



PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

SENATUL

L E G E

privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

Parlamentul României adoptă prezenta lege.

CAPITOLUL I **Dispoziții generale**

SECȚIUNEA 1 ***Obiect și scop***

Art. 1. – Prezenta lege stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu.

Art. 2. – (1) Scopul prezentei legi îl constituie:

a) stabilirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice;

b) desemnarea autorității competente la nivel național și a 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 intervenție în caz de incidente de securitate informatică;

c) 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.

(2) Prezenta lege nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale, precum și Oficiului Registrului Național al Informațiilor Secrete de Stat.

SECȚIUNEA a 2-a *Definiții și principii*

Art. 3. – În sensul prezentei legi, termenii și expresiile de mai jos au următoarea semnificație:

a) *administrarea incidentului* – toate procedurile utilizate pentru detectarea, analiza și limitarea unui incident și răspunsul la acesta;

b) *domain name system*, denumit în continuare *DNS* – sistem de atribuire de nume distribuite ierarhic într-o rețea în care se efectuează căutări de nume de domenii;

c) *furnizor de servicii digitale* – orice persoană juridică care furnizează un serviciu digital;

d) *furnizor de servicii DNS* – entitate care furnizează servicii DNS pe internet;

e) *incident* – orice eveniment care are un impact real negativ asupra securității rețelelor și a sistemelor informatice;

f) *internet exchange point*, denumit în continuare *IXP* – facilitate a rețelei care permite interconectarea a mai mult de două sisteme autonome independente, în special în scopul facilitării schimbului de trafic de internet; *IXP* furnizează interconectare doar pentru sisteme autonome; *IXP* nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interferează într-un alt mod cu acest trafic;

g) *motor de căutare online* – un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogări privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informații-cheie și care revine cu linkuri în care se pot găsi informații legate de conținutul căutat;

h) *operator de servicii esențiale* – persoană fizică sau juridică de drept public sau privat de tipul celor prevăzute în anexa care face parte integrantă din prezenta lege, care furnizează un serviciu care îndeplinește condițiile prevăzute la art. 6 alin. (1);

i) *piață online* – serviciu digital care permite consumatorilor și/sau comercianților, astfel cum sunt definiți la art. 3 alin. (1) lit. a) și b) din

Ordonanța Guvernului nr. 38/2015 privind soluționarea alternativă a litigiilor dintre consumatori și comercianți, cu modificările ulterioare, să încheie cu comercianții vânzări online sau contracte de servicii, fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online;

j) *registru de nume de domenii Top-level* – entitate care administrează și operează înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific;

k) *reprezentant* – orice persoană fizică sau juridică stabilită în Uniunea Europeană desemnată explicit să acționeze în numele unui furnizor de servicii digitale nestabilit în Uniunea Europeană, căreia i se poate adresa autoritatea competentă la nivel național sau echipa de răspuns la incidente de securitate informatică, denumită în continuare *echipă CSIRT* sau *CSIRT*, în locul furnizorului de servicii digitale în ceea ce privește obligațiile furnizorului de servicii digitale în temeiul prezentei legi;

1) *rețea și sistem informatic*:

1. rețea de comunicații electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare;

2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic;

3. datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la pct. 1 și 2 în vederea funcționării, utilizării, protejării și întreținerii lor;

m) *risc* – orice circumstanță sau eveniment ce poate fi identificat în mod rezonabil, anterior producerii sale, care are un efect potențial negativ asupra securității rețelelor și a sistemelor informatice;

n) *securitatea rețelelor și a sistemelor informatice* – capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea, confidențialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

o) *serviciu digital* – serviciu, în sensul prevederilor art. 4 alin. (1) pct. 2 din Hotărârea Guvernului nr. 1016/2004 privind măsurile pentru organizarea și realizarea schimbului de informații în domeniul standardelor și reglementărilor tehnice, precum și al regulilor referitoare la serviciile societății informaționale între România și statele membre ale Uniunii Europene, precum și Comisia Europeană, cu modificările și completările ulterioare, și care se încadrează într-una din categoriile:

1. piață online;
2. motor de căutare online;
3. serviciu de cloud computing;

p) *specificație* – specificație tehnică, în sensul prevederilor art. 2 pct. 4 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr.1673/2006/CE a Parlamentului European și a Consiliului;

q) *standard* – standard, în sensul prevederilor art. 2 pct. 1 din Regulamentul (UE) nr. 1025/2012;

r) *strategie națională privind securitatea rețelelor și a sistemelor informatice* – cadru care furnizează obiective și priorități strategice privind securitatea rețelelor și a sistemelor informatice la nivel național;

s) *serviciu de cloud computing* – serviciu digital care permite accesul la un sistem configurabil de resurse sau servicii informatice care pot fi puse în comun;

ș) *valoare de prag* – valoare minimă/maximă, cuantificabilă a indicatorilor în baza cărora se determină gradul de îndeplinire a unui criteriu.

Art. 4. – Principiile care stau la baza prezentei legi:

a) *principiul responsabilității și conștientizării* – constă în efortul continuu derulat de entitățile de drept public și privat în conștientizarea rolului și responsabilității individuale pentru atingerea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;

b) *principiul proporționalității* – constă în asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și cerințele de securitate implementate;

c) *principiul cooperării și coordonării* – constă în realizarea în timp oportun a schimbului de informații referitoare la riscurile de securitate la adresa rețelelor și sistemelor informatice și asigurarea într-o manieră sincronizată a reacției la producerea incidentelor.

CAPITOLUL II Domeniul de aplicare

SECȚIUNEA 1 *Operatorii de servicii esențiale*

Art. 5. – În vederea asigurării unui nivel ridicat de securitate, operatorii de servicii esențiale se identifică și se înscriu în Registrul operatorilor de servicii esențiale.

Art. 6. – (1) Un serviciu este considerat esențial dacă furnizarea lui îndeplinește cumulativ următoarele condiții:

- a) serviciul este esențial în susținerea unor activități societale și/sau economice de cea mai mare importanță;
- b) furnizarea sa depinde de o rețea sau de un sistem informatic;
- c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.

(2) Evaluarea gradului de perturbare a furnizării serviciului esențial se realizează în funcție de următoarele criterii intersectoriale, fără a fi cumulative:

- a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;
- b) dependența altor sectoare prevăzute în anexa la prezenta lege de serviciul furnizat de entitatea în cauză;
- c) impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;
- d) cota de piață a entității în cauză;
- e) distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;
- f) importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

(3) Ministerul Comunicațiilor și Societății Informaționale denumit în continuare *MCSI*, la propunerea Centrului Național de Răspuns la Incidente de Securitate Cibernetică denumit în continuare *CERT-RO*, supune aprobării prin hotărâre a Guvernului în termen de 5 luni de la data intrării în vigoare a prezentei legi:

- a) valorile de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale;

b) valorile de prag corespunzătoare criteriilor intersectoriale stabilite potrivit dispozițiilor alin. (2);

c) criteriile sectoriale specifice și valorile de prag corespunzătoare fiecărui sector și subsector de activitate prevăzut în anexă;

d) normele tehnice de stabilire a impactului incidentelor.

(4) La nivelul MCSI, se înființează și funcționează Grupul de lucru interinstituțional pentru determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale, prevăzute la alin. (3).

(5) MCSI, la propunerea CERT-RO, în termen de 3 luni de la data intrării în vigoare a prezentei legi, supune aprobării prin hotărâre a Guvernului componența, atribuțiile și modul de organizare a Grupului de lucru interinstituțional prevăzute la alin. (4).

(6) Determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul operatorilor de servicii esențiale care furnizează servicii din sectorul prevăzut la pct. 7 din anexă, se realizează cu consultarea Autorității Naționale pentru Administrare și Reglementare în Comunicații.

Art. 7. – (1) Registrul prevăzut la art. 5 se alcătuiește pentru sectoarele și subsectoarele prevăzute în anexă și raportat la criteriile prevăzute la art.6 și valorile de prag prevăzute la art. 6 alin. (3).

(2) Registrul prevăzut la alin. (1) se înființează, se întreține și se actualizează periodic, cel puțin o dată la doi ani de la data intrării în vigoare a prezentei legi de către CERT-RO în calitate de autoritate competentă la nivel național.

(3) Registrul prevăzut la alin. (1) face parte din categoria documentelor clasificate.

(4) Normele metodologice de organizare și funcționare a registrului prevăzut la art. 5 se aprobă, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicațiilor și societății informaționale, care se publică în Monitorul Oficial al României, Partea I.

Art. 8. – (1) Entitățile care îndeplinesc condițiile și criteriile prevăzute la art. 6 și activează într-unul sau mai multe dintre sectoarele sau subsectoarele de activitate prevăzute în anexă, au obligația să notifice CERT-RO în vederea înscrierii în Registrul operatorilor de servicii esențiale.

(2) Prin excepție de la alin. (1) identificarea în vederea înscrierii în Registrul operatorilor de servicii esențiale se poate face și de către CERT-RO din oficiu în vederea îndeplinirii obligațiilor legale ce îi revin sau în urma unei sesizări privind sustragerea de la obligația de notificare și înscriere în Registrul operatorilor de servicii esențiale făcută de către orice persoană

interesată, aducând la cunoștința entității vizate declanșarea procedurii de identificare și comunicând la final operatorului rezultatul acesteia.

(3) Operatorii de servicii esențiale pot solicita asistența CERT-RO în procesul de identificare.

(4) Înscrierea operatorilor de servicii esențiale în Registrul operatorilor de servicii esențiale se realizează prin decizia directorului general al CERT-RO care se comunică operatorului de servicii esențiale în urma depunerii unui raport de audit care atestă îndeplinirea cerințelor minime de securitate și notificare, întocmit de un auditor atestat în conformitate cu prevederile art. 32 și a evaluării informațiilor și documentațiilor furnizate de operator în cadrul procesului de identificare.

(5) Atunci când o entitate furnizează un serviciu dintre cele reglementate la art. 6 alin. (1) lit. a) și în cadrul altor state membre ale Uniunii Europene, CERT-RO se consultă cu autoritățile omologe din statele respective în procesul de identificare înainte de adoptarea unei decizii privind identificarea operatorului.

(6) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data îndeplinirii condițiilor prevăzute la art. 6 alin. (1) prin raportare la criteriile intersectoriale de stabilire a impactului unui incident prevăzute la art. 6 alin. (2), respectiv la criteriile sectoriale, precum și la valorile de prag prevăzute la art. 6 alin. (3) prin depunerea unei declarații pe propria răspundere.

(7) Operatorii economici și celelalte entități care operează ori furnizează servicii în cadrul sectoarelor și subsectoarelor definite în anexă au obligația de a pune la dispoziția CERT-RO, la cererea acesteia în calitate de autoritate competentă la nivel național, în termen de 60 de zile de la data primirii solicitării, documentațiile necesare, inclusiv rapoarte de audit, pentru:

a) stabilirea calității de operator de servicii esențiale în conformitate cu prevederile art. 6 și 7;

b) stabilirea măsurilor necesare pentru conformarea cu cerințele prezentei legi;

c) stabilirea interdependenței și interconectării rețelelor și sistemelor informatice cu cele ale altor operatori de servicii esențiale ori furnizori de servicii digitale, inclusiv a celor pe care se bazează furnizarea serviciilor entității în cauză;

d) stabilirea listei de autorități ale statului pentru care furnizează serviciile definite la art. 6 alin. (1).

(8) Prin excepție de la termenul general de furnizare a documentațiilor stabilit la alin. (7), termenul de realizare a auditurilor și de depunere a rapoartelor de audit prevăzute la alin. (4) și (7), precum și tematica și obiectivele acestora se stabilesc de către CERT-RO în urma

evaluării celorlalte informații furnizate în conformitate cu prevederile alin. (7) și curge de la data primirii comunicării termenului de către entitatea vizată.

(9) Documentația prevăzută la alin. (7) și (8) va fi stabilită prin normele metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale, aprobate la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicațiilor și societății informaționale, care se publică în Monitorul Oficial al României, Partea I.

Art. 9. – (1) Entitățile care nu mai îndeplinesc condițiile și criteriile prevăzute la art. 6 notifică CERT-RO în vederea radierii din Registrul operatorilor de servicii esențiale și furnizează documentațiile relevante în conformitate cu art. 8 alin. (7) lit. a).

(2) CERT-RO dispune prin decizia directorului general radierea din Registrul operatorilor de servicii esențiale la cerere sau din oficiu, în urma evaluării documentațiilor prevăzute la alin. (1) și comunică operatorului decizia.

(3) Operatorii de servicii esențiale pot solicita asistența CERT-RO cu privire la documentațiile prevăzute la alin. (1) necesare în procesul de radiere.

(4) Atunci când o entitate furnizează un serviciu esențial și în cadrul altor state membre ale Uniunii Europene, CERT-RO se consultă cu autoritățile omologe din statele respective înainte de adoptarea unei decizii privind radierea.

(5) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data la care entitatea nu mai îndeplinește condițiile prevăzute la art. 6.

Art. 10. – (1) În scopul asigurării securității rețelelor și sistemelor informatice, operatorii de servicii esențiale au următoarele obligații:

a) implementează măsurile tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate stabilite în temeiul prevederilor art. 25 alin. (3);

b) implementează măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea acestor servicii esențiale, cu scopul de a asigura continuitatea serviciilor respective, stabilite în temeiul prevederilor art. 25 alin. (3);

c) notifică de îndată CERT-RO în calitate de CSIRT național incidentele care au un impact semnificativ asupra continuității serviciilor esențiale furnizând cel puțin informațiile prevăzute la art. 26 alin. (3);

d) pun la dispoziția CERT-RO informații care să permită stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) se supun controlului desfășurat de către CERT-RO în vederea stabilirii gradului de respectare a obligațiilor ce le revin în temeiul prezentei legi;

f) stabilesc mijloacele permanente de contact, desemnează responsabilii cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea mijloacelor de contact și comunică CERT-RO în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esențiale lista acestora, precum și orice modificări ulterioare de îndată ce au survenit;

g) comunică în termen de maximum 30 de zile către CERT-RO, în calitate de autoritate competentă la nivel național, orice schimbare survenită în datele furnizate în cadrul procesului de identificare ca operator de servicii esențiale;

h) se interconectează în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esențiale la serviciul de alertare și cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact și ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul rețelelor și sistemelor informatice proprii;

i) asigură de îndată răspunsul la incidentele survenite, restabilesc în cel mai scurt timp funcționarea serviciului la parametrii dinaintea incidentului și realizează auditul de securitate, conform prezentei legi.

(2) Operatorii de servicii esențiale pun la dispoziția CERT-RO în calitate de autoritate competentă la nivel național, la solicitarea acesteia făcută cu menționarea scopului și precizând informațiile necesare și termenul de furnizare a acestora:

a) informațiile necesare pentru evaluarea securității rețelelor și a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat la solicitarea CERT-RO, inclusiv informațiile și documentațiile pe care se bazează acesta, precum și alte elemente care atestă punerea efectivă în aplicare a cerințelor minime de securitate.

(3) Notificarea de îndată a afectării serviciilor esențiale prevăzută la alin. (1) lit. c) se face și în situația în care afectarea se datorează unor incidente care afectează un furnizor de servicii digitale de care depinde furnizarea serviciilor esențiale.

(4) Termenul de conformare pentru îndeplinirea obligațiilor prevăzute la alin. (1) lit. a) și b) este de 6 luni de la data intrării în vigoare a normelor tehnice privind cerințele de securitate și notificare ori, după caz, de la data înscrierii în Registrul operatorilor de servicii esențiale.

Art. 11. – Operatorii de servicii esențiale au obligația să implementeze în termenul de conformare stabilit în conformitate cu dispozițiile art.37, măsurile dispuse de CERT-RO pentru îndeplinirea cerințelor minime de securitate, în vederea remedierii deficiențelor constatate cu ocazia controlului exercitat în temeiul art. 35.

SECȚIUNEA a 2-a
Furnizorii de servicii digitale

Art. 12. – (1) Furnizorii de servicii digitale au următoarele obligații:

a) implementează măsurile tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate a rețelelor și sistemelor informatice stabilite în temeiul prevederilor prezentei legi cu privire la serviciile prevăzute la art. 3 lit. o) pe care le oferă pe teritoriul Uniunii Europene ținând cont de normele tehnice prevăzute la art.25 alin. (1), în termen de 6 luni de la data intrării în vigoare a acestora;

b) implementează, în termen de 6 luni de la data intrării în vigoare a normelor tehnice prevăzute la art. 25 alin. (1) măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea serviciilor prevăzute la lit.a), asigură răspunsul la incidente și continuitatea serviciilor acestora;

c) notifică de îndată CERT-RO în calitate de CSIRT național incidentele care au un impact semnificativ asupra furnizării serviciilor prevăzute la art. 3 lit. o) furnizând cel puțin informațiile prevăzute la art. 26 alin. (3);

d) pun la dispoziția CERT-RO informații care să permită stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) stabilesc mijloace permanente de contact, desemnează responsabilii cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea canalelor de contact și comunică CERT-RO în termen de 60 de zile de la data intrării în vigoare a prezentei legi, lista acestora precum și orice modificări ulterioare de îndată ce au survenit;

f) se interconectează în termen de 60 de zile de la data intrării în vigoare a prezentei legi la serviciul de alertare și cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact și ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul rețelelor și sistemelor informatice proprii.

(2) Furnizorii de servicii digitale pun la dispoziția CERT-RO în calitate de autoritate competentă la nivel național, la solicitarea acesteia făcută cu menționarea scopului și precizând informațiile necesare și termenul de furnizare a acestora:

a) informațiile necesare pentru evaluarea securității rețelelor și a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat, inclusiv informațiile și documentațiile pe care se bazează acesta, precum și alte elemente care atestă punerea efectivă în aplicare a cerințelor minime de securitate.

(3) Obligația de notificare prevăzută la alin. (1) lit. c) se aplică doar în cazul în care furnizorul de servicii digitale are acces la informațiile necesare pentru evaluarea impactului incidentului prevăzute la art. 26 și care să permită evaluarea prevăzută la art. 28.

(4) Prevederile prezentei legi se aplică furnizorilor de servicii digitale care au stabilit sediul social pe teritoriul României, precum și celor din afara Uniunii Europene care stabilesc sediul reprezentanței din Uniune pe teritoriul României.

(5) Prevederile alin. (1) – (4), art. 25 alin. (4), art. 26 alin. (2) din prezenta lege nu se aplică furnizorilor de servicii digitale care se încadrează în categoria întreprinderilor mici și mijlocii, așa cum sunt definite în Legea nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare.

(6) Operatorii economici, precum și celelalte entități care furnizează servicii digitale, au obligația de a furniza către CERT-RO, în termen de 60 de zile de la data primirii solicitării făcută cu menționarea scopului și precizând informațiile necesare următoarele categorii de documente:

a) documentațiile necesare stabilirii calității de furnizor de servicii digitale în sensul prezentei legi;

b) documentațiile necesare stabilirii interdependenței și interconectării rețelelor și sistemelor informatice cu cele ale altor operatori de servicii esențiale ori furnizori de servicii digitale;

c) stabilirea listei de autorități ale statului pentru care furnizează serviciile definite la art. 3 lit. o).

(7) Documentația prevăzută la alin. (6) va fi stabilită prin normele metodologice prevăzute la art. 8 alin. (9).

CAPITOLUL III

Roluri și responsabilități

SECȚIUNEA 1

Coordonarea strategică la nivel național

Art. 13. – Coordonarea strategică, la nivel național a activităților de asigurare a unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice se realizează de către Guvern prin Ministerul Comunicațiilor și

Societății Informaționale sub aspectul politicilor publice și al inițiativei legislative în domeniu.

Art. 14. – Strategia națională privind securitatea rețelelor și a sistemelor informatice se aprobă prin hotărâre a Guvernului, la propunerea MCSI în termen de 6 luni de la data intrării în vigoare a prezentei legi.

SECȚIUNEA a 2-a

Autorități competente și responsabilități

Art. 15. – (1) CERT-RO este autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale identificate în temeiul prezentei legi.

(2) Pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice, CERT-RO se consultă și cooperează cu:

a) Serviciul Român de Informații, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale a căror afectare aduce atingere securității naționale;

b) Ministerul Apărării Naționale, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea națională;

c) Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate și responsabilitate.

Art. 16. – CERT-RO se consultă și cooperează, după caz, cu:

a) organele de urmărire penală;

b) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, atunci când incidentele au ca rezultat afectarea securității ori funcționării rețelelor publice de comunicații electronice, ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate și responsabilitate a acesteia;

c) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii.

*SECȚIUNEA a 3-a****Echipele de intervenție în caz de incidente de securitate informatică***

Art. 17. – (1) Echipa *CSIRT* definită la art. 19 lit. b) respectă cerințele de la art. 24 și acoperă sectoarele din anexa și serviciile prevăzute la art. 3 lit. o).

(2) Persoanele juridice care activează în cadrul aceluiași sector sau subsector de activitate din anexa la prezenta lege pot constitui echipe *CSIRT* proprii sau sectoriale ori pot achiziționa servicii de specialitate de tip *CSIRT*.

(3) Entitățile prevăzute la art. 15 alin. (2) și art. 16 lit. b) pot constitui echipe *CSIRT* pentru asigurarea securității rețelelor și sistemelor informatice conform domeniului de activitate și responsabilitate.

(4) Echipele *CSIRT* sectoriale se autorizează și se desemnează de către CERT-RO în urma evaluării îndeplinirii condițiilor specifice de autorizare a acestui tip de echipe elaborate în conformitate cu prevederile art. 20 lit e).

Art. 18. – (1) Echipele *CSIRT* proprii, sectoriale sau serviciile de specialitate prevăzute la art.17 alin. (2) care deserveșc operatori de servicii esențiale și furnizori de servicii digitale au următoarele obligații:

a) să fie autorizate de către CERT-RO în temeiul prezentei legi;

b) să asigure compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate cu cele ale echipei *CSIRT* naționale din cadrul CERT-RO;

c) să furnizeze cel puțin setul minim de servicii de tip *CSIRT* necesar asigurării la nivel național a unei protecții unitare a operatorilor și furnizorilor ce fac obiectul prezentei legi;

d) să utilizeze în cadrul echipelor un număr corespunzător de persoane calificate în conformitate cu prezenta lege;

e) să se interconecteze la serviciul de alertă, monitorizare și cooperare al CERT-RO și să asigure un răspuns prompt la alertele și solicitările transmise de echipa *CSIRT* națională.

(2) Normele tehnice privind compatibilitatea și interoperabilitatea prevăzute la alin.(1) lit.b), setul minim de servicii menționat la alin. (1) lit. c) și criteriile de stabilire a numărului de persoane calificate prevăzute la alin. (1) lit. d) se aprobă, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicațiilor și societății informaționale, care se publică în Monitorul Oficial al României, Partea I.

SECȚIUNEA a 4-a
Autoritatea competentă la nivel național – CERT-RO

Art. 19. – În cadrul CERT-RO se organizează și funcționează și:

- a) Punctul unic de contact la nivel național;
- b) Echipa de răspuns la incidente de securitate informatică la nivel național, denumită în continuare *echipa CSIRT națională* sau *CSIRT național*.

Art. 20. – CERT-RO în calitate de autoritate competentă la nivel național are următoarele atribuții generale:

- a) identifică, cu consultarea autorităților și entităților de reglementare și administrare a sectoarelor și subsectoarelor prevăzute în anexă, operatorii de servicii esențiale care au sediul social, filială, sucursală sau punct de lucru pe teritoriul României;
- b) elaborează și actualizează normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice;
- c) elaborează și actualizează normele tehnice privind îndeplinirea obligațiilor de notificare a incidentelor de securitate de către operatorii și furnizorii prevăzuți de prezenta lege;
- d) coordonează activitatea Grupului de lucru interinstituțional menționat la art. 6 alin. (4);
- e) elaborează și actualizează, după consultarea celorlalte instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, precum și a altor instituții și autorități, după caz, normele metodologice, tehnice, precum și regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și a serviciilor digitale, precum și normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare pentru activitățile prevăzute la literele o) și p);
- f) elaborează și promovează practici comune pentru administrarea incidentelor și a riscurilor și pentru sistemele de clasificare a incidentelor, riscurilor și informațiilor;
- g) participă, prin reprezentanți, la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și compus din reprezentanți ai statelor membre, ai Comisiei Europene și ai Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor – ENISA, în vederea adoptării

soluțiilor optime pentru atingerea obiectivului de securitate și a schimbului de informații între statele membre respectiv:

i. după caz, participă la schimbul de experiență privind aspecte legate de securitatea rețelelor și a sistemelor informatice cu instituții, organe, oficii și agenții relevante ale Uniunii Europene;

ii. participă la dezbateri privind standardele și specificațiile prevăzute la art.25 alin.(6) cu reprezentanți ai organizațiilor de standardizare europene relevante;

iii. colectează exemple de bune practici privind riscurile și incidentele;

h) permite echipelor CSIRT, acces la datele privind incidentele notificate de operatorii de servicii esențiale sau de furnizorii de servicii digitale, în măsura necesară pentru a-și îndeplini atribuțiile, cu respectarea legii;

i) verifică în condițiile art. 35 – 42 respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor ce le revin conform prezentei legi;

j) emite în temeiul art. 37 dispoziții cu caracter obligatoriu pentru operatorii de servicii esențiale în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze;

k) instituie măsuri de supraveghere ex post pentru furnizorii de servicii digitale cu privire la neîndeplinirea obligațiilor ce le revin conform prevederilor prezentei legi;

l) primește sesizări cu privire la neîndeplinirea obligațiilor operatorilor și furnizorilor prevăzuți de prezenta lege;

m) cooperează cu autoritățile competente din celelalte state și oferă asistență acestora, prin schimbul de informații, transmiterea de solicitări și sesizări, efectuarea controlului ori luarea de măsuri de supraveghere și remediere a deficiențelor constatate, în cazul operatorilor și furnizorilor prevăzuți de prezenta lege care își au sediul principal în România ori care, deși au sediul principal stabilit în alt stat membru, rețelele sau sistemele informatice acestora sunt situate și pe teritoriul României;

n) monitorizează aplicarea prevederilor prezentei legi;

o) autorizează, revocă sau reînnoiește autorizarea echipelor CSIRT ce deservește operatori de servicii esențiale ori furnizori de servicii digitale;

p) eliberează, revocă sau reînnoiește atestatele auditorilor de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale în condițiile prezentei legi;

q) autorizează, revocă sau reînnoiește autorizarea formatorilor și furnizorilor de servicii de formare pentru activitățile prevăzute la lit.o) și p);

r) alcătuiește și actualizează periodic, cel puțin o dată la doi ani, începând cu data intrării în vigoare a prezentei legi, lista serviciilor esențiale care îndeplinesc condițiile de la art. 6 alin. (1) cu consultarea autorităților și entităților prevăzute la lit. a), precum și a celor prevăzute la art. 15 alin. (2) și o înaintează MCSI spre a fi supusă aprobării, prin hotărâre a Guvernului. Prima listă se supune aprobării Guvernului în termen de 6 luni de la data intrării în vigoare a prezentei legi;

s) propune spre aprobare MCSI normele tehnice, metodologice și regulamentele prevăzute de prezenta lege, în termen de 6 luni de la data intrării în vigoare a acesteia.

Art. 21. – În calitate de Punct național unic de contact, CERT-RO are următoarele atribuții:

a) exercită o funcție de legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică, denumită în continuare *rețeaua CSIRT*;

b) elaborează și transmite Grupului de cooperare rapoarte de sinteză privind notificările primite și acțiunile întreprinse;

c) transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, notificările și solicitările privind incidentele ce afectează funcționarea serviciilor esențiale și a celor digitale de pe teritoriul respectivelor state;

d) transmite autorităților prevăzute la art. 15 alin. (2) și art. 16 notificările și cererile primite din alte state membre, potrivit ariei de responsabilitate.

Art. 22. – (1) În calitate de CSIRT național, CERT-RO are următoarele atribuții:

a) monitorizează incidentele de securitate a rețelelor și sistemelor informatice la nivel național;

b) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către autoritățile prevăzute la art. 15 alin. (2), precum și orice entitate de drept public sau privat căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice;

c) primește notificări privind incidentele care afectează rețelele și sistemele operatorilor de servicii esențiale ori ale furnizorilor de servicii digitale;

d) furnizează operatorului de servicii esențiale care a făcut notificarea, în măsura posibilităților, informații relevante în ceea ce privește acțiunile ulterioare notificării;

e) stabilește, în baza notificărilor primite, impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național precum și autoritățile similare din alte state potențial afectate;

f) aduce la cunoștința publicului periodic și ori de câte ori este necesar avertizări, alerte și informări privind riscuri și amenințări, posibile măsuri de prevenire și contracarare în scopul cunoașterii de către public a acestora și al luării măsurilor adecvate și publică statistici privitoare la incidentele identificate la nivel național, cu respectarea condițiilor prezentei legi;

g) asigură răspunsul la incidente în limitele prezentei legi;

h) elaborează analize dinamice de risc și de incident;

i) cooperează, la nivel național, cu echipele CSIRT în cadrul unei platforme de management al incidentelor și pentru schimbul de informații;

j) participă la acțiunile comune în cadrul rețelei CSIRT la nivel european, precum și, după necesități, la acțiunile solicitate în cadrul rețelelor internaționale de cooperare;

k) poate solicita asistența ENISA pentru aducerea la îndeplinire a atribuțiilor sale;

l) înființează, întreține și operează serviciul de alertare și cooperare cu operatorii de servicii esențiale și furnizorii de servicii digitale menționat la art. 10 alin. (1) lit. h) și art. 12 alin. (1) lit. f).

(2) Echipele CSIRT se conectează și realizează schimbul de informații cu echipa CSIRT națională aflată în cadrul CERT-RO prin intermediul platformei de management al incidentelor, menționată la alin. (1) lit. i).

(3) În vederea administrării adecvate a incidentelor majore la nivel național ori pentru administrarea unor incidente care necesită înaltă specializare și pregătire tehnică de specialitate, CERT-RO poate dezvolta parteneriate și alcătui echipe mixte compuse din specialiștii proprii și specialiști proveniți de la alte instituții ori entități din mediul privat, cu respectarea legii și asigurarea condițiilor privind confidențialitatea și accesul la informații în limitele legii și cu acordul părților implicate în incident.

Art. 23. – (1) În scopul cooperării operaționale, Echipa CSIRT națională care funcționează în cadrul CERT-RO participă la Rețeaua CSIRT compusă din reprezentanți ai echipelor CSIRT naționale ale statelor membre din Uniunea Europeană și cea a CERT-UE.

(2) Cooperarea prevăzută la alin. (1) se realizează prin:

a) schimbul de informații privind serviciile, operațiunile și posibilitățile de cooperare;

b) schimbul și analiza informațiilor fără caracter comercial referitoare la incidentele ce afectează un stat membru;

c) schimbul de informații fără caracter confidențial privind incidente individuale;

d) participarea la elaborarea unui răspuns coordonat al Rețelei CSIRT, pentru managementul unui incident identificat pe teritoriul unui alt stat membru;

e) acordarea de sprijin voluntar în abordarea incidentelor transfrontaliere;

f) analiza și identificarea de noi forme de cooperare operațională în cadrul Rețelei CSIRT;

g) participarea la elaborarea de orientări și practici unitare în domeniul cooperării operaționale;

h) solicitarea Rețelei CSIRT de a asigura un răspuns coordonat la un incident identificat la nivel național.

(3) Fac excepție de la schimbul de informații prevăzut la alin. (2) lit. c) situațiile în care schimbul ar periclita investigarea incidentului.

(4) Echipa CSIRT participă și la alte rețele internaționale de cooperare, după necesități.

Art. 24. – (1) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de autoritate competentă la nivel național în temeiul art. 20, din bugetul CERT-RO se asigură resursele materiale, financiare și umane suficiente pentru:

a) desfășurarea activităților de normare prevăzute la art. 20 lit. a) – f) și r);

b) primirea sesizărilor, efectuarea controlului, verificărilor și supravegheților prevăzute la art. 20 lit. i) – l), precum și pentru asigurarea punerii în aplicare a deciziilor și sancțiunilor, rezolvării contestațiilor și reprezentarea în contencios administrativ;

c) desfășurarea activităților de cooperare prevăzute la art. 20 lit. g), h) și m), înființarea, administrarea și funcționarea registrelor și evidențelor prevăzute de art. 20 lit. o) – r), precum și a registrului operatorilor de servicii esențiale prevăzut la art. 5;

d) desfășurarea activităților de autorizare și acreditare prevăzute la art. 20 lit. o) – q);

e) luarea măsurilor cu caracter excepțional prevăzute la art. 41.

(2) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de Punct unic de contact la nivel național, din bugetul CERT-RO se asigură resursele materiale, financiare și umane suficiente pentru asigurarea în regim permanent a funcției de legătură, primire și retransmitere a cererilor și solicitărilor prevăzute la art. 21 lit. a), c) și d).

(3) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de echipă CSIRT națională conform prevederilor art. 22 și 23, din bugetul CERT-RO se asigură resursele materiale, financiare și umane suficiente pentru:

a) alertele prevăzute la art. 22 alin. (1) lit. a) și c);

b) emiterea avertizărilor, contactarea și alertarea altor entități și diseminarea de informații relevante în temeiul art. 22 alin. (1) lit. b), d) – f) și l);

c) asigurarea răspunsului, intervenției și cooperării în temeiul art. 22 alin. (1) lit. g), i) – l);

d) stabilirea impactului incidentelor și analiza acestora în temeiul art. 22 alin. (1) lit. e) și h).

(4) Resursele financiare, materiale și umane alocate CERT-RO vor asigura:

a) continuitatea activităților și disponibilitatea permanentă a serviciilor;

b) participarea la Grupul de cooperare prevăzut de art. 20 lit. g);

c) un sistem adecvat de gestionare și transmitere a cererilor;

d) o infrastructură adecvată prevăzută cu sisteme redundante;

e) spațiu de lucru de rezervă în amplasamente securizate;

f) disponibilitatea ridicată a serviciilor de comunicații prin mijloace multiple de contact, capacitatea de a contacta alte entități în orice moment și evitarea punctelor unice de defecțiune;

g) amplasamente securizate a sediilor echipei CSIRT naționale din cadrul CERT-RO și a sistemelor informatice de suport;

h) mijloacele necesare asigurării controlului punerii în aplicare a dispozițiilor prezentei legi și aplicării de sancțiuni, precum și pentru îndeplinirea celorlalte obligații ce îi revin conform legii;

i) personalul adecvat, inclusiv din punct de vedere al competențelor.

(5) Începând cu 1 ianuarie 2019 resursele financiare necesare pentru funcționarea CERT-RO se asigură din venituri proprii prevăzute la alin.(6) și în completare din subvenții de la bugetul de stat prin bugetul MCSI.

(6) Începând cu 1 ianuarie 2019 CERT-RO poate reține și utiliza următoarele categorii de venituri proprii:

a) sumele provenite din activitățile prevăzute la art. 32 alin. (2) lit. c) și e), respectiv activitățile prevăzute la art. 33 alin. (2) lit. c) și e);

b) sumele provenite din furnizarea serviciului prevăzut la art. 22 alin. (1) lit. l).

(7) Cuantumul tarifului pentru serviciile prevăzute la alin. (6) se stabilește prin ordin al ministrului comunicațiilor și societății informaționale, la propunerea directorului general al CERT-RO și se publică în Monitorul Oficial al României, Partea I.

(8) Din bugetul CERT-RO se asigură cu respectarea prevederilor legale în vigoare și următoarele categorii de cheltuieli:

a) achiziționarea de servicii de specialitate;

b) închirierea, achiziționarea sau construcția de imobile în vederea desfășurării activității;

c) achiziția de echipamente și software, inclusiv software dezvoltat la comandă;

d) afilierea la rețele și organizații internaționale de profil și participarea prin reprezentanți la lucrările acestora, precum și la alte evenimente de profil;

e) cursuri de formare și perfecționare, precum și certificări ale personalului propriu;

f) editarea de publicații, ghiduri de specialitate, clipuri video de conștientizare;

g) organizarea de conferințe, seminarii și alte evenimente de profil;

h) efectuarea de studii statistice și activități de cercetare;

i) renovări și îmbunătățiri ale sediilor și locațiilor de desfășurare a activității.

(9) CERT-RO poate folosi pentru desfășurarea activității bunuri materiale și fonduri bănești primite de la persoanele juridice și fizice, sub formă de donații și sponsorizări, cu respectarea dispozițiilor legale și asigurarea transparenței privind donațiile, sponsorizările și sursa acestora.

(10) CERT-RO poate înființa birouri și sedii la nivel local în vederea asigurării activităților și reprezentării adecvate pentru îndeplinirea obligațiilor ce îi revin în temeiul prezentei legi.

CAPITOLUL IV

Asigurarea securității rețelelor și sistemelor informatice

SECȚIUNEA 1

Cerințele minime de securitate

Art. 25. – (1) În vederea asigurării unui nivel comun de securitate a rețelelor și sistemelor informatice, operatorii de servicii esențiale și furnizorii de servicii digitale au obligația de a respecta normele tehnice elaborate de CERT-RO în temeiul prevederilor art. 20 lit. b).

(2) CERT-RO elaborează cu consultarea autorităților care reglementează sectoarele și subsectoarele prevăzute în anexă ghiduri în sprijinul implementării măsurilor minime de securitate pentru operatorii și furnizorii prevăzuți în prezenta lege.

(3) Normele tehnice prevăzute la alin. (1) aplicabile operatorilor de servicii esențiale se stabilesc în baza cel puțin a următoarelor categorii de activități de asigurare a securității rețelelor și sistemelor informatice:

a) managementul drepturilor de acces;

b) conștientizarea și instruirea utilizatorilor;

c) jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice;

- d) testarea și evaluarea securității rețelelor și sistemelor informatice;
- e) managementul configurațiilor rețelelor și sistemelor informatice;
- f) asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice;
- g) managementul continuității funcționării serviciului esențial;
- h) managementul identificării și autentificării utilizatorilor;
- i) răspunsul la incidente;
- j) mentenanța rețelelor și sistemelor informatice;
- k) managementul suporturilor de memorie externă;
- l) asigurarea protecției fizice a rețelelor și sistemelor informatice;
- m) realizarea planurilor de securitate;
- n) asigurarea securității personalului;
- o) analiza și evaluarea riscurilor;
- p) asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice;

q) managementul vulnerabilităților și alertelor de securitate.

(4) Normele tehnice prevăzute la alin. (1) aplicabile furnizorilor de servicii digitale se stabilesc în baza următoarelor categorii de activități de asigurare a securității rețelelor și sistemelor informatice:

- a) securitatea sistemelor și a instalațiilor;
- b) gestionarea incidentelor;
- c) gestionarea continuității activității;
- d) monitorizarea, auditarea și testarea;
- e) conformitatea cu standardele europene și internaționale.

(5) În implementarea măsurilor de la alin. (1) operatorii de servicii esențiale:

a) identifică rețelele și sistemele informatice care susțin furnizarea de servicii esențiale;

b) elaborează și implementează politici și planuri proprii de securitate a rețelelor și sistemelor informatice;

c) asigură managementul incidentelor care afectează securitatea rețelelor și sistemelor informatice;

d) previn accesul neautorizat la rețelele și sistemele informatice;

e) previn diseminarea datelor deținute la nivelul rețelelor și sistemelor informatice către alte persoane decât cele autorizate să cunoască conținutul acestora;

f) implementează un sistem de management al riscului;

g) implementează planuri de acțiune pe niveluri de alertă de securitate a rețelelor și sistemelor informatice;

h) asigură continuitatea serviciilor.

(6) Normele tehnice prevăzute la alin. (1) se emit cu luarea în considerare a cerințelor și standardelor europene și internaționale fără a impune sau a discrimina în favoarea utilizării unui anumit tip de tehnologie.

SECȚIUNEA a 2-a *Notificarea incidentelor de securitate*

Art. 26. – (1) Notificările efectuate de operatorii de servicii esențiale în temeiul art. 10 alin. (1) lit. c) trebuie să îndeplinească condițiile și să conțină informațiile prevăzute în normele tehnice prevăzute la art. 20 lit. c).

(2) Notificările efectuate de furnizorii de servicii digitale în temeiul prevederilor art. 12 alin. (1) lit. c) trebuie să îndeplinească condițiile și să conțină informațiile prevăzute în normele tehnice prevăzute la art. 20 lit. c).

(3) Notificarea incidentelor conține, în mod obligatoriu, următoarele informații:

a) elementele de identificare ale infrastructurii și operatorului sau furnizorului în cauză;

b) descrierea incidentului;

c) perioada de desfășurare a incidentului;

d) impactul estimat al incidentului;

e) măsuri preliminare adoptate;

f) lista de autorități ale statului afectate de incident;

g) întinderea geografică potențială a incidentului;

h) date despre efecte potențial transfrontaliere ale incidentului.

(4) Notificarea prevăzută la alin. (1) și (2) nu va conține:

a) informații clasificate;

b) date care pot aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități implicate în incident, în condițiile legii.

(5) CERT-RO în calitate de autoritate competentă la nivel național elaborează și actualizează prin decizia directorului general publicată în Monitorul Oficial al României, Partea I, formularele necesare notificărilor de incident efectuate în temeiul prezentului articol, detaliind informațiile și documentațiile necesare a fi furnizate.

(6) CERT-RO în calitate de CSIRT național va stabili și va aduce la cunoștința publicului, precum și operatorilor și furnizorilor menționați în prezenta lege, mijloacele de comunicare pentru efectuarea notificărilor cerute prin prezenta lege.

(7) Notificările privind incidentele ce fac obiectul prezentei legi pot fi făcute și de către echipele CSIRT ale entităților de drept public sau privat ori care deservește un anumit sector de activitate, ori de către furnizorii de servicii

de securitate aflați în relație contractuală, conform atribuțiilor ce le revin în baza actului de înființare ori a contractului de prestări servicii, după caz.

(8) Notificarea făcută de o echipă CSIRT în temeiul alin. (7) echivalează cu notificarea făcută de operatorul sau furnizorul afectat, acesta purtând întreaga răspundere pentru conținutul notificării și îndeplinirea celorlalte obligații ce îi revin conform prezentei legi.

(9) Obligația de a notifica un incident de către furnizorii de servicii digitale se aplică doar în cazul în care aceștia au acces la informațiile necesare pentru a evalua impactul unui incident asupra parametrilor menționați la art. 28 alin. (2).

(10) Entitățile care nu au fost identificate drept operatori de servicii esențiale și nu sunt furnizori de servicii digitale pot notifica voluntar CERT-RO în calitate de CSIRT național furnizând cel puțin informațiile prevăzute la alin. (3), incidentele care au un impact semnificativ asupra continuității serviciilor pe care le furnizează.

(11) CERT-RO tratează notificările obligatorii cu prioritate față de notificările voluntare.

(12) Notificările voluntare se tratează doar atunci când această prelucrare nu împiedică îndeplinirea celorlalte obligații ce îi revin autorității competente la nivel național și în limita resurselor existente.

(13) Notificarea voluntară nu impune entității notificatoare nicio obligație care nu i-ar fi revenit dacă nu ar fi făcut notificarea.

(14) Notificările prevăzute la alin. (1) și (2) nu atrag răspunderea pentru entitățile care notifică, în condițiile respectării obligațiilor prevăzute de prezenta lege.

SECȚIUNEA a 3-a *Managementul incidentelor*

Art. 27. – După primirea notificării, CERT-RO în calitate de CSIRT național:

a) evaluează preliminar impactul incidentului la nivel național și alertează, sesizează ori notifică, sau după caz, poate solicita operatorului sau furnizorului să alerteze alte entități afectate, precum și autoritățile cu responsabilități în prevenirea, limitarea și combaterea efectelor incidentului, precum și autoritățile prevăzute la art. 16, potrivit legii;

b) poate solicita informații suplimentare operatorului sau furnizorului care a făcut notificarea în vederea îndeplinirii obligațiilor ce îi revin menționând termenul de furnizare a acestora;

c) oferă operatorului sau furnizorului care a făcut notificarea, atunci când circumstanțele o permit, informații care ar putea sprijini administrarea incidentului;

d) în calitate de Punct unic de contact informează celelalte state membre sau parteneri afectați dacă incidentul are un impact semnificativ asupra continuității serviciilor esențiale ori a serviciilor digitale în statele respective;

e) în urma analizei incidentelor, poate, după caz, declanșa acțiune de control pentru verificarea respectării cerințelor prezentei legi;

f) poate lua măsurile prevăzute la art. 41;

g) coordonează la nivel național răspunsul la incident în colaborare cu celelalte autorități și entități publice sau private, conform domeniului de activitate și responsabilitate.

Art. 28. – (1) Impactul unui incident se determină ținând cont cel puțin de următorii parametri:

i. în cazul operatorilor de servicii esențiale:

a) numărul de utilizatori afectați de perturbarea serviciului esențial;

b) durata incidentului;

c) distribuția geografică în ceea ce privește zona afectată de incident.

ii. în cazul furnizorilor de servicii digitale:

a) numărul de utilizatori afectați de incident, în special utilizatori care se bazează pe serviciul pentru furnizarea propriilor servicii;

b) durata incidentului;

c) distribuția geografică în ceea ce privește zona afectată de incident;

d) amploarea perturbării funcționării serviciului;

e) amploarea impactului asupra activităților economice și societale.

(2) Grupul de lucru interinstituțional prevăzut la art. 6 alin. (4) elaborează și actualizează normele tehnice de stabilire a impactului pentru categoriile de operatori și furnizori prevăzuți de prezenta lege.

(3) Criteriile prevăzute la pct. 2 se aplică și notificărilor voluntare efectuate în temeiul prevederilor art. 26 alin. (10).

Art. 29. – (1) CERT-RO poate înștiința publicul, atunci când informarea este necesară pentru a preveni un incident sau pentru a se administra un incident în curs.

(2) Pentru incidentele care afectează un operator de servicii esențiale sau un furnizor de servicii digitale informarea menționată la alin. (1) se realizează după consultarea prealabilă a acestuia asupra conținutului înștiințării.

(3) În cazul furnizorilor de servicii digitale, informarea publicului specificată la alin. (1) poate fi făcută și direct de către aceștia la solicitarea CERT-RO ori a autorităților sau echipelor CSIRT ale altor state membre afectate.

Art. 30. – (1) În activitățile de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale, de control, de primire a notificărilor privitoare la incidente și de management al acestora desfășurate în baza prezentei legi, precum și în procesele interne, CERT-RO protejează interesele de securitate și comerciale ale operatorului de servicii esențiale și ale furnizorului de servicii digitale, precum și confidențialitatea informațiilor furnizate.

(2) Cu excepția informațiilor necesare înștiințării de la art. 29 alin. (1), informațiile prelucrate în sensul îndeplinirii obligațiilor de la alin. (1) nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

(3) Informațiile confidențiale conform legislației naționale și normelor Uniunii Europene, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia Europeană și cu alte autorități numai dacă acest lucru este necesar pentru aplicarea prezentei legi.

(4) Informațiile care fac obiectul schimbului menționat la alin. (3) se limitează la informații relevante și proporționale cu scopul urmărit.

(5) Schimbul de informații menționat la alin. (3) se va face cu garantarea păstrării confidențialității informațiilor și protejarea securității și intereselor comerciale ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale.

(6) Prelucrările de date cu caracter personal ce intră sub incidența prezentei legi se efectuează cu respectarea reglementărilor legale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

(7) Notificările realizate în temeiul prezentei legi nu afectează obligațiile operatorilor de date cu caracter personal stabilite potrivit art. 33 și 34 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.

(8) În scopul îndeplinirii atribuțiilor ori furnizării serviciilor prevăzute de prezenta lege, precum și în scopul prevenirii și răspunsului la incidentele de securitate informatică, ori al cooperării la nivel național, comunitar și internațional în prevenirea și răspunsul la incidentele de securitate informatică, CERT-RO colectează, primește, prelucrează și

transmite date și informații ce pot constitui sau pot conține date cu caracter personal, în limitele legislației aplicabile, cu asigurarea respectării prevederilor alin. (6).

CAPITOLUL V Audit și autorizare

SECȚIUNEA 1

Auditul de securitate a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale

Art. 31. – Poate fi auditor de securitate a rețelelor și sistemelor informatice – persoana fizică sau persoana juridică ce realizează, audit de securitate a rețelelor și sistemelor informatice, adică desfășoară acea activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora.

Art. 32. – (1) Auditul de securitate specificat la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) și art. 12 alin. (2) lit. b) se realizează de către auditorii de securitate informatică ce dețin atestat valabil eliberat de către CERT-RO pentru a audita rețele și sisteme informatice ce deservește servicii esențiale sau servicii digitale în sensul prezentei legi.

(2) În acest sens CERT-RO:

- a) întreține și actualizează Registrul auditorilor menționați la alin. (1);
- b) elaborează și transmite spre aprobare MCSI în conformitate cu prevederile art. 20 lit. e) și s), regulamentul pentru atestarea și verificarea auditorilor de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale și stabilește condițiile de valabilitate pentru atestatele acordate;
- c) acordă, prelungește, suspendă sau retrage atestarea pentru auditorii de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale, în conformitate cu prevederile regulamentulului prevăzut la lit. b);
- d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35 – 42 îndeplinirea de către auditorii atestați în temeiul prezentei legi a obligațiilor legale ce le revin;
- e) elaborează și aprobă prin decizia directorului general publicată în Monitorul Oficial al României, Partea I, tematicile pentru specializarea auditorilor în vederea atestării prevăzute la lit. c) și autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul auditului de

securitate informatică pentru rețelele și sistemele informatice ale operatorilor de servicii esențiale și furnizorilor de servicii digitale.

(3) Nu pot realiza auditul solicitat la art. 10 alin. (2) lit. b), respectiv art. 12 alin. (2) lit. b):

a) auditorii atestați care asigură în mod curent servicii de securitate informatică ori servicii de tip CSRIT operatorului de servicii esențiale sau furnizorul de servicii digitale, ori sunt angajați ai acestora;

b) auditorul care are un contract de prestări servicii pentru rețeaua și sistemul supus auditului aflat în desfășurare la momentul la care se efectuează auditul sau într-un termen mai mic de un an;

c) auditorul care a mai efectuat 3 audituri consecutive la același operator de servicii esențiale sau furnizor de servicii digitale.

(4) Activitatea de audit se efectuează potrivit standardelor și specificațiilor europene și internaționale aplicabile în domeniu.

(5) Tematicile de audit vor ține seama de normele tehnice în vigoare privind securitatea rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și a furnizorilor de servicii digitale elaborate în temeiul prezentei legi.

(6) Atestatele au o valabilitate de 3 ani.

(7) Constituie excepție de la prevederile alin. (1) auditul de securitate realizat la nivelul instituțiilor cu responsabilități în domeniul apărării, ordinii publice și securității naționale cât și pentru serviciile puse la dispoziție de către aceștia.

(8) Lista standardelor și specificațiilor europene și internaționale prevăzute la alin. (4) se elaborează și se aprobă prin decizia directorului general al CERT-RO, se actualizează periodic și se publică în Monitorul Oficial al României, Partea I.

SECȚIUNEA a 2-a

Autorizarea echipelor CSIRT ce deservește rețele și sisteme informatice din categoria serviciilor esențiale și serviciilor digitale

Art. 33. – (1) Echipete CSIRT care deservește operatori de servicii esențiale ori furnizori de servicii digitale se autorizează de către CERT-RO în calitate de autoritate competentă la nivel național.

(2) În acest sens CERT-RO:

a) întreține și actualizează Registrul echipelor CSIRT prevăzute la alin. (1);

b) elaborează și transmite spre aprobare MCSI în conformitate cu prevederile art. 20 lit. e) și s), regulamentul pentru autorizarea și verificarea echipelor CSIRT care deservește operatorii de servicii esențiale sau furnizorii

de servicii digitale și stabilește condițiile de valabilitate pentru autorizațiile acordate;

c) acordă, prelungește, suspendă sau retrage autorizarea pentru echipele CSIRT, în conformitate cu prevederile regulamentului prevăzut la lit. b);

d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35 – 42 îndeplinirea de către echipele CSIRT autorizate în temeiul prezentei legi a obligațiilor legale ce le revin;

e) elaborează tematicile pentru formarea membrilor echipelor CSIRT în vederea autorizării prevăzute la lit. c) și autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul asigurării de servicii de tip CSIRT pentru rețelele și sistemele informatice ale operatorilor de servicii esențiale și furnizorilor de servicii digitale.

(3) În vederea autorizării, echipa CSIRT trebuie să îndeplinească condițiile prevăzute în normele tehnice elaborate în temeiul prevederilor art. 20 lit. e).

(4) Autorizațiile au o valabilitate de 3 ani.

CAPITOLUL VI

Cooperare

Art. 34. – (1) Autoritățile și entitățile care reglementează sectoarele și subsectoarele de activitate prevăzute în anexă au obligația de a coopera și sprijini CERT-RO în calitate de autoritate competentă la nivel național și de a răspunde solicitărilor acesteia, potrivit domeniilor de activitate și responsabilitate pentru:

a) identificarea serviciilor esențiale din sectoarele de activitate reglementate de acestea;

b) identificarea operatorilor de servicii esențiale în sensul prezentei legi și actualizarea listei acestora;

c) identificarea cerințelor de securitate și notificare existente în cadrul sectorului sau subsectorului respectiv, în vederea determinării nivelului de securitate asigurat de acestea;

d) stabilirea cerințelor specifice de asigurare a securității rețelelor și sistemelor informatice și de notificare a incidentelor survenite pentru sectoarele și subsectoarele prevăzute în anexă;

e) armonizarea cerințelor specifice prevăzute la punctele anterioare cu cerințele de securitate și notificare prevăzute de prezenta lege;

f) luarea măsurilor cu caracter excepțional prevăzute la art. 41;

g) stabilirea criteriilor și valorilor de prag specifice, necesare pentru determinarea impactului unui incident la nivelul sectorului sau subsectorului respectiv;

h) armonizarea reglementărilor emise de acestea la nivel de sector cu cerințele prezentei legi.

(2) Cerințele specifice de securitate impuse operatorilor de servicii esențiale sau furnizorilor de servicii digitale prin acte juridice ale Uniunii Europene de directă aplicare sau prin acte juridice ale Uniunii Europene transpuse la nivel național care reglementează respectivul sector de activitate se aplică doar în măsura în care nivelul de securitate asigurat este cel puțin echivalent cu obligațiile prevăzute în prezenta lege.

(3) Aplicarea actelor juridice ale Uniunii Europene prevăzute la alin. (2) nu derogă de la celelalte obligații care revin operatorilor de servicii esențiale și furnizorilor de servicii digitale conform prezentei legi.

CAPITOLUL VII Supraveghere, control, sancționare

SECȚIUNEA 1 Activitatea de control

Art. 35. – (1) CERT-RO exercită controlul respectării prevederilor prezentei legi, a obligațiilor impuse prin actele emise de CERT-RO în aplicarea prezentei legi, în limitele competențelor legale de monitorizare sau de verificare.

(2) În vederea efectuării controlului prevăzut la alin.(1), directorul general al CERT-RO, prin decizie, desemnează personalul de specialitate împuternicit să efectueze controlul și stabilește atribuțiile acestuia.

(3) Normelor de aplicare a dispozițiilor privind controlul îndeplinirii obligațiilor de securitate și notificare de către operatorii de servicii esențiale și furnizorii de servicii digitale și controlul îndeplinirii obligațiilor de către auditorii de securitate informatică atestați ori de către echipele CSIRT autorizate să deservească operatori de servicii esențiale și furnizori de servicii digitale se aprobă, la propunerea CERT-RO, prin ordin al ministrului comunicațiilor și societății informaționale care se publică în Monitorul Oficial al României, Partea I.

Art. 36. – (1) În urma sesizărilor primite, din oficiu, sau în urma autosesizării în temeiul art. 27 lit. e), precum și în situația existenței unor indicii temeinice privind sustragerea unui operator sau furnizor de la obligațiile ce îi revin în temeiul prezentei legi, ori încălcarea de către un auditor, echipă CSIRT sau furnizor de formare autorizat, a obligațiilor ce le revin în temeiul prezentei legi, personalul de control poate să efectueze acțiuni de control, în cadrul cărora poate să solicite, menționând temeiul legal și scopul solicitării, documentele necesare pentru efectuarea controlului, să

ridice copii de pe registre ori alte acte sau documente, în condițiile legii, inclusiv a prevederilor referitoare la păstrarea confidențialității tuturor documentelor și informațiilor primite.

(2) În cadrul acțiunilor de control, personalul de control poate să solicite și să primească, la fața locului sau la termenul solicitat, informațiile necesare pentru efectuarea controlului și poate stabili termene până la care aceste informații să îi fie furnizate, în condițiile legii, inclusiv a prevederilor referitoare la păstrarea confidențialității tuturor documentelor și informațiilor primite.

(3) Rezultatul acțiunilor de control va fi consemnat într-o notă de control.

Art. 37. – (1) Înainte de aplicarea unei sancțiuni, în cazul descoperirii nerespectării de către un furnizor de servicii digitale sau operator de servicii esențiale a unei obligații prevăzută de prezenta lege sau de un act emis de CERT-RO în baza prezentei legi, CERT-RO va transmite entității în cauză o notificare prin care îi va aduce la cunoștință încălcarea constatată, măsurile cu caracter obligatoriu ce trebuie luate în vederea remedierii deficiențelor constatate și stabilește termenul de conformare, precum și sancțiunea aplicabilă.

(2) Termenul de conformare se calculează începând cu data comunicării notificării prevăzute la alin. (1).

Art. 38. – Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate potrivit legii infracțiuni:

1. neîndeplinirea obligației de notificare în vederea înscrierii în registrul operatorilor de servicii esențiale, prevăzută la art. 8 alin. (1) în termenul prevăzut la art. 8 alin. (6);

2. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. a);

3. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. b);

4. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. c);

5. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. d);

6. nedepunerea raportului de audit specificat la art. 8 alin. (4) și (7) în termenul comunicat de către CERT-RO persoanei juridice în temeiul art. 8 alin. (8);

7. neîndeplinirea obligației prevăzută la art. 9 alin. (1) în termenul prevăzut la art. 9 alin. (5);

8. neducerea la îndeplinire a măsurilor dispuse de CERT-RO prin notificarea transmisă în urma controlului, pentru remedierea deficiențelor constatate, în termenul de conformare stabilit în conformitate cu prevederile art.37;

9. neîndeplinirea de către operatorii de servicii esențiale a obligației de implementare a măsurilor pentru îndeplinirea cerințelor minime de securitate în conformitate cu art. 10 alin. (1) lit. a) în termenul stabilit la art. 10 alin. (4);

10. neîndeplinirea de către operatorii de servicii esențiale a obligației de implementare a măsurilor adecvate pentru a preveni și minimiza impactul incidentelor în conformitate cu art. 10 alin. (1) lit. b) în termenul stabilit la art. 10 alin. (4);

11. încălcarea de către operatorii de servicii esențiale a obligației stabilită la art. 10 alin. (1) lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatării acestuia;

12. încălcarea obligației stabilită la art. 10 alin. (1) lit. d) prin nefurnizarea în cadrul notificării privitoare la incidentul de securitate a informațiilor care să permită stabilirea impactului transfrontalier a acestuia;

13. nerespectarea prevederilor art. 10 alin. (1) lit. e) în termen de 48 de ore de la data comunicării de către CERT-RO a ordinului de începere a controlului;

14. necomunicarea către CERT-RO a informațiilor și mijloacelor permanente de contact ori a actualizărilor acestora în termenele stabilite la art. 10 alin. (1) lit. f);

15. neîndeplinirea obligației de comunicare prevăzută la art. 10 alin. (1) lit. g) în termen de 30 de zile;

16. neîndeplinirea obligației de interconectare prevăzută la art. 10 alin. (1) lit. h) în termen de 60 de zile;

17. neluarea de către operatorul de servicii esențiale a măsurilor adecvate de răspuns în termen de 12 ore de la primirea prin serviciul de alertare și cooperare al CERT-RO menționat la art. 10 alin. (1) lit. h) ori prin celelalte mijloace de contact a alertelor și solicitărilor privitoare la incidente;

18. neîndeplinirea de îndată a obligației de a asigura răspunsul la incidentele survenite stabilită la art. 10 alin. (1) lit. i) ori îndeplinirea acesteia cu o întârziere mai mare de 12 ore de la data constatării incidentului;

19. neîndeplinirea obligației stabilită la art. 10 alin. (1) lit. i) de a restabili funcționarea serviciului esențial afectat de incident la parametrii dinaintea incidentului ori întârzierea nejustificată a restabilirii funcționării acestuia;

20. neîndeplinirea în urma răspunsului la incident a obligației stabilită la art. 10 alin. (1) lit. i) de a efectua auditul de securitate a rețelelor și sistemelor informatice afectate;

21. nefurnizarea în termenul stabilit de CERT-RO a informațiilor și documentațiilor solicitate în temeiul art. 10 alin. (2) lit. a);

22. neefectuarea auditului de securitate și netransmiterea rezultatelor acestuia și a datelor necesare în termenul stabilit de CERT-RO în urma solicitării făcute în temeiul prevederilor art. 10 alin. (2) lit. b);

23. încălcarea cumulativă a obligațiilor prevăzute la art. 10 alin. (3) și art. 26 alin. (1) – (3) într-un termen de 12 ore de la data constatării incidentului de către operatorul de servicii esențiale;

24. neîndeplinirea de către operatorii de servicii esențiale a obligației prevăzute la art. 11 în termenele stabilite de CERT-RO prin actul de control comunicat operatorului de servicii esențiale;

25. neducerea la îndeplinire de către furnizorul de servicii digitale a măsurilor dispuse de CERT-RO prin notificarea transmisă în urma controlului, pentru remedierea deficiențelor constatate în aplicarea prevederilor art. 12 alin. (1) lit. a) și b) în termenul de conformare stabilit în conformitate cu prevederile art. 37;

26. neîndeplinirea de către furnizorii de servicii digitale, în termenul stabilit, a obligației de implementare a măsurilor pentru respectarea cerințelor minime de securitate în conformitate cu prevederile art. 12 alin. (1) lit. a);

27. neîndeplinirea de către furnizorii de servicii digitale a obligației de implementare, în termenul stabilit, a măsurilor adecvate pentru a preveni și minimiza impactul incidentelor în conformitate cu prevederile art. 12 alin. (1) lit. b);

28. încălcarea de către furnizorii de servicii digitale a obligației stabilită la art. 12 alin. (1) lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatării acestuia;

29. încălcarea obligației stabilită la art. 12 alin. (1) lit. d) prin nefurnizarea în cadrul notificării privitoare la incidentul de securitate a informațiilor care să permită stabilirea impactului transfrontalier a acestuia;

30. necomunicarea către CERT-RO a informațiilor și mijloacelor permanente de contact în termenul stabilit la art. 12 alin. (1) lit. e);

31. neîndeplinirea obligației de comunicare a modificărilor survenite în datele de contact prevăzută la art. 12 alin. (1) lit. e) în termen de 30 de zile;

32. neîndeplinirea obligației de interconectare prevăzută la art. 12 alin. (1) lit. f) în termen de 60 de zile;

33. neluarea de către furnizorul de servicii digitale a măsurilor adecvate de răspuns în termen de 12 ore de la primirea prin serviciul de

alertare și cooperare al CERT-RO menționat la art. 12 alin. (1) lit. f) ori prin celelalte mijloace de contact a alertelor și solicitărilor privitoare la incidente;

34. neîndeplinirea obligației de a asigura răspunsul la incidentele de securitate și de a asigura continuitatea serviciilor stabilite la art. 12 alin. (1) lit. b) ori îndeplinirea acestora cu o întârziere mai mare de 12 ore de la data constatării incidentului;

35. nefurnizarea în termenul stabilit de CERT-RO a informațiilor și documentațiilor solicitate în temeiul art. 12 alin. (2) lit. a);

36. neefectuarea auditului de securitate și netransmiterea rezultatelor acestuia și a datelor necesare în termenul stabilit de CERT-RO în urma solicitării făcute în temeiul art. 12 alin. (2) lit. b);

37. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. a);

38. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. b);

39. neîndeplinirea în termenul prevăzut a obligației de furnizare a informațiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. c);

40. neducerea la îndeplinire a măsurilor instituite de CERT-RO în temeiul art.20 lit.k), în termen de 60 de zile de la data comunicării;

41. neconformarea cu normele tehnice prevăzute la art. 25 alin. (1);

42. neconformarea operatorilor de servicii esențiale cu normele tehnice privitoare la notificarea incidentelor de securitate prevăzute la art. 26 alin. (1);

43. neconformarea furnizorilor de servicii digitale cu normele tehnice privitoare la notificarea incidentelor de securitate prevăzute la art. 26 alin. (2);

44. nefurnizarea de către operatorul de servicii esențiale ori furnizorul de servicii digitale în termenul stabilit de CERT-RO a informațiilor suplimentare solicitate de CERT-RO în temeiul art. 27 lit. b);

45. încălcarea de către auditorii specificați la art. 32 alin. (1) a normelor privind incompatibilitatea, prevăzute la art. 32 alin. (3);

46. furnizarea de rapoarte de audit de securitate dintre cele prevăzute la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) și art. 12 alin. (2) lit. b) realizate de către auditori fără atestat valabil eliberat de CERT-RO în temeiul art. 32 alin. (1) și (2) lit. c) ori aflați într-una din stările de incompatibilitate prevăzute la art. 32 alin. (3);

47. asigurarea de servicii de tip echipă CSIRT către operatorii de servicii esențiale ori furnizorii de servicii digitale de către entități care nu dețin autorizație valabil, eliberată în temeiul art. 33 alin. (1) de către CERT-RO în calitate de autoritate competentă la nivel național;

48. neîndeplinirea de către autoritățile și entitățile de reglementare pentru sectoarele și subsectoarele de activitate prevăzute în anexă a

obligațiilor prevăzute la art. 34 alin. (1), precum și neparticiparea în procesul de stabilire a nivelului de securitate menționat la art. 34 alin.(2);

49. refuzul de a se supune controlului declanșat de CERT-RO în temeiul prevederilor art. 36 ori întârzierea în furnizarea informațiilor și documentelor solicitate în cadrul activităților de control în temeiul prevederilor art. 37.

Art. 39. – (1) Contravențiile prevăzute la art. 38 se sancționează astfel:

a) cu amendă de la 3.000 lei la 50.000 lei, iar în cazul constatării unor încălcări repetate limita maximă a amenzii este de 100.000 lei;

b) prin derogare de la dispozițiile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, pentru persoanele cu o cifră de afaceri de peste 2.000.000 lei, cu amendă în cuantum de la 0,5% la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, limita maximă a amenzii este de 5% din cifra de afaceri.

(2) În vederea individualizării sancțiunii, CERT-RO va lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligația legală a fost încălcată, precum și, dacă este cazul, consecințele încălcării.

(3) Cifra de afaceri este cea prevăzută în ultima situație financiară anuală raportată de operatorul economic.

(4) Pentru persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cifrei de afaceri prevăzute la alin. (1) lit. b) îi corespunde totalitatea veniturilor brute, astfel cum sunt definite de Legea nr. 227/2015 privind Codul fiscal, cu modificările și completările ulterioare, realizate de respectivele entități.

(5) Prin excepție de la prevederile alin. (3) și (4), în cazul în care, în anul financiar anterior sancționării, întreprinderea nu a înregistrat cifra de afaceri sau cifra de afaceri nu poate fi determinată, va fi luată în considerare cea aferentă anului financiar în care entitatea a înregistrat cifra de afaceri, an imediat anterior anului de referință pentru calcularea cifrei de afaceri în vederea aplicării sancțiunii. În ipoteza în care nici în anul anterior anului de referință pentru calcularea cifrei de afaceri în vederea aplicării sancțiunii entitatea nu a realizat cifra de afaceri, va fi luată în calcul ultima cifră de afaceri înregistrată de entitate.

(6) Pentru entitățile nou înființate și care nu au înregistrat cifra de afaceri în anul anterior sancționării, amenda prevăzută la alin. (1) se stabilește în cuantum de minimum unu și maximum 25 de salarii minime brute pe economie.

(7) În măsura în care prezenta lege nu prevede altfel, contravențiilor prevăzute la art. 38 li se aplică dispozițiile Ordonanței Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

Art. 40. – (1) Contravențiile prevăzute la art. 38 se constată de către personalul de control din cadrul CERT-RO prin procesul-verbal de constatare a contravenției și de aplicare a sancțiunii semnat de către personalul care efectuează controlul și de către reprezentantul operatorului sau furnizorului prezent la momentul încheierii procesului-verbal căruia i se va înmâna o copie a procesului-verbal.

(2) Sancțiunea pentru contravențiile prevăzute la alin. (1) se aplică de către personalul de control care a făcut constatarea.

Art. 41. – (1) În cazul constatării unei contravenții în conformitate cu prevederile art. 38, CERT-RO dispune încetarea încălcării dispozițiilor respective fie imediat, fie într-un termen rezonabil, precum și orice măsuri necesare pentru a asigura încetarea încălcării și remedierea situației produse. Măsurile vor fi adecvate și proporționale cu încălcarea săvârșită și vor prevedea un termen în care operatorul de servicii esențiale ori furnizorul de servicii digitale trebuie să se conformeze acestora.

(2) În cazul în care nerespectarea de către operatori sau furnizori a obligațiilor din prezenta lege poate crea probleme grave de natură economică sau operațională altor operatori sau furnizori, CERT-RO poate lua măsuri urgente cu caracter provizoriu pentru remedierea situației.

(3) În cazul în care nerespectarea de către operatori sau furnizori a obligațiilor prevăzute de prezenta lege prezintă un pericol grav și iminent la adresa apărării naționale, ordinii publice, securității naționale sau sănătății publice, CERT-RO va informa organele judiciare și va notifica instituțiile competente din domeniul apărării și securității naționale, ordinii publice sau sănătății publice.

(4) Atunci când apreciază că este necesar, CERT-RO poate menține măsurile dispuse conform prevederilor alin. (2) pentru o perioadă de cel mult 90 de zile. În cazul în care punerea în executare a acestora necesită o durată mai mare de timp, CERT-RO poate dispune prelungirea aplicabilității pentru o perioadă suplimentară de cel mult 90 de zile. Operatorului sau furnizorului în cauză i se va acorda posibilitatea de a-și prezenta punctul de vedere și de a propune soluții pentru remedierea definitivă a situației create.

(5) Măsurile prevăzute la alin. (2) se dispun prin decizie a directorului general al CERT-RO ce poate fi atacată cu plângere în termen de 30 zile de la comunicare.

(6) Măsurile prevăzute la alin. (2) se pot dispune de către CERT-RO cu titlu excepțional și în situația administrării unor incidente de natură să prezinte pericolele ori să aibă urmările prevăzute la alin. (3) cu consultarea, precum și la solicitarea motivată a instituțiilor prevăzute la alineatul respectiv.

Art. 42. – (1) În exercitarea atribuțiilor ce îi revin potrivit actelor normative în vigoare, CERT-RO va fi sprijinită operativ, la cerere, de către autoritățile publice, precum și de către organele de poliție în cazuri temeinic justificate, în vederea identificării și localizării persoanelor fizice sau juridice care săvârșesc fapte de natură contravențională.

(2) Orice decizie a CERT-RO prin care se vatărnă drepturile unei persoane fizice sau juridice, ori refuzul nejustificat al CERT-RO de a-i procesa cererea referitoare la un drept recunoscut de prezenta lege pot fi atacate în contencios administrativ.

CAPITOLUL VIII

Dispoziții tranzitorii

Art. 43. – Înscrierea în Registrul prevăzut la art. 8, în primii 2 ani de la data intrării în vigoare a prezentei legi, se face prin depunerea unei declarații pe propria răspundere însoțită de o documentație de autoevaluare a îndeplinirii cerințelor minime de securitate și notificare.

CAPITOLUL IX

Dispoziții finale

Art. 44. – Până la 9 august 2018 și, ulterior, în fiecare an, CERT-RO în calitate de Punct unic de contact transmite grupului de cooperare un raport de sinteză privind notificările primite, care include numărul de notificări și natura incidentelor notificate, precum și acțiunile întreprinse în conformitate cu prevederile art. 10 alin. (1) lit. c), art. 12 alin. (1) lit. c) coroborate cu art. 27 lit. d).

Art. 45. – (1) Strategia națională prevăzută la art. 14 va acoperi cel puțin următoarele elemente:

a) obiectivele și prioritățile strategiei naționale privind securitatea rețelelor și a sistemelor informatice;

b) un cadru de guvernanză pentru realizarea obiectivelor și a priorităților strategiei naționale privind securitatea rețelelor și a sistemelor informatice, care să includă rolurile și responsabilitățile organismelor guvernamentale și ale altor actori relevanți;

c) identificarea măsurilor referitoare la gradul de pregătire, răspuns și redresare, inclusiv cooperarea dintre sectorul public și cel privat;

d) indicarea programelor de instruire, sensibilizare și formare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

e) indicarea planurilor de cercetare și dezvoltare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

f) un plan de evaluare a riscurilor pentru identificarea riscurilor;

g) o listă a diferiților actori implicați în punerea în aplicare a strategiei naționale privind securitatea rețelelor și a sistemelor informatice.

(2) În elaborarea strategiei, MCSI poate solicita asistența ENISA.

(3) În termen de 3 luni de la data intrării în vigoare a prezentei legi, MCSI transmite Comisiei Europene strategia adoptată în temeiul art. 14.

(4) Comunicarea de la alin. (3) nu va conține elementele care au legătură cu securitatea națională.

Art. 46. – CERT-RO identifică și stabilește documentele și detaliile tehnice necesare pentru evaluarea inițială a securității entităților care urmează să se declare operator de servicii esențiale.

Art. 47. – Cerințele de securitate și notificare prevăzute la cap. IV nu se aplică:

a) furnizorilor de rețele publice de comunicații electronice și furnizorilor de servicii de comunicații electronice destinate publicului;

b) prestatorilor de servicii de încredere calificați și necalificați care fac obiectul art. 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Art. 48. – (1) Până la 9 noiembrie 2018, pentru fiecare sector și subsector menționat în anexă, pe lângă primirea de notificări în vederea înscrierii în Registrul operatorilor de servicii esențiale conform art. 8 alin. (1), CERT-RO identifică operatorii de servicii esențiale care au sediul social, filială, sucursală, punct de lucru sau altă formă de reprezentare legal stabilită pe teritoriul României.

(2) În termen de 30 zile de la data intrării în vigoare a prezentei legi, MCSI notifică Comisiei Europene regimul sancționator aplicabil în temeiul prezentei legi, precum și orice modificare ulterioară a acestuia.

(3) În termenul prevăzut la alin. (1) și ulterior la fiecare doi ani, CERT-RO transmite Comisiei Europene următoarele informații în vederea evaluării aplicării prezentei legi:

- a) lista măsurilor care permit identificarea operatorilor de servicii esențiale;
- b) lista serviciilor prevăzute la art. 6 alin. (1) lit. a);
- c) numărul operatorilor de servicii esențiale identificați pentru fiecare sector menționat în anexă și o indicație a importanței lor în legătură cu sectorul respectiv;
- d) limite, atunci când acestea există, pentru determinarea nivelului relevant de furnizare, în raport cu numărul de utilizatori care se bazează pe serviciul respectiv sau cu importanța operatorului de servicii esențiale.

Art. 49. – (1) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la desemnarea autorității competente, a Punctului unic de contact și atribuțiilor acestora.

(2) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, orice modificare a actelor normative în baza cărora a fost făcută desemnarea de la alin. (1).

(3) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la misiunea, precum și la principalele elemente ale procedurilor de administrare a incidentelor folosite de echipa CSIRT națională.

Art. 50. – CERT-RO își desfășoară activitatea în baza prevederilor prezentei legi și a Hotărârii Guvernului nr. 494 din 11 mai 2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, care va fi modificată și completată corespunzător prevederilor prezentei legi.

* *
*

Prezenta lege transpune în totalitate Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene seria L nr. 194 din 19 iulie 2016.

Această lege a fost adoptată de Parlamentul României, în condițiile art. 147 alin. (2), cu respectarea prevederilor art. 75 și ale art. 76 alin. (2) din Constituția României, republicată.

p. PREȘEDINTELE
CAMEREI DEPUTAȚILOR



~~FLO~~RIN IORDACHE

PREȘEDINTELE
SENATULUI



CĂLIN POPESCU-TĂRICEANU

București, 28 decembrie 2018.
Nr. 362.

Sectoare de activitate și tipuri de entități

Sectorul	Subsectorul	Tipul de entitate
1. Energie	a) Electricitate	- Operatori economici din domeniul energiei electrice astfel cum sunt definiți la art. 3 pct. 42 din Legea energiei electrice și a gazelor naturale nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de distribuție, astfel cum sunt definiți la art. 3 pct. 39 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de transport și de sistem, astfel cum sunt definiți la art. 3 pct. 40 din Legea nr. 123/2012, cu modificările și completările ulterioare;
	b) Petrol	- Operatori de conducte de transport al petrolului;
		- Operatori ai instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport;
	c) Gaze naturale	- Furnizori persoană fizică sau juridică, astfel cum sunt definiți la art. 100 pct. 44 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de distribuție, astfel cum sunt definiți la art. 100 pct. 63 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de transport și de sistem, astfel cum sunt definiți la art. 100 pct. 65 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de înmagazinare, astfel cum sunt definiți la art. 100 pct. 64 din Legea nr. 123/2012, cu modificările și completările ulterioare;

		- Operatori ai terminalelor GNL, astfel cum sunt definiți la art. 100 pct. 60 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori economici din sectorul gazelor naturale, astfel cum sunt definiți la art. 100 pct. 67 din Legea nr. 123/2012, cu modificările și completările ulterioare;
		- Operatori de instalație de rafinare și de tratare a gazelor naturale;
2. Transport	a) Transport aerian	- Transportatori aerieni, astfel cum sunt definiți la art. 3 punctul 4 din Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002;
		- Organe de administrare a aeroportului, astfel cum sunt definite la art. 4 din Hotărârea Guvernului nr. 455/2011 privind tarifele de aeroport, inclusiv aeroporturile principale enumerate în Secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și de abrogare a Deciziei nr. 661/2010/UE, precum și entități care operează instalații auxiliare în cadrul aeroporturilor;
		- Operatori de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la art. 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea

		cerului unic European (regulament-cadru);
	b) Transport feroviar	- Administratori de infrastructuri, astfel cum sunt definiți la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spațiul feroviar unic european;
		- Întreprinderi feroviare, astfel cum sunt definite la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spațiul feroviar unic european;
	c) Transport pe apă	- Companii de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare, fără a include navele individuale operate de companiile respective;
		- Organe de gestionare a porturilor, astfel cum sunt definite la art. 3 din Ordinul ministrului transporturilor nr. 290/2007 pentru introducerea măsurilor de întărire a securității portuare, inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004 și entitățile care operează lucrări și echipamente în cadrul porturilor;
		- Operatori de servicii de trafic naval, astfel cum sunt definiți la art. 3 din Hotărârea Guvernului nr. 1016/2010 pentru stabilirea Sistemului de informare și monitorizare a traficului navelor maritime care intră/ies în/din apele naționale navigabile ale României, cu modificările și completările ulterioare;

	d) Transport rutier	- Autorități rutiere, astfel cum sunt definite la art. 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic, responsabile pentru controlul gestionării traficului;
		- Operatori de sisteme de transport inteligente, astfel cum sunt definiți la art. 4 din Ordonanța Guvernului nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru realizarea interfețelor cu alte moduri de transport, aprobată prin Legea nr. 221/2012;
3. Sectorul bancar		- Instituții de credit, astfel cum sunt definite la art. 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012;
4. Infrastructuri ale pieței financiare		- Operatori de locuri de tranzacționare, astfel cum sunt definite la art. 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE;
		- Contrapartide centrale, astfel cum sunt definite la art. 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate

		extrabursiere, contrapărțile centrale și registrele centrale de tranzacții;
5. Sectorul sănătății	Instituții de asistență medicală (inclusiv spitale și clinici private)	- Furnizori de servicii medicale, astfel cum sunt definiți în Hotărârea Guvernului nr. 304 din 16 aprilie 2014 pentru aprobarea Normelor metodologice privind asistența medicală transfrontalieră;
6. Furnizarea și distribuirea de apă potabilă		- Furnizori și distribuitori de apă destinată consumului uman, astfel cum sunt definiți la art. 2 din Legea nr. 458/2002 privind calitatea apei potabile, republicată, cu modificările și completările ulterioare, excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă doar o parte din activitatea lor generală de distribuire a altor produse de bază și produs care nu sunt considerate servicii esențiale;
7. Infrastructură digitală		- IXP
		- DNS
		- TLD