EXPUNERE DE MOTIVE

Secţiunea 1
Titlul proiectului de act normativ

Lege privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice

Secţiunea a 2-a
Motivul emiterii actului normativ

1. Descrierea situaţiei actuale

Cadrul normativ european

În iulie 2016 a fost adoptată *Directiva (UE) 2016/1148*[1] *privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune*, aceasta fiind primul act legislativ al Uniunii privind securitatea reţelelor şi sistemelor informatice menit să transpună obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS.

Directiva creează structurile necesare pentru cooperarea strategică şi operaţională între statele membre şi pentru creşterea nivelului de reziliență al reţelelor şi al sistemelor informatice de pe teritoriul UE.

Constatând faptul că amploarea, frecvenţa şi impactul incidentelor de securitate este în creştere, reprezentând o ameninţare gravă pentru funcţionarea reţelelor şi a sistemelor informatice, fapt ce poate împiedica desfăşurarea activităţilor economice şi genera pierderi financiare substanţiale subminând încrederea utilizatorilor şi provocând pagube majore economiei Uniunii, Directiva impune o abordare globală la nivelul Uniunii, care să includă cerinţe comune privind crearea capacităţilor minime şi planificarea, schimb de informaţii, cooperare şi cerinţe comune de securitate pentru operatorii de servicii esenţiale şi furnizorii de servicii digitale, fără a-i împiedica pe aceştia să adopte măsuri de securitate mai stricte decât cele prevăzute de Directivă.

Directiva stabileşte data de 9 mai 2018 ca moment până la care statele membre să transpună şi să adopte în legislaţia naţională actele normative cu putere de lege şi actele administrative care să asigure:

1. Adoptarea unei strategii de securitate a reţelelor şi sistemelor informatice;
2. Stabilirea uneia sau mai multe autorităţi naţionale competente în domeniul NIS;

[1] Jurnalul Oficial al Uniunii Europene L 194/1, 19.7.2016

3. Stabilirea punctului național unic de contact;

4. Stabilirea și dotarea corespunzătoare a uneia sau mai multor echipe naționale de răspuns la incidente de Securitate cibernetică (echipa CSIRT națională);

5. Inițierea unui proces de identificare a operatorilor de servicii esențiale (OSE);

6. Stabilirea cerințelor minime de securitate pentru operatorii de servicii esențiale și furnizorii de servicii digitale (FSD);

7. Stabilirea cerințelor de notificare a incidentelor de securitate survenite la nivelul rețelelor și sistemelor OSE și FSD;

8. Crearea cadrului național și a mecanismelor care să garanteze aplicarea prevederilor Directivei;

9. Crearea cadrului național de cooperare și răspuns coordonat la incidentele de securitate survenite la nivelul rețelelor OSE și FSD;

10. Participarea în organismele și în cadrul mecanismelor de cooperare la nivel uniunii, respective la Grupul de Cooperare în vederea coordonării la nivel strategic și în cadrul Rețelei CSIRT în răspunsul comun la incidentele cu impact la nivel European.

11. Raportarea periodică de date privind progresul transpunerii și eficiența aplicării, permițând Comisiei evaluarea la nivel UE a acestora.

Directiva prevede totodată reguli de aplicabilitate raportat la reglementările privind securitatea rețelelor și sistemelor cuprinse în alte norme europene precum și de cooperare și relaționare cu autorități din celelalte domenii precum asigurarea ordinii publice, protecția datelor cu caracter personal, precum și delimitarea de acțiunile statelor membre întreprinse pentru salvgardarea funcțiilor lor esențiale de stat, în special pentru salvgardarea securității naționale.

Astfel până la 9 noiembrie 2018, statele membre identifică operatorii de servicii esențiale care au un sediu pe teritoriul lor. Identificarea se face pentru fiecare sector și subsector din anexa II a Directivei.

Sectoarele vizate pentru identificarea serviciilor esențiale și a operatorilor de servicii esențiale cuprind: energia, transporturile, sectorul bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructura digitală.

Cerințele de securitate și notificare aplicabile operatorilor de servicii esențiale stabilite de Directivă sunt mai stricte decât cele aplicabile furnizorilor de servicii digitale, dată fiind importanța sub aspectul impactului incidentelor ce pot surveni la nivelul rețelelor și sistemelor acestora. Cu toate acestea OSE vor notifica și impactul asupra serviciilor esențiale datorat unor incidente la nivelul unor furnizori de servicii digitale pe care se bazează furnizarea serviciului esențial.

Regimul sancționator cerut de Directivă pentru nerespectarea cerințelor de securitate și notificare trebuie să fie eficace, proporțional și disuasiv, statele membre garantând punerea în aplicare a acestora.

În baza notificărilor privitoare la incidente, Directiva prevede stabilirea amplorii acestuia și determinarea afectării altor entități, în special stabilirea impactului transfrontalier și alertarea și cooperarea cu statele potențial afectate în managementul incidentelor.

Prelucrarea datelor cu caracter personal în aplicarea directivei se va face în conformitate cu legislația aplicabilă prelucrării datelor cu caracter personal.

Autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, păstrează interesele de securitate și comerciale ale operatorilor și furnizorilor vizați de directivă, precum și confidențialitatea informațiilor furnizate în notificări și în cursul administrării incidentelor, această cerință a directivei NIS constituind fundament pentru stabilirea încrederii și cooperării în domeniul asigurării securității rețelelor și sistemelor informatice.

Pentru ducerea la îndeplinire a obiectivelor, Directiva impune statelor membre alocarea de resurse suficiente și adecvate autorităților competente la nivel național, punctului unic de contact și echipei CSIRT naționale pentru desfășurarea activităților, asigurând atât condiții tehnice adecvate, locații securizate, sisteme de comunicații reziliente cât și resursele umane necesare, obligații ce se regăsesc atât în cuprinsul directivei cât și în anexa I a acesteia.

Cadrul normativ național

La nivel național, în domeniul securității, există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar, cum ar fi:

- Ordonanța de urgență a Guvernului nr.98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr.757 din 12 noiembrie 2010, aprobată prin Legea nr.18/2011, publicată în Monitorul Oficial al României, Partea I, nr.183 din 16 martie 2011, cu modificările și completările ulteriorare, stabilește cadrul legal privind identificarea, desemnarea infrastructurilor critice naționale/europene și evaluarea necesității de a îmbunătăți protecția acestora, în scopul creșterii capacității de asigurare a stabilității, securității și siguranței sistemelor economico-sociale și protecției persoanelor. Legea transpune prevederile Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008. Actul normativ definește infrastructura critică națională, denumită ICN ca fiind un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții. Actul normativ stabilește criteriile intersectoriale de identificare a ICN: criteriul privind victimele, evaluat în funcție de numărul posibil de decese sau vătămări; criteriul privind efectele economice, evaluat în funcție de importanța pierderilor economice și/sau a degradării produselor sau serviciilor, inclusiv eventualele efecte asupra mediului; criteriul privind efectul asupra populației, evaluat în funcție de impactul asupra încrederii acesteia, suferința fizică sau perturbarea vieții cotidiene, inclusiv pierderea de servicii esențiale. În conformitate cu procedura prevăzută de ordonanța de urgență, autoritățile publice responsabile identifică potențialele ICN care corespund criteriilor sectoriale și intersectoriale. Actul normativ conține 3 anexe: anexa nr.1 - Lista sectoarelor, subsectoarelor infrastructurii critice naționale/infrastructurii critice europene (ICN/ICE) și

autorităţilor publice responsabile; anexa nr.2 - Procedura de identificare de către autorităţile publice responsabile de infrastructuri critice care pot fi desemnate drept infrastructuri critice naţionale/infrastructuri critice europene (ICN/ICE) şi anexa nr.3 - Procedura privind planul de securitate pentru operator.

În aplicarea ordonanţei de urgenţă, Guvernul a emis Hotărârea Guvernului nr.718/2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critic, publicată în Monitorul Oficial al României, Partea I, nr.555 din 4 august 2011, prin care aprobă Strategia naţională privind protecţia infrastructurilor critice.

Hotărârea Guvernului nr. 494/2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, reglementează înfiinţarea ca instituţie publică cu personalitate juridică, în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, a Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice, definind totodată termeni şi expresii precum infrastructură cibernetică, spaţiu cibernetic, securitate cibernetică, atac cibernetic, incident cibernetic etc.

Un alt act normativ emis în domeniul securităţii naţionale îl constituie 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, publicată în Monitorul Oficial al României, Partea I, nr. 296 din 23 mai 2013.

Strategia de securitate cibernetică prezintă obiectivele, principiile şi direcţiile majore de acţiune pentru cunoaşterea, prevenirea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor la adresa securităţii cibernetice a României şi pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic. În acest sens, stabileşte semnificaţia termenilor şi expresiilor utilizaţi în domeniu, prevede înfiinţarea Sistemului naţional de securitate cibernetică (SNSC) care reprezintă cadrul general de cooperare care reuneşte autorităţi şi instituţii publice, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile neguvernamentale. De asemenea, prevede că Consiliul operativ de securitate cibernetică (COSC) reprezintă organismul prin care se realizează coordonarea unitară a SNSC. Din COSC fac parte, în calitate de membri permanenţi, reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Telecomunicaţii Speciale, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază, Oficiului Registrului Naţional pentru Informaţii Secrete de Stat, precum şi secretarul Consiliului Suprem de Apărare a Ţării. Conducerea COSC este asigurată de un preşedinte (consilierul prezidenţial pe probleme de securitate naţională) şi un vicepreşedinte (consilierul prim-ministrului pe probleme de securitate naţională). Coordonatorul tehnic al COSC este Serviciul Român de Informaţii, în condiţiile legii.

Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică este conţinut în anexa nr.2 la Hotărâre şi este un document clasificat.

Prin Hotărârea Guvernului nr. 494/2011, Centrul național de răspuns la incidente de securitate cibernetică - CERT-RO are o serie de atribuții similare celor din Directiva 1148/2016 fiind Centru Național de Răspuns la Incidente de Securitate Cibernetică cu atribuții si de punct de contact cu celelalte echipe CERT.

Cu toate acestea, nu există prevederi unitare în legislația națională privitoare la notificarea în sensul Directivei NIS a incidentelor de securitate a rețelelor și sistemelor informatice.

O situație similară se constată și în privința cerințelor de securitate a rețelelor și sistemelor informatice, la nivel național existând doar cerințe specifice derivate din transpunerea unor acte normative europene care reglementează anumite sectoare de activitate.

În conformitate cu art. 25 alin. (1) din directiva 1148/2016 (NIS) România are obligația, în calitate de stat membru al Uniunii Europene, de a asigura transpunerea Directivei în legislația națională până cel târziu la data de 9 mai 2018, toate actele normative cu putere de lege precum și cele administrative necesare trebuind să producă efecte începând cu data de 10 mai 2018.

În cazul nerespectării termenului de transpunere a Directivei 2008/6/CE, Comisia Europeană poate demara acțiunea în constatarea neîndeplinirii obligațiilor în temeiul art. 258 din Tratatul privind Funcționarea Uniunii Europene, iar potrivit art. 260 alin. (2) și (3) din Tratatul privind Funcționarea Uniunii Europene, răspunderea României pentru încălcarea obligațiilor de a transpune Directiva 1148/2016 se poate concretiza atât în plata unei sume forfetare, cât și a unor penalități cu titlu cominatoriu.

2. Schimbări preconizate

Pentru transpunerea prevederilor Directivei 1148/2016 (NIS) în legislația națională este necesară modificarea cadrului legal în sensul transpunerii prin act cu putere de lege a prevederilor directivei, precum și asigurarea prin acte normative și administrative subsecvente a cadrului legal necesar aplicării acesteia.

În acest scop, prin prezentul proiect de act normativ se propune adoptarea unui set de norme coerente, clare și transparente, menite să instituie un cadru național unitar de asigurare a securității informatice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în conformitate cu cerințele Directivei 1148/2016.

Prezentul proiect de act normativ propune:

- stabilirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice
- desemnarea autorităților și entităților de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor prezentei legi, a punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate informatică
- stabilirea cerințelor de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale și instituirea mecanismelor de actualizare a acestora în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice

În vederea delimitării sferei de aplicabilitate a proiectului de act normativ de sfera mai largă a securității cibernetice - așa cum este definită în actele normative la nivel național și care cuprinde și activitățile din domeniile securitate națională și apărare – proiectul preia și utilizează terminologia din Directiva 1148/2016 referindu-se la *securitatea rețelelor și sistemelor informatice*. În același sens, proiectul delimitează explicit activitățile reglementate de cele ale instituțiilor din domeniile apărare și securitate națională prevăzând mecanisme de cooperare în situațiile în care un incident aduce atingere activităților acestor instituții ori prin amploarea sa afectează apărarea sau securitatea națională.

În privința autorității competente la nivel național, a punctului unic și a echipei CSIRT naționale proiectul propune dezvoltarea acestora în cadrul aceleiași instituții, respectiv a Centrului Național de Răspuns la Incidente de Securitate - CERT-RO care îndeplinește în prezent rolul de CSIRT/CERT național, reprezintă România în grupul de cooperare și este punct unic de contact cu celelalte echipe CERT la nivel național și internațional.

Proiectul preia definițiile specifice enunțate în directivă integrând totodată la art. 3 lit o) cuprinsul anexei III a Directivei în sensul delimitării furnizorilor de servicii digitale la categoriile din respectiva anexă și aliniază o serie de definiții la cele exitente la nivel național.

În vederea asigurării unei aplicări unitare, proiectul definește un set de trei principii, respectiv principiul responsabilității și conștientizării, principiul proporționalității și principiul cooperării și coordonării.

Pentru definirea transparentă și cu claritate a domeniului de aplicare, proiectul propune definirea operatorilor de servicii esențiale raportat la anexa cu sectoare și subsectoare de activitate (anexa II a Directivei) și la definirea serviciilor esențiale respectiv la modalitatea de analiza a gradului de perturbare a furnizării unui serviciu esențial, enunțând criteriile trans-sectoriale de analiză, urmând a fi emise prin hotărâre de guvern valorile de prag și criteriile specifice fiecărui sector de activitate.

Proiectul propune alcătuirea unui Registru al operatorilor de servicii esențiale, înscrierea în acesta putându-se face fie voluntar prin notificarea transmisă de operator autorității competente la nivel național – CERT-RO, fie din oficiu în urma verificărilor efectuate de către CERT-RO.

Pentru a diminua din sarcina financiară legată de efectuarea auditurilor de securitate la înscrierea în Registru, în condițiile în care transpunerea Directivei impune cerințe de securitate în sarcina operatorilor și furnizorilor vizați ce implică costuri, operatorii de servicii esențiale se pot înscrie în primii doi ani de la adoptarea actului normativ prin notificare voluntară în vederea înscrierii și depunerea unei declarații pe proprie răspundere însoțită de documentațiile aferente. Totodată, operatorii de servicii esențiale pot solicita sprijinul autorității în procesul de identificare.

Proiectul prevede dreptul autorității de a solicita operatorilor economici informațiile și documentațiile necesare pentru a determina dacă aceștia se încadrează în categoria operatori de servicii esențiale, pentru a permite și identificarea din oficiu de către autoritate în cazul sustragerii de la obligația de notificare și înscriere în Registru, prevăzând și sancțiuni în acest caz.

În privința furnizorilor de servicii digitale, proiectul nu prevede alcătuirea unui registru al acestora, însă permite autorității identificarea acestora în vederea stabilirii îndeplinirii cerințelor de securitate și notificare, proiectul preluând excepțiile de la aplicare și cerințele mai reduse ce se aplică acestora, conform Directivei.

În vederea coordonării la nivel național în managementul incidentelor, proiectul de act normativ prevede furnizarea de către CERT-RO a unui serviciu de alertare și cooperare la care se vor interconecta operatorii și furnizorii prevăzuți de prezentul proiect de act normativ, stabilind totodată obligația acestora de a monitoriza alertele primite și a asigura răspunsul prompt în caz de necesitate.

Sub aspectul cerințelor de securitate și notificare, proiectul prevede cerințele și capitolele minimale, instituind mecanismul de actualizare și publicare a acestora de către autoritatea competentă la nivel național în urma consultărilor cu celelalte autorități, astfel încât cerințele să poată evolua în pas cu evoluția amenințărilor cât și a tehnologiilor.

Proiectul statuează utilizarea standardelor internaționale, fără a impune sau discrimina în favoarea unei anumite tehnologii în soluțiile impuse.

Sub aspectul confidențialității, întrucât cerința Directivei este ca echipele CSIRT și autoritățile competente la nivel național să păstreze confidențialitatea informațiilor primite de la operatori și furnizori în cadrul notificărilor, proiectul statuează reguli clare atât privind confidențialitatea cât și sub aspectul comunicării publice în cadrul managementului unor incidente.

Proiectul de act normativ prevede instituirea unui mecanism de primire și triaj de către CERT-RO a notificărilor astfel încât să fie îndeplinite atât condițiile cerute de Directivă de evaluare a impactului la nivel transfrontalier cât și de alertare și cooperare cu celelalte instituții și entități care pot fi afectate ori pot contribui la remedierea situației, prevăzând și o platformă de cooperare cu echipele CSIRT pentru realizarea rapidă și eficientă a intervențiilor.

Proiectul de act normativ își propune stimularea dezvoltării pieței de securitate informatică în acest sens definind un set de măsuri care privesc piața de audit de securitate pentru rețelele și sistemele operatorilor și furnizorilor vizați cât și piața de servicii de securitate informatică de tip CSIRT, astfel:

- deși Directiva NIS statuează posibilitatea realizării de către autoritățile competente la nivel național a auditurilor de securitate, proiectul adoptă varianta realizării auditurilor de către auditori independenți, prevăzând însă un mecanism pentru atestarea acestora care să asigure menținerea unui nivel al auditului corespunzător cu evoluția amenințărilor și tehnologiilor.
- o soluție similară este propusă și pentru echipele CSIRT care deservesc OSE și FSD și pentru cele sectoriale, proiectul propunând un sistem de autorizare a acestora.
- pentru a stimula furnizarea de servicii de formare corespunzător cu evoluția amenințărilor și tehnologiilor, proiectul propune de asemeni un sistem de acreditare formatorilor și furnizorilor de servicii de formare pentru auditorii și echipele CSIRT vizate.
- Cele trei servicii se limitează însă doar la acei auditori ori furnizori de servicii de tip CSIRT care deservesc operatori de servicii esențiale ori furnizori de servicii digitale.

Sub aspectul regimului sancționator, proiectul oferă autorității competente la nivel

național – CERT-RO dreptul de realizare a controlului implementării cerințelor de securitate și notificare, precum și de îndeplinire a obligațiilor de către celelalte entități vizate de proiect, definind un set de contravenții și sancțiuni în linie cu cerințele directivei și oferind un set de garanții în privința contestării acestora.

Până la 9 noiembrie 2018, statele membre identifică operatorii de servicii esențiale care au un sediu pe teritoriul lor. Sectoarele vizate pentru identificarea serviciilor esențiale și a operatorilor de servicii esențiale cuprind: energia, transporturile, sectorul bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructura digitală precum și administrație publică.

În procesul de identificare a operatorilor de servicii esențiale, în cadrul autorității competente la nivel național se constituie Registrul operatorilor de servicii esențiale. Întrucât Registrul cuprinde lista operatorilor de o importanță deosebită în furnizarea serviciilor esențiale la nivel național, Registrul va face parte din categoria documentelor clasificate.

Strategia națională privind securitatea rețelelor și a sistemelor informatice, menționată în proiect este diferită de strategia de securitate cibernetică a României, prezentul proiect neaducând atingere activităților de asigurare a securității naționale și apărării.

Proiectul are drept scop asigurarea unui nivel ridicat de securitate a rețelelor și a sistemelor informatice la nivel național și creșterea capacității de prevenție, răspuns și a pregătirii naționale la nivelul cerut pentru asigurarea unui răspuns unitar la nivelul Uniunii Europene.

În acest scop, proiectul stabilește cerințe comune pentru operatorii de servicii esențiale și furnizorii de servicii digitale precum și mecanisme de actualizare și aliniere a acestor cerințe la cele comunitare.

Pentru a răspunde eficient la provocările din domeniul securității rețelelor și a sistemelor informatice, se impune o abordare globală la nivelul României, care să includă cerințe comune privind crearea capacităților minime și planificarea, schimb de informații, cooperare și cerințe comune de securitate pentru operatorii de servicii esențiale și furnizorii de servicii digitale. Cu toate acestea, operatorii de servicii esențiale și furnizorii de servicii digitale nu sunt împiedicați să pună în aplicare măsuri de securitate care să fie mai stricte decât cele prevăzute în temeiul prezentului proiect de act normativ.

Pentru a putea acoperi toate incidentele și riscurile relevante, prezentul proiect de act normativ ar trebui să se aplice atât operatorilor de servicii esențiale, cât și furnizorilor de servicii digitale. Cu toate acestea, obligațiile care revin operatorilor de servicii esențiale și furnizorilor de servicii digitale nu ar trebui să se aplice nici întreprinderilor care pun la dispoziție rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului în sensul Directivei 2002/21/CE a Parlamentului European și a Consiliului, cărora li se aplică cerințele specifice de securitate și integritate prevăzute în directiva respectivă, nici furnizorilor de servicii de încredere în sensul Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului (4), cărora li se aplică cerințele de securitate prevăzute în regulamentul respectiv.

Prezentul proiect de act normativ nu ar trebui să aducă atingere posibilității de care dispune România de a lua măsurile necesare pentru a asigura protecția intereselor sale esențiale de securitate, a apăra ordinea și siguranța publică și a permite investigarea,

detectarea şi urmărirea infracţiunilor.

Anumite sectoare ale economiei sunt deja reglementate sau ar putea fi reglementate în viitor prin acte normative ale Uniunii Europene specifice fiecărui sector care includ norme legate de securitatea reţelelor şi a sistemelor informatice. Atunci când aceste acte juridice ale Uniunii conţin dispoziţii care impun cerinţe privind securitatea reţelelor şi a sistemelor informatice sau notificarea incidentelor, aceste dispoziţii ar trebui să se aplice în cazul în care conţin cerinţe care sunt cel puţin echivalente ca efect cu obligaţiile conţinute în prezentul proiect de act normativ. În acest caz, România ar trebui să aplice dispoziţiile unor astfel de acte juridice ale Uniunii specifice fiecărui sector, inclusiv cele privind jurisdicţia, şi nu ar trebui să execute procesul de identificare pentru operatorii de servicii esenţiale definit de prezentul proiect de act normativ. În acest context, România va furniza Comisiei Europene informaţii privind aplicarea dispoziţiei privind astfel de dispoziţii de lex specialis.

În sectorul transportului pe apă, cerinţele de securitate pentru societăţi, nave, instalaţii portuare, porturi şi servicii de trafic naval în temeiul actelor juridice ale Uniunii Europene reglementează toate operaţiunile, inclusiv sistemele de radio şi telecomunicaţii, sistemele informatice şi reţelele. Printre procedurile obligatorii care trebuie să fie urmate se numără raportarea tuturor incidentelor şi ar trebui, prin urmare, să fie considerate lex specialis, în măsura în care cerinţele respective sunt cel puţin echivalente cu dispoziţiile corespunzătoare ale prezentului proiect de act normativ.

La identificarea operatorilor din sectorul transportului pe apă, România ar trebui să ţină cont de codurile şi orientările internaţionale existente şi viitoare elaborate în special de Organizaţia Maritimă Internaţională, pentru a se oferi operatorilor maritimi individuali o abordare coerentă.

Riscul operaţional reprezintă o parte esenţială a reglementării şi supravegherii prudenţiale în sectoarele infrastructurilor bancare şi ale pieţei financiare. Acesta acoperă toate operaţiunile, inclusiv securitatea, integritatea şi reziliența reţelelor şi a sistemelor informatice. Cerinţele cu privire la aceste sisteme, care depăşesc adesea cerinţele prevăzute în temeiul prezentului proiect de act normativ, figurează în mai multe acte juridice ale Uniunii Europene, inclusiv în normele privind accesul la activitatea instituţiilor de credit şi supravegherea prudenţială a instituţiilor de credit şi a firmelor de investiţii şi în normele privind cerinţele prudenţiale pentru instituţiile de credit şi firmele de investiţii, care includ cerinţe privind riscul operaţional; norme privind pieţele instrumentelor financiare, care includ cerinţe privind evaluarea riscului pentru firmele de investiţii şi pentru pieţele reglementate, dar şi în normele privind instrumentele financiare derivate extrabursiere, contrapartidele centrale şi registrele centrale de tranzacţii, care includ cerinţe privind riscul operaţional pentru contrapartidele centrale şi registrele centrale de tranzacţii şi în normele privind îmbunătăţirea decontării titlurilor de valoare în Uniune şi privind depozitarele centrale pentru instrumente financiare, care includ cerinţe privind riscul operaţional. În plus, cerinţele de notificare a incidentelor fac parte din practica normală de supraveghere în sectorul financiar şi sunt incluse adesea în manualele de supraveghere. România trebuie să ia în considerare dispoziţiile şi cerinţele respective atunci când aplică lex specialis.

Conform avizului Băncii Centrale Europene din 25 iulie 2014, Directiva NIS nu

afectează regimul de supraveghere, în temeiul dreptului Uniunii, de către Eurosistem a sistemelor de plată şi de decontare. Este necesar ca autoritățile responsabile pentru această supraveghere să facă schimb de experienţă în aspecte legate de securitatea reţelelor şi a sistemelor informatice cu autoritățile competente în temeiul directivei NIS. Aceeaşi consideraţie se aplică şi membrilor Sistemului European al Băncilor Centrale care nu fac parte din zona euro, care exercită această supraveghere a sistemelor de plată şi de decontare pe baza actelor legislative şi de reglementare naţionale.

O piaţă online ar trebui să permită consumatorilor şi comercianţilor să încheie contracte de vânzări sau servicii online cu comercianţii şi reprezintă destinaţia finală pentru încheierea acestor contracte. Aceasta nu ar trebui să includă servicii online care folosesc doar ca intermediar pentru servicii prestate de o parte terţă prin care în final se încheie un contract. Prin urmare, aceasta nu ar trebui să includă serviciile online care compară preţul anumitor produse sau servicii de la diferiţi comercianţi şi reorientează apoi utilizatorul la comerciantul preferat pentru achiziţionarea produsului. Serviciile de calcul oferite de piaţa online pot include tratarea tranzacţiilor, cumularea datelor sau profilarea utilizatorilor. Magazinele de aplicaţii, care funcţionează ca magazine online, permiţând distribuţia digitală a aplicaţiilor sau a programelor software de la părţi terţe, urmează să fie înţelese ca un tip de piaţă online.

Un motor de căutare online permite utilizatorului să efectueze căutări în principiu pe toate site-urile internet pe baza unei interogaţii pe orice subiect. Alternativ, această căutare s-ar putea concentra pe site-uri internet într-o anumită limbă. Definiţia unui motor de căutare online prevăzută de prezentul proiect de act normativ nu ar trebui să cuprindă funcţiile de căutare limitate la conţinutul unui anumit site internet, chiar şi atunci când funcţia de căutare este furnizată de un motor de căutare extern. De asemenea, aceasta nu ar trebui să acopere serviciile online care compară preţul anumitor produse sau servicii de la diferiţi comercianţi şi reorientează apoi utilizatorul la comerciantul preferat pentru achiziţionarea produsului.

Serviciile de cloud computing includ o gamă largă de activităţi care pot fi oferite în funcţie de diferite modele. În sensul prezentului proiect de act normativ, „servicii de cloud computing" înseamnă servicii care permit accesul la un bazin redimensionabil şi elastic de resurse informatice care pot fi puse în comun. Noţiunea „resurse informatice" include resurse precum reţelele, serverele sau alte infrastructuri, stocarea, aplicaţiile şi serviciile. Noţiunea de „redimensionabil" se referă la resursele informatice care se alocă flexibil de către furnizorul de servicii cloud, indiferent de poziţia geografică a resurselor, pentru a administra fluctuaţiile de cerere. Noţiunea „bazin elastic" descrie acele resurse informatice care sunt atribuite şi transferate în funcţie de cerere, pentru a înmulţi şi a reduce rapid resursele disponibile în conformitate cu necesarul de lucru. Sintagma „care pot fi puse în comun" descrie acele resurse informatice care sunt furnizate mai multor utilizatori care au acces comun la serviciu, dar tratamentul se efectuează separat pentru fiecare utilizator, deşi serviciul este furnizat de acelaşi echipament electronic.

Funcţia unui internet exchange point (IXP) este de a interconecta reţele. Un IXP nu oferă acces la reţea şi nici nu acţionează ca furnizor sau transportator de tranzit. De asemenea, un IXP nu furnizează nici alte servicii care nu au legătură cu interconectarea (deşi aceasta nu împiedică un operator IXP să furnizeze şi astfel de servicii). Un IXP

există pentru a interconecta rețele separate din punct de vedere tehnic și organizațional. Noțiunea de „sistem autonom" se utilizează pentru a descrie o rețea care se autosusține din punct de vedere tehnic.

România este responsabilă pentru stabilirea entităților care îndeplinesc criteriile definiției operatorului de servicii esențiale. Pentru a se asigura o abordare uniformă, toate statele membre ar trebui să aplice în mod consistent definiția operatorului de servicii esențiale. În acest scop, prezentul proiect de act normativ prevede evaluarea entităților active în sectoare și subsectoare specifice, instituirea unei liste de servicii esențiale, luarea în considerare a unei liste comune a factorilor transsectoriali care urmează să stabilească dacă un incident potențial ar avea un efect perturbator semnificativ, un proces de consultare care să implice statele membre relevante în cazul entităților care furnizează servicii în mai multe state membre și sprijinul grupului de cooperare în procesul de identificare. Pentru a asigura reflectarea corectă a posibilelor modificări în piață, România ar trebui să revizuiască periodic lista operatorilor identificați și ar trebui să o actualizeze atunci când este necesar. România ar trebui să transmită Comisiei informațiile necesare pentru a evalua măsura în care această metodologie comună permite o aplicare coerentă a definiției de către statele membre.

În procesul de identificare a operatorilor de servicii esențiale, România ar trebui să evalueze, cel puțin pentru fiecare subsector menționat în prezentul proiect de act normativ, care dintre servicii trebuie să fie considerate drept esențiale pentru susținerea activităților societale și economice de cea mai mare importanță și să evalueze dacă entitățile enumerate în sectoarele și în subsectoarele menționate în prezentul proiect de act normativ care furnizează serviciile respective îndeplinesc criteriile de identificare a operatorilor. Atunci când se evaluează dacă o entitate furnizează un serviciu esențial pentru susținerea activităților societale și economice de cea mai mare importanță, este suficient să se examineze dacă o anumită entitate furnizează un serviciu inclus pe lista serviciilor esențiale. În plus, ar trebui să se demonstreze că furnizarea unui serviciu esențial depinde de rețele și de sisteme informatice. În sfârșit, atunci când evaluează dacă un incident ar avea un efect perturbator semnificativ asupra furnizării serviciului, România ar trebui să țină cont de mai mulți factori transsectoriali, precum și, după caz, de factorii sectoriali specifici.

Pentru identificarea operatorilor de servicii esențiale, instituirea în România implică exercitarea efectivă și reală a activității prin acorduri stabile. Forma juridică a acestor acorduri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

Este posibil ca entitățile care operează în sectoarele și subsectoarele menționate în prezentul proiect de act normativ să furnizeze atât servicii esențiale, cât și neesențiale. De exemplu, în sectorul transportului aerian, aeroporturile furnizează servicii care pot fi considerate de către un stat membru ca fiind esențiale, precum gestionarea pistelor de aterizare/decolare, dar și mai multe servicii care pot fi considerate neesențiale, precum furnizarea de spații comerciale. Operatorii de servicii esențiale ar trebui să facă obiectul unor cerințe de securitate specifice doar în legătură cu serviciile considerate esențiale. Pentru identificarea operatorilor, România ar trebui, prin urmare, să stabilească o listă a serviciilor considerate drept esențiale.

Lista serviciilor ar trebui să conțină toate serviciile furnizate pe teritoriul României care îndeplinesc cerințele prevăzute de prezentul proiect de act normativ. Proiectul include mecanismul de actualizare și includere de noi servicii pe lista serviciilor esențiale. Lista serviciilor ar trebui să servească drept punct de referință, permițând identificarea operatorilor de servicii esențiale. Scopul acesteia este de a identifica tipurile de servicii esențiale în orice sector dat menționat în prezentul proiect de act normativ, distingându-le, astfel, de activitățile neesențiale de care ar putea fi răspunzătoare o entitate activă în orice sector determinat. Lista serviciilor instituită de România ar servi drept informație suplimentară în evaluarea practicii de reglementare a fiecărui stat membru, în vederea asigurării nivelului general de coerență între statele membre ale Uniunii Europene al procesului de identificare.

În sensul procesului de identificare, atunci când o entitate furnizează un serviciu esențial în două sau mai multe state membre, statele membre respective ar trebui să intre în discuții bilaterale sau multilaterale unele cu altele. Acest proces de consultare este destinat să le ajute să evalueze importanța operatorului din punct de vedere al impactului transfrontalier și să permită fiecărui stat membru implicat să își exprime opiniile în privința riscurilor asociate serviciilor furnizate. România ar trebui să țină cont de opiniile exprimate de fiecare dintre ele în cadrul acestui proces și poate solicita în această privință asistența grupului de cooperare.

Ca rezultat al procesului de identificare, România ar trebui să adopte la nivel național măsuri prin care se stabilesc entitățile cărora le revin obligații referitoare la securitatea rețelelor și a sistemelor informatice. Acest rezultat ar putea fi obținut prin adoptarea unei liste care include toți operatorii de servicii esențiale sau prin adoptarea la nivel național a unor măsuri care includ criterii obiective cuantificabile (de exemplu, rezultatele operatorului sau numărul de utilizatori), care permit să se determine căror entități le revin obligații referitoare la securitatea rețelelor și a sistemelor informatice. Măsurile la nivel național deja existente sau cele adoptate în cadrul prezentului proiect de act normativ ar trebui să includă toate măsurile legislative, administrative și de politică permițând identificarea operatorilor de servicii esențiale în temeiul prezentului proiect de act normativ.

Pentru a indica importanța operatorilor de servicii esențiale identificați în raport cu sectorul în cauză, România ar trebui să țină cont de numărul și de dimensiunea operatorilor respectivi, de exemplu în ceea ce privește cota de piață sau cantitatea produsă sau transportată, fără a divulga informații care ar dezvălui care operatori au fost identificați.

Pentru a stabili importanța efectului perturbator al unui incident asupra unui serviciu esențial, România ar trebui să țină cont de o serie de diverși factori, ca de exemplu numărul utilizatorilor serviciului respectiv în scop privat sau profesional. Utilizarea serviciului respectiv poate fi directă, indirectă sau prin intermediere. La evaluarea impactului pe care l-ar putea avea respectivul incident, din punct de vedere al gradului și duratei acestuia, asupra activităților economice și societale sau a siguranței publice, România ar trebui să evalueze și intervalul de timp probabil până când discontinuitatea ar începe să aibă un impact negativ.

Pentru a stabili dacă un incident ar putea avea un efect perturbator asupra

furnizării unui serviciu, în afara factorilor transsectoriali, ar trebui să se ia în considerare şi factori specifici fiecărui sector. În ceea ce priveşte furnizorii de energie, printre aceşti factori s-ar putea număra volumul sau proporţia de energie generată la nivel naţional; pentru furnizorii de petrol, volumul zilnic; pentru transportul aerian, inclusiv aeroporturile şi transportatorii aerieni, transportul feroviar şi porturile maritime, volumul de trafic naţional şi numărul de pasageri sau de operaţiuni de transport de mărfuri pe an; pentru infrastructurile pieţelor bancare sau financiare, importanţa lor sistemică, pe baza activelor totale sau a raportului dintre activele totale respective şi PIB; pentru sectorul sănătăţii, numărul anual de pacienţi aflaţi în grija furnizorului; pentru producţia, tratarea şi furnizarea de apă, volumul şi numărul şi tipul de utilizatori incluzând, de exemplu, spitale, organizaţii de serviciu public sau persoane fizice, precum şi existenţa surselor de apă alternative care să acopere aceeaşi zonă geografică.

Pentru a atinge şi menţine un nivel ridicat de securitate a reţelelor şi a sistemelor informatice, România ar trebui să aibă o strategie naţională privind securitatea reţelelor şi a sistemelor informatice, care să definească obiectivele strategice şi acţiunile concrete de politică ce trebuie puse în aplicare.

Pentru a facilita cooperarea şi comunicarea transfrontalieră şi pentru a permite aplicarea efectivă a prezentului proiect de act normativ, este necesar ca România, fără a aduce atingere acordurilor de reglementare sectoriale, să desemneze un punct unic de contact la nivel naţional responsabil pentru coordonarea aspectelor legate de securitatea reţelelor şi a sistemelor informatice şi pentru cooperarea transfrontalieră la nivelul Uniunii. Ar trebui să se acorde autorităţii competente şi punctului unic de contact resurse tehnice, financiare şi umane adecvate pentru a se asigura posibilitatea acestora de a-şi îndeplini efectiv şi eficient atribuţiile şi a realiza astfel obiectivele prezentului proiect de act normativ. Având în vedere că prezentul proiect de act normativ vizează îmbunătăţirea funcţionării pieţei interne a Uniunii Europene prin consolidarea încrederii reciproce, este necesar ca organismele abilitate să aibă posibilitatea de a coopera efectiv cu actorii economici şi să fie structurate în consecinţă.

Autoritatea competentă sau echipa de intervenţie în caz de incidente de securitate informatică („CSIRT") ar trebui să primească notificările incidentelor. Punctul unic de contact nu ar trebui să primească direct nicio notificare de incident, cu excepţia cazului în care acţionează. Totuşi, autoritatea competentă sau CSIRT ar trebui să poată atribui punctului unic de contract responsabilitatea de a transmite notificările de incidente punctelor unice de contact ale altor state membre afectate.

Pentru a furniza efectiv informaţii statelor membre şi Comisiei, punctul unic de contact ar trebui să transmită grupului de cooperare un raport de sinteză care ar trebui să fie anonimizat pentru a se păstra confidenţialitatea notificărilor şi identitatea operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale, deoarece informaţiile privind identitatea entităţilor care notifică nu sunt necesare pentru schimbul de bune practici în grupul de cooperare. Raportul de sinteză ar trebui să includă informaţii privind numărul de notificări primite, dar şi să indice natura incidentelor notificate, precum tipurile de încălcări ale securităţii, gravitatea sau durata acestora.

România ar trebui să fie echipată în mod adecvat, din punct de vedere al capacităţii atât tehnice, cât şi organizatorice, pentru a preveni, a detecta, a combate şi a atenua

incidentele şi riscurile la care sunt supuse reţelele şi sistemele informatice. Prin urmare, România ar trebui să se asigure că deţine CSIRT care funcţionează corespunzător, cunoscute şi drept echipe de intervenţie în caz de urgenţă informatică („CERT"), care respectă cerinţele esenţiale pentru a garanta existenţa capacităţilor eficace şi compatibile care să administreze incidentele şi riscurile şi să asigure o cooperare eficientă la nivelul Uniunii. Pentru ca toate tipurile de operatori de servicii esenţiale şi furnizori de servicii digitale să beneficieze de pe urma acestor capacităţi şi a acestei cooperări, România ar trebui să se asigure că toate tipurile sunt acoperite de o CSIRT desemnată. Având în vedere importanţa cooperării internaţionale în privinţa securităţii cibernetice, CSIRT ar trebui să aibă posibilitatea să participe la reţele de cooperare internaţională, în plus faţă de reţeaua CSIRT instituită prin prezenta directivă.

Deoarece majoritatea reţelelor şi a sistemelor informatice au operatori privaţi, cooperarea dintre sectorul public şi cel privat este esenţială. Operatorii de servicii esenţiale şi furnizorii de servicii digitale ar trebui să fie încurajaţi să-şi creeze propriile mecanisme de cooperare informală pentru asigurarea securităţii reţelelor şi a sistemelor informatice. Pentru a încuraja efectiv schimbul de informaţii şi de bune practici, este esenţial să se asigure că operatorii de servicii esenţiale şi furnizorii de servicii digitale care participă la aceste schimburi nu sunt dezavantajaţi ca urmare a cooperării lor.

Informaţiile privind incidentele sunt tot mai valoroase pentru publicul larg şi pentru întreprinderi, în special pentru întreprinderile mici şi mijlocii. În unele cazuri, aceste informaţii se furnizează deja prin site-uri internet la nivel naţional, în limba unei anumite ţări şi sunt orientate în special asupra incidentelor şi evenimentelor cu dimensiune naţională. Având în vedere că întreprinderile operează din ce în ce mai mult transfrontalier şi că cetăţenii utilizează servicii online, informaţiile privind incidentele ar trebui să fie furnizate într-o formă agregată la nivelul Uniunii.

CSIRT-urile participante la reţeaua CSIRT sunt încurajate să furnizeze voluntar informaţiile care urmează să fie publicate pe site-ul internet respectiv, fără a se include informaţii confidenţiale sau sensibile.

Dacă informaţiile sunt considerate a fi confidenţiale în conformitate cu normele Uniunii şi cele naţionale privind secretul comercial, această confidenţialitate ar trebui să fie asigurată atunci când se efectuează activităţile şi se îndeplinesc obiectivele stabilite de prezentul proiect de act normativ.

Prezentul proiect de act normativ se aplică numai administraţiilor publice identificate drept operatori de servicii esenţiale.

Măsurile de gestionare a riscurilor includ măsurile de identificare a oricăror riscuri de incidente, de prevenire, detectare şi administrare a incidentelor şi de diminuare a impactului acestora. Securitatea reţelelor şi a sistemelor informatice include securitatea datelor stocate, transmise şi prelucrate.

Autoritatea competentă ar trebui să îşi păstreze capacitatea de a adopta orientări la nivel naţional privind circumstanţiale în care operatorii de servicii esenţiale sunt obligaţi să notifice incidente.

Numeroase întreprinderi se bazează, pentru furnizarea propriilor servicii, pe furnizori de servicii digitale. Ţinând cont că unele servicii digitale ar putea reprezenta o resursă importantă pentru utilizatorii lor, inclusiv operatorii de servicii esenţiale, şi ţinând

cont că aceşti utilizatori s-ar putea să nu aibă întotdeauna la dispoziţie alternative, prezentul proiect de act normativ ar trebui să se aplice şi furnizorilor de astfel de servicii. Securitatea, continuitatea şi fiabilitatea tipului de servicii digitale menţionat în prezentul proiect de act normativ sunt esenţiale pentru buna funcţionare a multor întreprinderi. O perturbare a unui astfel de serviciu digital ar putea împiedica furnizarea altor servicii care se bazează pe acesta şi ar putea, astfel, să aibă impact asupra unor activităţi economice şi societale esenţiale la nivel naţional sau European. Aceste servicii digitale ar putea fi, prin urmare, de importanţă esenţială pentru buna funcţionare a întreprinderilor care depind de ele şi, mai mult, pentru participarea acestor întreprinderi la piaţa internă europeană şi la comerţul transfrontalier în întreaga Uniune Europeană. Furnizorii de servicii digitale care intră sub incidenţa prezentului proiect de act normativ sunt cei consideraţi că oferă servicii digitale pe care se bazează din ce în ce mai mult numeroase întreprinderi la nivel naţional şi al Uniunii Europene.

Furnizorii de servicii digitale ar trebui să asigure un nivel de securitate proporţional cu gradul de risc prezentat pentru securitatea serviciilor digitale pe care le furnizează, ţinând cont de importanţa serviciilor lor pentru operaţiunile altor întreprinderi din României sau la nivelul Uniunii Europene. În practică, gradul de risc pentru operatorii de servicii esenţiale, care sunt adesea de cea mai mare importanţă pentru întreţinerea unor activităţi societale şi economice esenţiale, este mai mare decât pentru furnizorii de servicii digitale. Prin urmare, cerinţele de securitate pentru furnizorii de servicii digitale ar trebui să fie mai puţin stricte. Furnizorii de servicii digitale ar trebui să rămână liberi să adopte măsuri pe care le consideră adecvate pentru gestionarea riscurilor pentru securitatea reţelelor şi sistemelor lor informatice.

Măsurile tehnice şi organizatorice impuse operatorilor de servicii esenţiale şi furnizorilor de servicii digitale nu ar trebui să implice proiectarea, dezvoltarea sau fabricarea într-un anumit mod a unui anumit produs comercial al tehnologiei informaţiei şi comunicaţiilor.

Operatorii de servicii esenţiale şi furnizorii de servicii digitale ar trebui să asigure securitatea reţelelor şi a sistemelor informatice pe care le utilizează. Acestea sunt în principal reţele şi sisteme informatice private, gestionarea securităţii lor fiind efectuată de către personalul IT intern sau externalizată. Cerinţele în materie de securitate şi de notificare ar trebui să se aplice operatorilor de servicii esenţiale şi furnizorilor de servicii digitale relevanţi, indiferent dacă aceştia asigură ei înşişi întreţinerea propriilor reţele şi sisteme informatice sau externalizează această activitate.

Pentru a evita impunerea unei sarcini financiare şi administrative disproporţionate asupra operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale, cerinţele ar trebui să fie proporţionale cu riscurile la care este expusă reţeaua şi sistemul informatic în cauză, ţinând seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. În cazul furnizorilor de servicii digitale, aceste cerinţe nu ar trebui să se aplice microîntreprinderilor şi întreprinderilor mici.

Prezentul proiect de act normativ nu ar trebui să aducă atingere cerinţelor specifice de securitate pe care autorităţile publice le impun prin contract pentru servicii de cloud computing.

Ţinând cont de diferenţele fundamentale dintre operatorii de servicii esenţiale, în

special de legătura lor directă cu infrastructura fizică, şi furnizorii de servicii digitale, în special natura transfrontalieră a acestora, prezentul proiect de act normativ ar trebui să adopte o abordare diferenţiată în legătură cu nivelul de armonizare în legătură cu aceste două grupuri de entităţi.

Pentru operatorii de servicii esenţiale, România ar trebui să fie capabilă să identifice operatorii relevanţi şi să impună cerinţe mai stricte decât cele prevăzute de prezentul proiect de act normativ. România nu ar trebui să identifice furnizorii de servicii digitale, deoarece prezentul proiect de act normativ ar trebui să se aplice tuturor furnizorilor de servicii digitale din domeniul său de aplicare. În plus, prezentul proiect de act normativ şi actele de punere în aplicare a Directivei NIS ar trebui să asigure un nivel ridicat de armonizare pentru furnizorii de servicii digitale în ceea ce priveşte cerinţele de securitate şi de notificare. Aceasta ar trebui să permită un tratament uniform al furnizorilor de servicii digitale la nivel naţional şi în întreaga Uniune, proporţional cu natura acestora şi cu gradul de risc cu care aceştia s-ar putea confrunta.

Autoritatea competentă ar trebui să acorde atenţia cuvenită menţinerii unor canale informale şi sigure pentru schimbul de informaţii. Anunţarea publică a incidentelor raportate autorităţii competente ar trebui să găsească echilibrul cuvenit între interesul publicului de a fi informat cu privire la ameninţări şi eventualele daune comerciale sau de reputaţie pe care le pot suferi operatorii de servicii esenţiale şi furnizorii de servicii digitale care raportează incidente.

Atunci când sunt puse în aplicare obligaţiile de notificare, autoritatea competentă şi CSIRT ar trebui să acorde o atenţie deosebită necesităţii de a păstra stricta confidenţialitate a informaţiilor despre vulnerabilităţile unui produs înainte de apariţia unor soluţii de securitate adecvate.

Furnizorii de servicii digitale ar trebui să facă obiectul unor activităţi de supraveghere ex post lejere şi bazate pe reacţie, justificate de natura serviciilor şi a operaţiunilor lor. Prin urmare, respectiva autoritate competentă ar trebui să acţioneze doar atunci când i se prezintă dovezi (de exemplu, chiar de către furnizorul de servicii digitale, de către o altă autoritate competentă, inclusiv o autoritate competentă a unui alt stat membru, sau de către un utilizator al serviciului) conform cărora furnizorul de servicii digitale nu se conformează cerinţelor prezentei directive, în special în urma unui incident care a avut loc. Prin urmare, autorităţii competente nu ar trebui să-i revină nicio obligaţie generală de a supraveghea furnizorii de servicii digitale.

Autoritatea competentă ar trebui să deţină mijloacele necesare pentru a-şi îndeplini atribuţiile, inclusiv competenţele de a obţine suficiente informaţii pentru a evalua nivelul securităţii reţelelor şi a sistemelor informatice.

Incidentele pot fi rezultatul activităţilor criminale, a căror prevenire, anchetare şi urmărire penală este sprijinită prin coordonarea şi cooperarea dintre operatorii de servicii esenţiale, furnizorii de servicii digitale, autorităţile competente şi autorităţile de aplicare a legii. În cazul în care un incident este suspectat că ar fi legat de activităţi criminale grave în temeiul dreptului Uniunii sau al dreptului intern, România ar trebui să încurajeze operatorii de servicii esenţiale şi furnizorii de servicii digitale să raporteze autorităţilor de aplicare a legii incidentele suspecte de a fi de natură penală gravă.

În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente.

În acest context, autoritățile competente și autoritățile de protecție a datelor ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante pentru abordarea oricăror cazuri de încălcare a securității datelor cu caracter personal în urma unor incidente.

Jurisdicția cu privire la furnizorii de servicii digitale ar trebui să fie atribuită statului membru în care furnizorul de servicii digitale își are sediul principal în Uniune, care, în principiu, corespunde locului în care furnizorul își are sediul social în Uniune. Stabilirea implică exercitarea efectivă și reală a activității în cadrul unor acorduri stabile. Forma juridică a acestor acorduri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință. Acest criteriu nu ar trebui să depindă de situarea fizică sau nu a rețelei și a sistemelor informatice în locul respectiv, prezența și utilizarea acestor sisteme neconstituind, prin ele însele, acest sediu principal și, prin urmare, nu este un criteriu de determinare a sediului principal.

În cazul în care un furnizor de servicii digitale care nu este stabilit în Uniune oferă servicii în cadrul Uniunii, acesta ar trebui să desemneze un reprezentant. Pentru a determina dacă un astfel de furnizor de servicii digitale oferă servicii în cadrul Uniunii, ar trebui să se confirme că furnizorul de servicii digitale intenționează să ofere servicii persoanelor din unul sau mai multe state membre. Simpla accesibilitate în Uniune a unui site internet al furnizorului de servicii digitale sau al unui intermediar sau disponibilitatea unei adrese de e-mail și a altor date de contact, sau utilizarea unei limbi folosite în general în țara terță în care furnizorul de servicii digitale își are sediul, sunt insuficiente pentru a se confirma o astfel de intenție. Cu toate acestea, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda servicii în respectiva limbă sau menționarea unor clienți sau utilizatori din Uniune pot conduce la concluzia că furnizorul de servicii digitale intenționează să ofere servicii în Uniune. Reprezentantul ar trebui să acționeze în numele furnizorului de servicii digitale, iar autoritățile competente sau CSIRT ar trebui să poată contacta reprezentantul. Reprezentantul ar trebui să fie desemnat explicit printr-un mandat scris al furnizorului de servicii digitale să acționeze în numele acestuia în privința obligațiilor care îi revin acestuia în temeiul prezentei directive, inclusiv raportarea incidentelor.

Standardizarea cerințelor de securitate este un proces impulsionat de piață. Pentru a asigura o aplicare convergentă a standardelor de securitate, România ar trebui să încurajeze respectarea standardelor indicate sau conformitatea cu acestea, în vederea garantării unui nivel ridicat de securitate al rețelelor și sistemelor informatice la nivelul Uniunii.

Entitățile care nu intră în domeniul de aplicare al prezentului proiect de act normativ pot suferi incidente care au un impact semnificativ asupra serviciilor pe care le furnizează. Atunci când consideră că este de interes public să notifice apariția acestor incidente, entitățile respective ar trebui să aibă posibilitatea să facă acest lucru voluntar. Aceste notificări ar trebui să fie tratate de autoritatea competentă sau CSIRT în cazul în care aceasta nu constituie o sarcină disproporționată sau neavenită.

Schimbul de informații cu privire la riscuri și incidente desfășurat în cadrul grupului de cooperare și al rețelei CSIRT, precum și îndeplinirea cerințelor de notificare a incidentelor către autoritățile naționale competente sau CSIRT ar putea necesita

prelucrarea datelor cu caracter personal. Prelucrarea acestora ar trebui să se conformeze legislației în vigoare. Prezentul proiect de act normativ respectă Constituția, drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezentul proiect de act normativ ar trebui să fie pus în aplicare în conformitate cu drepturile și principiile menționate.	
3. Alte informații	Nu au fost identificate. Proiectul necesită punct de vedere: ANSPDCP, ANCOM,ANRE, MP.
Secțiunea a 3-a ***Impactul socioeconomic al proiectului de act normativ***	
1. Impactul macroeconomic	Actul normativ propus are impact asupra sectoarelor vizate în anexa: energia, transporturile, sectorul bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructura digitală.
1[1]. Impactul asupra mediului concurențial și domeniului ajutoarelor de stat	Proiectul de act normativ nu se referă la acest subiect.
2. Impactul asupra mediului de afaceri	Directiva 1148/2016 și pe cale de consecință și proiectul impune cerințe de securitate operatorilor de servicii esențiale și furnizorilor de servicii digitale, cerințe care se reflectă în costuri de implementare.
2[1] Impactul asupra sarcinilor administrative	Proiectul de act normativ nu se referă la acest subiect.
2[2] Impactul asupra întreprinderilor mici și mijlocii	Proiectul de act normativ nu se referă la acest subiect.
3. Impactul social	Constituind cadrul legal care reglementează securitatea rețelelor și sistemelor informatice ce susțin servicii esențiale din domenii cheie la nivel social, este de așteptat o creștere a rezilienței acestor servicii și respectiv o reducere a riscurilor la nivel social asociate cu atacurile cibernetice. Indirect va duce pe termen lung la o creștere a încrederii în serviciile societății digitale și o dezvoltare a serviciilor de securitate informatică.
4. Impactul	Proiectul de act normativ nu se referă la acest subiect

asupra mediului	
5. Alte informaţii	Nu au fost identificate

Secţiunea a 4-a

Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani)

Având în vedere că proiectul de act normativ transpune prevederile Directivei UE 1148/2016 stabilind cadrul juridic general, desemnând autorităţile competente la nivel naţional, obligaţiile generale şi cadrul de reglementare subsecventă a obligaţiilor specifice, proiectul de act normativ nu are un impact asupra bugetului general consolidat.

- 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) contribuţii de asigurări						
2. Modificări ale cheltuielilor bugetare, minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri si						

servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri şi servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri si 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						

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.	In aplicarea proiectului, vor fi emise: **A. Hotărâri de Guvern** 1. Hotărârea Guvernului privind componenţa, atribuţiile şi modul de lucru ale Grupului de lucru interinstituţional pentru determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale 2. Hotărâre a Guvernului privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale. 3. Hotărârea Guvernului pentru modificarea şi completarea Hotărârii Guvernului nr. 494/2011. 4. Hotărârea Guvernului pentru aprobarea Strategiei naţionale privind securitatea reţelelor şi a sistemelor informatice. 5. Hotărârea Guvernului pentru aprobarea Listei serviciilor esenţiale. 6. Hotărârea Guvernului pentru aprobarea normelor de aplicare a legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice
1^1Compatibilitatea actului normativ cu legislaţia în domeniul achiziţiilor publice	Proiectul de act normativ nu se referă la acest subiect.
2. Conformitatea proiectului de act normativ cu legislaţia comunitară în cazul proiectelor ce transpun prevederi comunitare	Proiectul de act normativ transpune: - 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
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se referă la acest subiect
4. Hotărâri ale Curţii de Justiţie a Uniunii Europene	Proiectul de act normativ se conformează prevederilor cuprinse în legislaţia UE menţionată la punctul 2.
5. Alte acte normative şi/sau	Proiectul de act normativ nu se referă la acest subiect.

documente internaţionale din care decurg angajamente	
6. Alte informaţii	Nu au fost identificate.
Secţiunea a 6-a ***Consultările efectuate în vederea elaborării proiectului de act normativ***	
1. Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate	Proiectul de act normativ nu se referă la acest subiect.
2. Fundamentarea alegerii organizaţiilor cu care a avut loc consultarea, precum şi a modului în care activitatea acestor organizaţii este legată de obiectul proiectului de act normativ	Proiectul de act normativ nu se referă la acest subiect.
3. Consultările organizate cu autorităţile administraţiei publice locale, în situaţia în care proiectul de act normativ are ca obiect activităţi ale acestor autorităţi, în condiţiile Hotărârii Guvernului nr. 521/2005 privind	Proiectul de act normativ nu se referă la acest subiect

procedura de consultare a structurilor asociative ale autorităţilor administraţiei publice locale la elaborarea proiectelor de acte normative, cu modificările ulterioare	
4. Consultările desfăşurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr. 750/2005 privind constituirea consiliilor interministeriale permanente, cu modifiările şi completările ulterioare	Proiectul de act normativ nu se referă la acest subiect
5. Informaţii privind avizarea de către: a) Consiliul Legislativ b) Consiliul Suprem de Apărare a Ţării c) Consiliul Economic şi Social d) Consiliul Concurenţei e) Curtea de Conturi	Proiectul prezentului act normativ a fost avizat favorabil de Consiliul Legislativ prin avizul nr. 273/2018. Proiectul prezentului act normativ a fost avizat de către Consiliului Concurenței potrivit adresei 1775/23.02.2018
6. Alte informaţii	Nu au fost identificate

Secţiunea a 7-a *Activităţi de informare publică privind elaborarea si implementarea proiectului de act normativ*	
1. Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ	Proiectul a fost publicat pe site-ul MCSI şi a lansat în consultare publică în perioada 3 oct 2017 - 3 noiembrie 2017. În data de 9 noiembrie 2017 a avut loc o consultare publică la care au fost prezenţi reprezentanţi ai societăţii civile.
2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice	Proiectul de act normativ nu se referă la acest subiect
3. Alte informaţii	Nu au fost identificate
Secţiunea a 8-a *Măsuri de implementare*	
1. Măsurile de punere în aplicare a proiectului de act normativ de către autorităţile administraţiei publice centrale şi/sau locale - înfiinţarea unor noi organisme	a) instituţii ce urmează a fi înfiinţate, reorganizate sau desfiinţate – proiectul de act normativ nu se referă la acest subiect; b) rezultatul se poate obţine cu instituţiile existente; c) sursa de finanţare a instituţiilor ce urmează a fi înfiinţate - proiectul de act normativ nu se referă la acest subiect.

sau extinderea competentelor instituţiilor existente.	
2. **Alte informaţii**	Nu au fost identificate

Faţă de cele prezentate, a fost elaborat proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, pe care îl supunem Parlamentului, spre adoptare, cu procedura de urgenţă prevăzută de art.76 alin. (3) din Constituţia României, republicată.

PRIM – MINISTRU

VIORICA DĂNCILĂ