzute la art. 21 nu pot fi comunicate complet în termenul prevăzut la alin. (1), acestea se transmit în cel mult 5 zile de la notificarea inițială.	(1) Persoanele juridice care au în responsabilitate rețele și sisteme informatice 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 24 de ore de la constatarea incidentului. (2) Dacă informațiile prevăzute la art. 21 nu pot fi comunicate complet în termenul prevăzut la alin. (1), acestea se transmit în cel mult 5 zile **lucrătoare** de la notificarea inițială, **informațiile putând fi completate și ulterior cu informații ce reies din investigațiile realizate pe baza evenimentului.**	Termenul de 5 zile nu este clar specificat (lucrătoare sau calendaristice). Termenul de 5 zile nu poate fi respectat în situația unui eveniment cibernetic major. Un eveniment de securitate cibernetică poate necesita mai mult de 5 zile doar pentru a restabili funcționalitatea sistemelor, iar investigația poate dura până la 6 luni (în funcție de gravitate). Astfel, informațiile cumulate în 5 zile sunt irelevante pentru ceilalți participanți la viața cibernetică românească. Nu este clar ce trebuie raportat către DNSC prin PNRISC – ce înseamnă „informații comunicate complet”? – de exemplu, s-ar putea să nu cunoaștem niciodată sursa sau actorul care a generat atacul. S-ar putea să nu cunoaștem natura atacului sau întinderea pe care a avut-o, respectiv să putem oferi

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			doar o estimare bazată pe coroborarea informațiilor obținute cu informații de actualitate din viața cibernetică. În ceea ce privește operatorii telecom, OUG nr. 111/2011 stabilește obligația acestora de a notifica ANCOM incidentele cu impact semnificativ asupra rețelelor de comunicații electronice. Mai mult, o dată cu transpunerea Directivei privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune și de abrogare a Directivei (UE) 2016/1148 (”Directiva NIS 2”) obligațiile operatorilor telecom cu privire la securitatea și integritatea rețelelor de comunicații vor fi transferate din legislația specifică sectorului telecom (OUG nr. 111/2011) în legea de transpunere a Directivei NIS 2. În acest context, nu este foarte clar cum vor fi aplicate și interpretate prevederile articolului 20 alineatul (1) în raport de prevederile OUG nr. 111/2011 și ulterior în raport de prevederile legii de transpunere a Directivei NIS 2. Mai mult, având în vedere că anumite incidente de securitate cibernetică pot presupune și o dezvăluire /accesare/ștergere neautorizată de date cu caracter personal, considerăm important de

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			clarificat interacțiunea Proiectului de lege privind securitatea și apărarea cibernetică a României cu Regulamentul General privind protecția datelor în ceea ce privește încălcărea securității datelor cu caracter personal și notificarea către autoritatea competentă a unei astfel de încălcări.
Art. 21	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 informatice.	N/A	În baza Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice ("**Legea nr. 362/2018**"), operatorii care intră sub incidența legii au obligația de a raporta incidentele de securitate cibernetică. Mai mult, OUG nr. 111/2011 stabilește obligația pentru operatorii telecom de a notifica incidentele cu impact semnificativ asupra rețelelor de comunicații electronice. Odată cu transpunerea Directivei NIS 2, obligația de notificare va fi reglementată prin legea de transpunere și va include și operatorii telecom. În acest context, nu este clar cum se vor aplica prevederile Proiectului de lege privind securitatea și apărarea cibernetică a României în situația în care sunt incidente prevederile Legii nr. 362/2018, ale OUG nr. 111/2011 și ulterior ale legii de transpunere a Directivei NIS 2.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

Art. 24 alin (1)	Furnizorii de servicii 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 sistem informatic a deținătorului sau a unor terți.	Furnizorii de servicii de securitate cibernetică **care oferă servicii de securitate cibernetică autorităților prevăzute la art. 10**, au obligația de a pune la dispoziția **acestora,** la cererea **lor** motivată, 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 sistem informatic ~~a deținătorului sau a unor terți.~~ **propriu și care pot afecta securitatea naţională.**	Credem că la baza motivării cererii menționate în cadrul art. 24 alin. (1) trebuie să existe o legătura strânsă dintre potențialele „incidente, amenințări, riscuri sau vulnerabilități" și calitatea acestora de a avea un potențial impact la nivelul rețelei sau sistemului propriu al autorităților prevăzute la art. 10 sau care prezintă un risc pentru securitatea națională. În caz contrar, asemenea obligație poate să ducă la obligații duble de raportare, la crearea premiselor înaintării unor solicitări efectuate în absența unui mandat judecătoresc, precum și la încălcarea confidențialității datelor clienților acestor furnizori.
Art. 33 alin. (1) lit. e)	(1) Cooperarea în domeniul securității și apărării cibernetice la nivel național are următoarele obiective: (...) e) dezvoltarea și implementarea de soluții de securitate cibernetică;	N/A	Din formularea textului de lege nu este clar cui se adresează aceste soluții de securitate cibernetică și dacă acestea trebuie în mod obligatoriu implementate de anumite entități.
Art. 34 lit. g)	Cooperarea internațională în domeniile securității și apărării cibernetice are următoarele obiective: g) evaluarea și implementarea de soluții revoluționare de securitate cibernetică,	N/A	Similar cu cele menționate în legătură cu articolul 33 alineatul (1) litera e) de mai sus, nu este clar cui îi vor fi adresate aceste soluții de securitate cibernetică. Mai mult, considerăm important a se clarifica care va fi statutul sistemele

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

	precum și adoptarea de concepte noi de proiectare și utilizare a tehnologiilor emergente în spațiul cibernetic;		europene de certificare a securității cibernetice, adoptate în baza Regulamentului (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).
Art. 40	(1) Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare. (2) Riscurile lanțului de aprovizionare includ: livrarea de soluții informatice contrafăcute, producție neautorizată, manipulare frauduloasă, inserarea de componente și servicii software și hardware periculoase, spionaj, compromiteri neintenționate, practice deficitare de fabricație și dezvoltare de produse. (...)	(1) Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare. (2) Riscurile lanțului de aprovizionare includ: **legalitatea existenței furnizorului**. ~~livrarea de soluții informatice contrafăcute, producție neautorizată manipulare frauduloasă, inserarea de componente și servicii software și hardware periculoase spionaj compromiteri neintenționate practice deficitare de fabricație și dezvoltare de produse~~	În mediul comercial verificarea extensivă a produselor informatice este de multe ori un demers care nu se poate realiza (ex. lipsa capacității obiective de a analiza un produs, lipsa accesului la codul sursă etc), astfel, există o incapacitate obiectivă de a cunoaște, respectiv verifica, anumite aspecte despre soluțiile utilizate în cadrul companiei (în speță, riscuri asociate lanțului de aprovizionare), precum cele propuse spre eliminare în coloana precedentă (*livrarea de soluții informatice contrafăcute*, *producție neautorizată, manipulare frauduloasă, inserarea de componente și servicii software și hardware periculoase, spionaj, practici deficitare de fabricație și dezvoltare de produse)* în timp ce, cu privire la

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			compromiterile neintenționate, acest aspect se poate regăsi în toate produsele software existente pe piață, întrucât niciun furnizor nu poate garanta un grad de vulnerabilitate 0. Procesele care pot fi implementate la nivel de achiziție pot viza doar verificarea din punct de vedere al legalității existenței entității care furnizează produsele mai sus menționate, și nu verificarea in extenso a produselor în sine. Pe de altă parte, Directiva NIS 2 (adoptată recent de către Parlamentul European) conține o serie de prevederi în legătură cu evaluarea și managementul riscului de securitate cibernetică specifice lanțului de aprovizionare (a se vedea în acest sens recitalurile 59, 85, 90 și 91, precum și articolele 7 alineatul (2) litera a), 14 alineatul (4) litera i), 21 și 22). În acest sens, considerăm important să se asigure corelarea prevederilor prezentului proiect de lege cu cele din Directiva NIS 2. În caz contrar, există riscul de a avea prevederi contradictorii sau care dublează în mod nejustificat obligațiile impuse în sarcina entităților private.

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

Art. nou	N/A	*În legătură cu, între altele, Art. 24 din proiectul de lege, se propune adăugarea unui capitol nou cu conținutul următor:* **Capitolul [X]. Confidențialitatea și protecția securității datelor și informațiilor entităților private** **(1) Dezvăluirea de date și informații de către entități private, inclusiv notificarea de incidente de securitate și interceptarea de date și informații de către autoritățile publice prevăzute la art. 10 de mai sus, potrivit prevederilor acestei legi și reglementărilor și măsurilor adoptate în aplicarea acesteia, va fi efectuată în condițiile menționate în actele de autorizare dispuse în conformitate cu dispozițiile Legii nr. 135/2010 privind Codul de procedură penală, cu modificările și completările ulterioare, și ale Legii nr. 51/1991 privind securitatea națională a României, republicată, cu modificările și completările ulterioare.** **(2) Autoritățile prevăzute la art. 10 care solicită și primesc date și informații de la orice entitate privată în temeiul acestei legi vor lua măsuri adecvate pentru a proteja interesele de securitate și comerciale ale**	Modificările propuse au în vedere stabilirea unor garanții cu privire la dezvăluirea de informații de către entitățile private către autorități publcie, având în vedere că acestea pot include informații protejate de secretul comercial sau date cu caracter personal.

AMERICAN CHAMBER OF COMMERCE IN ROMANIA

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

		entităților de natură privată care furnizează datele și informațiile respective și ale entităților la care se referă datele și informațiile respective, precum și confidențialitatea datelor și informațiilor furnizate. **(3) Transmiterea de date și informații obținute potrivit acestei legi de la orice entități de natură privată poate fi efectuată numai pentru îndeplinirea obiectivelor prevăzute de prezenta lege, cu garantarea păstrării confidențialității datelor cu caracter personal și a protecției intereselor și secretelor comerciale ale entităților private.**	