Consiliul
Uniunii Europene

Bruxelles, 26 noiembrie 2021
(OR. en)

14337/21

Dosar interinstituțional:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTĂ

Sursă:	Secretariatul General al Consiliului
Destinatar:	Consiliul
Nr. doc. ant.:	9583/2/21, 11724/21
Nr. doc. Csie:	14150/20
Subiect:	Propunere de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 *- Abordare generală*

I. INTRODUCERE

1. La 16 decembrie 2020, Comisia a adoptat propunerea de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS revizuită sau „NIS 2”)[1], cu scopul de a înlocui actuala Directivă privind securitatea rețelelor și a sistemelor informatice („Directiva NIS”)[2].

[1] Propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148.

[2] 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.

Propunerea a fost una dintre acțiunile prevăzute în Strategia de securitate cibernetică a UE pentru deceniul digital[3], cu scopul de a asigura faptul că cetățenii și întreprinderile beneficiază de tehnologii digitale de încredere.

2. Propunerea se întemeiază pe articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE) și vizează îmbunătățirea și mai mult a capacității de reziliență și a capacității de răspuns la incidente ale entităților publice și private, ale autorităților competente și ale Uniunii în ansamblu.

3. În cadrul Parlamentului European, comisia competentă pentru propunere este Comisia pentru industrie, cercetare și energie (ITRE). Comisia ITRE a adoptat raportul raportorului la 28 octombrie 2021.

4. Comitetul Economic și Social European și-a adoptat avizul la 28 aprilie 2021.

5. La 3 februarie 2021, Comitetul Reprezentanților Permanenți a decis să consulte Comitetul European al Regiunilor cu privire la propunere[4]. Până în prezent, Comitetul European al Regiunilor nu și-a dat avizul.

6. Autoritatea Europeană pentru Protecția Datelor și-a adoptat avizul la 11 martie 2021[5].

7. În cadrul concluziilor sale[6] din 22 martie 2021 privind Strategia de securitate cibernetică a UE pentru deceniul digital, Consiliul a luat act de noua propunere, care se bazează pe Directiva NIS, și și-a reafirmat sprijinul pentru consolidarea și armonizarea cadrelor naționale în materie de securitate cibernetică și pentru cooperarea susținută dintre statele membre.

8. În concluziile sale din 21-22 octombrie 2021, Consiliul European a indicat necesitatea intensificării lucrărilor cu privire la propunerea de revizuire a Directivei NIS.

---

3 14133/20
4 5573/21
5 Avizul 5/2021 privind Strategia de securitate cibernetică și Directiva NIS 2.0.
6 6722/21

II. LUCRĂRILE DESFĂȘURATE ÎN CADRUL GRUPURILOR DE PREGĂTIRE ALE CONSILIULUI

9. La nivelul Consiliului, examinarea propunerii s-a desfășurat în cadrul Grupului de lucru orizontal pentru chestiuni cibernetice (denumit în continuare „HWPCI”). Examinarea propunerii a început în timpul președinției portugheze, la 19 ianuarie, cu o lectură integrală aprofundată a propunerii, ceea ce a permis statelor membre să își prezinte întrebările și să își evidențieze principalele preocupări, precum și să primească explicații detaliate din partea Comisiei cu privire la modificările aduse în directiva revizuită.

10. În timpul președinției portugheze, HWPCI a dedicat 17 reuniuni prezentării și lecturii integrale a propunerii. A fost transmis un raport intermediar al lecturii integrale Consiliului TTE din 4 iunie 2021.

11. De atunci, lucrările au continuat și s-au intensificat în timpul președinției slovene, cu obiectivul de a se ajunge la o abordare generală în cadrul reuniunii Consiliului (Transporturi, Telecomunicații și Energie) din 3 decembrie 2021. Președinția slovenă a dedicat 15 reuniuni revizuirii propunerii NIS 2 și mai multe discuții bilaterale la toate nivelurile.

12. HWPCI și-a concentrat activitatea pe reformularea textului propunerii, la început pe interacțiunea Directivei NIS 2 cu legislația sectorială și domeniul de aplicare, în special în ceea ce privește administrația publică, pe serverele rădăcină DNS și clauza de excludere, iar apoi, printre altele, pe evaluările *inter pares*, competența și asistența reciprocă, divulgarea coordonată a vulnerabilităților, bazele de date cu numele de domenii și datele de înregistrare și cooperarea internațională.

13. O primă propunere de compromis privind textul directivei propuse a fost emisă la 21 septembrie 2021[7], pe baza observațiilor scrise și a documentelor neoficiale primite din partea statelor membre, precum și pe baza propunerilor de compromis anterioare cu privire la interacțiunea Directivei NIS 2 cu legislația sectorială și la domeniul de aplicare al Directivei NIS 2.

[7] 12019/21

14. Ultima revizuire[8] a propunerii de compromis a președinției a fost discutată la nivelul grupului de lucru la 22 noiembrie 2021. Cu toate că delegațiile au salutat, în general, textul de compromis, unele dintre ele au exprimat în continuare rezerve de examinare sau au formulat observații cu privire la anumite părți ale propunerii de compromis. Au fost sugerate în continuare unele reformulări tehnice la anumite părți ale textului.

III. FOND

15. Pe baza discuțiilor purtate la nivelul grupului de lucru, au fost identificate următoarele puncte ca fiind principalele chestiuni politice:

a) Domeniul de aplicare (articolul 2)

De la începutul discuțiilor privind propunerea NIS 2, principala preocupare exprimată de statele membre a fost creșterea semnificativă a numărului de entități care intră sub incidența directivei și, în special, introducerea regulii privind un prag după criteriul de dimensiune, conform căreia toate entitățile medii și mari care își desfășoară activitatea în cadrul sectoarelor sau furnizează serviciile reglementate de Directiva NIS 2 intră în domeniul său de aplicare. Deși propunerea de compromis menține această regulă generală, ea include dispoziții suplimentare pentru a asigura proporționalitatea necesară, un nivel mai ridicat de gestionare a riscurilor și criterii clare de criticitate pentru stabilirea entităților care intră în domeniul de aplicare al directivei. În plus, propunerea de compromis include dispoziții specifice privind stabilirea priorităților în ceea ce privește utilizarea măsurilor de supraveghere, urmând o abordare bazată pe riscuri.

[8] 12019/5/21 REV 5

b) Administrația publică [articolul 2 alineatul (2a)]

Includerea administrației publice în domeniul de aplicare al Directivei NIS 2 a fost un subiect foarte dezbătut, având în vedere că sectorul administrației publice este mai diferențiat decât alte sectoare vizate de Directiva NIS 2. Președinția a căutat o abordare echilibrată care să țină seama de particularitățile cadrelor naționale specifice administrației publice și care să garanteze că statele membre dispun de un anumit grad de flexibilitate în ceea ce privește stabilirea entităților administrației publice care intră în domeniul de aplicare al NIS 2. Prin urmare, în textul de compromis, NIS 2 se aplică entităților administrației publice din administrația centrală, iar statele membre pot stabili, de asemenea, că directiva se aplică și entităților administrației publice de la nivel regional și local.

c) Clauza de excludere [articolul 2 punctele 3a și 3aa)]

Statele membre au dorit să clarifice mai bine clauza de excludere, în sensul că directiva nu se aplică entităților care desfășoară în principal activități în domeniul apărării, securității naționale, siguranței publice sau al asigurării respectării legii și nici activităților legate de securitatea sau apărarea națională. Sunt excluse, de asemenea, sistemul judiciar, parlamentele și băncile centrale.

d) Interacțiunea cu legislația sectorială

Statele membre au subliniat necesitatea alinierii între Directiva NIS 2 și legislația sectorială, în special Regulamentul privind reziliența operațională digitală a sectorului financiar („DORA”) și Directiva privind reziliența entităților critice (directiva „CER”). Directiva NIS 2, care ar trebui să fie referința pentru o armonizare minimă privind securitatea cibernetică, conține un articol specific referitor la actele sectoriale ale Uniunii (articolul 2b). În ceea ce privește interacțiunea cu Directiva CER, propunerea de compromis asigură o mai mare claritate în ceea ce privește abordarea bazată pe „toate pericolele”. Alte adăugiri importante sunt legate de acordurile de cooperare dintre autoritățile competente în temeiul respectivelor acte juridice.

e) Învățarea reciprocă (articolul 16)

Cu unele excepții, statele membre s-au opus instituirii de către Comisie a unor evaluări *inter pares* obligatorii. Compromisul propus asigură faptul că noul mecanism de învățare *inter pares* se bazează pe încredere reciprocă și este un proces voluntar și coordonat de statele membre.

f) Competență și teritorialitate (articolul 24) și asistență reciprocă (articolul 34)

Statele membre și-au exprimat îngrijorarea cu privire la consecințele unei jurisdicții diferențiate pentru entitățile din sectorul TIC, astfel cum a propus Comisia. Textul de compromis a clarificat competența în funcție de tipul de entități și a introdus formulări mai ferme privind asistența reciprocă.

g) Obligații de raportare (articolul 20)

În urma preocupărilor exprimate de statele membre, în sensul că aceste obligații ar reprezenta o sarcină excesivă pentru entitățile care intră sub incidența Directivei NIS 2 și ar conduce la supra-raportare, raportarea obligatorie pentru amenințările cibernetice semnificative a fost exclusă din textul de compromis.

IV. CONCLUZII

16. La 24 noiembrie 2021, Comitetul Reprezentanților Permanenți a ajuns la un acord cu privire la textul de compromis, astfel cum figurează în anexă, și a decis să îl transmită Consiliului (Transporturi, Telecomunicații și Energie) în vederea adoptării unei abordări generale.

17. Prin urmare, Consiliul este invitat să aprobe textul de compromis prezentat de președinție, astfel cum figurează în anexă, și să adopte o abordare generală în cadrul reuniunii sale din 3 decembrie 2021.

ANEXĂ

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[9],

având în vedere avizul Comitetului Regiunilor[10],

hotărând în conformitate cu procedura legislativă ordinară,

[9] JO C , , p. .
[10] JO C , , p. .

întrucât:

(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[11] vizează consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente de securitate cibernetică, contribuind astfel la funcționarea eficace a economiei și a societății Uniunii.

(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență a securității cibernetice în Uniune. Revizuirea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă de mentalitate. Această directivă a asigurat finalizarea cadrelor naționale prin definirea strategiilor naționale [...] **privind securitatea rețelelor și a sistemelor informatice**, prin stabilirea de capacități naționale și prin punerea în aplicare a măsurilor de reglementare care vizează infrastructurile esențiale și actorii identificați de fiecare stat membru. De asemenea, a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare[12] și a [...] **rețelei** de echipe naționale de intervenție în caz de incidente de securitate informatică („rețeaua CSIRT”)[13]. În pofida acestor realizări, revizuirea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să abordeze în mod eficace provocările contemporane și emergente în materie de securitate cibernetică.

---

11 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 (JO L 194/1, 19.7.2016, p. 1).

12 Articolul 11 din Directiva (UE) 2016/1148.

13 Articolul 12 din Directiva (UE) 2016/1148.

(3) Rețelele și sistemele informatice reprezintă acum o componentă centrală a vieții de zi cu zi, odată cu transformarea digitală rapidă și interconectarea societății, inclusiv în cadrul schimburilor transfrontaliere. Această transformare a condus la o extindere a situației amenințărilor la adresa securității cibernetice, generând noi provocări, care necesită răspunsuri adaptate, coordonate și inovatoare în toate statele membre. Incidentele de securitate sunt tot mai numeroase, mai ample, mai sofisticate și cu un impact tot mai mare, acestea reprezentând o amenințare gravă la adresa funcționării rețelelor și a sistemelor informatice. Prin urmare, incidentele cibernetice pot să împiedice desfășurarea activităților economice pe piața internă, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei și societății Uniunii. Prin urmare, pregătirea și eficacitatea în materie de securitate cibernetică sunt acum mai importante ca niciodată pentru buna funcționare a pieței interne.

(4) Temeiul juridic al Directivei (UE) 1148/2016 este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), al cărui obiectiv este instituirea și funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor naționale. Cerințele de securitate cibernetică impuse entităților care furnizează servicii sau activități relevante din punct de vedere economic variază considerabil de la un stat membru la altul în ceea ce privește tipul de cerință, nivelul lor de detaliere și metoda de supraveghere. Aceste disparități implică costuri suplimentare și creează dificultăți pentru întreprinderile care oferă bunuri sau servicii la nivel transfrontalier. Cerințele impuse de un stat membru care sunt diferite sau chiar în conflict cu cele impuse de un alt stat membru pot afecta în mod substanțial activitățile transfrontaliere respective.

În plus, conceperea unor standarde de securitate cibernetică sub nivelul optim sau punerea în aplicare sub nivel optim a [...] **măsurilor** de securitate cibernetică într-un stat membru pot avea repercusiuni asupra nivelului de securitate cibernetică al altor state membre, în special în contextul schimburilor transfrontaliere intense. Revizuirea Directivei (UE) 2016/1148 a arătat că punerea sa în aplicare diferă foarte mult de la un stat membru la altul, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată în mare măsură la latitudinea statelor membre. Directiva (UE) 2016/1148 a acordat, de asemenea, statelor membre o marjă de apreciere foarte largă în ceea ce privește punerea în aplicare a obligațiilor de raportare în materie de securitate și de raportare a incidentelor pe care le prevede aceasta. Prin urmare, aceste obligații au fost puse în aplicare în moduri foarte diferite la nivel național. Divergențe similare în ceea ce privește punerea în aplicare s-au înregistrat și în ceea ce privește dispozițiile directivei respective privind supravegherea și asigurarea respectării legislației.

(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență în materie de securitate cibernetică din cauza aplicării unor [...] **măsuri** diferite. Prezenta directivă urmărește să elimine divergențele importante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și sancțiuni eficace care sunt esențiale pentru asigurarea eficace a respectării acestor obligații. Directiva (UE) 2016/1148 trebuie, prin urmare, abrogată și înlocuită cu prezenta directivă.

(6) [...] Statele membre ar trebui să **poată** lua măsurile necesare pentru a asigura protecția intereselor lor esențiale de securitate, a apăra ordinea și siguranța publică și a permite investigarea, detectarea și urmărirea infracțiunilor[...].[...] **Directiva nu ar trebui să se aplice anumitor entități publice sau private care desfășoară activități în aceste domenii. De asemenea, directiva nu ar trebui să se aplice activităților entităților desfășurate în aceste domenii. În plus,** niciun stat membru nu are obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale siguranței sale publice. [...] Sunt relevante normele naționale **sau** cele ale Uniunii privind protecția informațiilor clasificate și acordurile de nedivulgare sau acordurile de nedivulgare informale, precum „Traffic Light Protocol”[14].

(6a) Dreptul Uniunii privind protecția datelor cu caracter personal și a vieții private se aplică oricărei forme de prelucrare a datelor cu caracter personal în temeiul prezentei directive. Concret, prezenta directivă nu aduce atingere Regulamentului (UE) 2016/679 și nici Directivei 2002/58/CE a Parlamentului European și a Consiliului și, prin urmare, nu ar trebui, în special, să aducă atingere sarcinilor și competențelor autorităților independente de supraveghere competente să monitorizeze respectarea dreptului respectiv al Uniunii în materie de protecție a datelor.

[14] Traffic Light Protocol (TLP) este un mijloc prin care cineva care face schimb de informații își informează publicul cu privire la eventualele limitări în răspândirea în continuare a acestor informații. Acest instrument este utilizat în aproape toate comunitățile CSIRT și în unele centre de schimb de informații și de analiză (ISAC).

(7) Odată cu abrogarea Directivei (UE) 2016/1148, domeniul de aplicare ar trebui extins la mai multe sectoare economice, având în vedere considerentele 4-6. Sectoarele reglementate de Directiva (UE) 2016/1148 ar trebui, prin urmare, să fie extinse pentru a oferi o acoperire cuprinzătoare a sectoarelor și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. Normele nu ar trebui să fie diferite în funcție de statutul entităților: operatori de servicii esențiale sau furnizori de servicii digitale. Această diferențiere s-a dovedit a fi caducă, deoarece nu reflectă importanța reală a sectoarelor sau a serviciilor pentru activitățile sociale și economice de pe piața internă.

(8) În conformitate cu Directiva (UE) 2016/1148, statele membre au fost responsabile de stabilirea entităților care îndeplinesc criteriile pentru a fi considerate operatori de servicii esențiale („procesul de identificare”). Pentru a elimina divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește cerințele de gestionare a riscurilor și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform care să stabilească care sunt entitățile ce intră în domeniul de aplicare al prezentei directive. Acest criteriu ar trebui să constea în aplicarea regulii privind criteriul de dimensiune, conform căruia toate întreprinderile mijlocii și mari, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[15], care își desfășoară activitatea în sectoarele reglementate de prezenta directivă sau furnizează tipul de servicii reglementate de aceasta, intră în domeniul său de aplicare. [...]

[15] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

(8a) Pentru a asigura o imagine de ansamblu clară a entităților care intră în domeniul de aplicare al prezentei directive, statele membre ar trebui să poată institui mecanisme naționale de autonotificare care să impună entităților care fac obiectul prezentei directive să transmită cel puțin numele, adresa și datele lor de contact, precum și sectorul în care își desfășoară activitatea sau tipul de serviciu pe care îl furnizează și, după caz, o listă a statelor membre în care entitatea își furnizează serviciile autorităților competente în temeiul prezentei directive sau organismelor desemnate în acest scop de către statele membre. Statele membre pot decide cu privire la mecanismele adecvate, în cazul în care există registre la nivel național, care să permită identificarea entităților care intră în domeniul de aplicare al prezentei directive.

(9) [...] **Microentitățile** sau entitățile mici care îndeplinesc anumite criterii ce indică un rol-cheie pentru economiile sau societățile statelor membre sau pentru anumite sectoare sau tipuri de servicii ar trebui să intre, de asemenea, sub incidența prezentei directive. Statele membre ar trebui să fie responsabile de [...] **transmiterea către** [...] Comisie **cel puțin a informațiilor relevante privind numărul de entități identificate, sectorul din care fac parte sau tipul de servicii pe care le furnizează, precum și criteriile specifice pe baza cărora au fost identificate. De asemenea, statele membre pot decide, în conformitate cu normele naționale în materie de securitate, să transmită Comisiei denumirile acestor entități.**

(9a) Entitățile administrației publice care desfășoară activități în domeniul securității naționale, al apărării, al securității publice și al asigurării respectării legii, precum și sistemul judiciar, parlamentele și băncile centrale sunt excluse din domeniul de aplicare al prezentei directive. În sensul prezentei directive, entitățile cu competențe de reglementare nu sunt considerate ca desfășurând activități în domeniul asigurării respectării legii și, prin urmare, nu sunt excluse din aceste motive din domeniul de aplicare al prezentei directive. În plus, entitățile administrației publice din administrația centrală care sunt înființate în comun cu o țară terță în conformitate cu un acord internațional, nu intră în domeniul de aplicare al prezentei directive.

(9aa) Statele membre ar trebui să poată stabili că entitățile identificate înainte de intrarea în vigoare a prezentei directive ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 vor fi considerate entități esențiale.

(9aaa) Prezenta directivă nu se aplică misiunilor diplomatice și consulare ale statelor membre în străinătate și nici infrastructurii TIC a acestora utilizate de astfel de misiuni, în măsura în care infrastructura respectivă este situată în străinătate sau este exploatată pentru utilizatori din străinătate.

(10) Comisia, în cooperare cu Grupul de cooperare, poate emite orientări privind punerea în aplicare a criteriilor aplicabile microîntreprinderilor și întreprinderilor mici.

(11) [...] **Entitățile care intră în domeniul de aplicare al prezentei directive ar trebui clasificate în două categorii - esențiale și importante - care țin seama de nivelul de criticitate al sectorului sau de tipul de servicii pe care le furnizează, precum și de dimensiunea acestora. În acest sens, ar trebui de asemenea să se țină seama în mod corespunzător de toate evaluările riscurilor sau orientările sectoriale relevante emise de către autoritățile competente, după caz.** Entitățile esențiale și cele importante ar trebui să fie supuse [...] cerințelor de gestionare a riscurilor și obligațiilor de raportare. Regimurile de supraveghere și de sancționare corespunzătoare acestor două categorii de entități ar trebui diferențiate pentru a asigura un echilibru corect între cerințele și obligațiile **bazate pe riscuri**, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.

(12) **Prezenta directivă stabilește nivelul de referință pentru măsurile de gestionare a riscurilor la adresa securității cibernetice și pentru obligațiile de raportare în toate sectoarele care intră în domeniul său de aplicare. Pentru a evita fragmentarea dispozițiilor privind securitatea cibernetică din actele juridice ale Uniunii, atunci când, pentru a se asigura un nivel ridicat de securitate cibernetică, sunt considerate necesare dispoziții sectoriale suplimentare legate de** măsurile de gestionare a riscurilor în materie de securitate cibernetică **și de obligațiile de raportare, Comisia ar trebui să evalueze dacă astfel de dispoziții ar putea fi prevăzute într-un act de punere în aplicare în temeiul împuternicirii prevăzute în prezenta directivă. În cazul în care astfel de acte nu sunt adecvate scopului respectiv,** legislația sectorială **ar putea** contribui la asigurarea **unui** nivel ridicat[...] de securitate cibernetică, ținând seama pe deplin de particularitățile și de complexitatea [...] sectoarelor **în cauză**. **Motivul pentru care un act de punere în aplicare în temeiul împuternicirii prevăzute în prezenta directivă nu a fost considerat adecvat trebuie explicat în legislația sectorială specifică. În același timp, astfel de dispoziții sectoriale ale actelor juridice ale Uniunii ar trebui să țină seama în mod corespunzător de necesitatea unui cadru cuprinzător și armonizat în materie de securitate cibernetică.** Aceasta nu aduce atingere competențelor de executare existente care i-au fost conferite Comisiei într-o serie de sectoare, inclusiv în domeniul transporturilor și în cel al energiei.

(12a) În cazul în care un act juridic sectorial al Uniunii **conține dispoziții** [...] **care impun** entităților esențiale sau importante să adopte **măsuri cu un efect cel puțin echivalent cu obligațiile prevăzute în prezenta directivă legate de** gestionarea riscurilor în materie de securitate cibernetică [...] **și cu obligațiile** de a notifica incidentele **semnificative** sau amenințările cibernetice semnificative [...], ar trebui să se aplice dispozițiile sectoriale respective**, inclusiv cele privind supravegherea și asigurarea respectării legii**. **La stabilirea efectului echivalent al obligațiilor prevăzute în dispozițiile sectoriale ale unui act juridic al Uniunii, ar trebui avute în vedere următoarele aspecte: (i) măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să constea în măsuri tehnice și organizatorice adecvate și proporționale de gestionare a riscurilor la adresa securității rețelelor și a sistemelor informatice pe care entitățile relevante le utilizează pentru furnizarea serviciilor lor și ar trebui să includă cel puțin toate elementele prevăzute în prezenta directivă; (ii) obligația de a notifica incidentele și amenințările cibernetice semnificative ar trebui să fie cel puțin echivalentă cu obligațiile prevăzute în prezenta directivă în ceea ce privește conținutul, formatul și termenele notificărilor; (iii) modalitățile de raportare de către entități și autoritățile relevante a actelor juridice sectoriale ale Uniunii ar trebui să fie cel puțin echivalente cu cerințele prevăzute în prezenta directivă în ceea ce privește conținutul, formatul și termenele și ar trebui să țină seama de rolul CSIRT; (iv) cerințele de cooperare transfrontalieră pentru autoritățile relevante ar trebui să fie cel puțin echivalente cu cele prevăzute în prezenta directivă. În cazul în care dispozițiile sectoriale ale unui act juridic al Uniunii nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive ar trebui să se aplice în continuare entităților care nu fac obiectul dispozițiilor sectoriale respective.**

(12aa) Comisia **ar trebui să revizuiască periodic aplicarea cerinței privind efectul echivalent în legătură cu dispozițiile sectoriale specifice ale actelor juridice ale Uniunii** [...]. **Comisia trebuie să consulte grupul de cooperare atunci când pregătește revizuirea periodică.**

(12aaa) Viitoarele acte legislative sectoriale ale Uniunii ar trebui să țină seama în mod corespunzător de definițiile enunțate la articolul 4 din prezenta directivă și de cadrul de supraveghere și de asigurare a respectării legii prevăzut în capitolul VI din prezenta directivă.

(12ab) În cazul în care dispozițiile sectoriale ale actelor juridice ale Uniunii impun entităților esențiale sau importante să adopte măsuri cu efect cel puțin echivalent cu obligațiile de raportare prevăzute în prezenta directivă, ar trebui evitată suprapunerea obligațiilor de raportare și ar trebui să se asigure coerența și eficacitatea gestionării notificărilor privind amenințările sau incidentele cibernetice. În acest scop, dispozițiile sectoriale respective pot permite statelor membre să instituie un mecanism de raportare comun, automat și direct pentru notificarea incidentelor și a amenințărilor cibernetice semnificative atât autorităților ale căror sarcini sunt prevăzute în dispozițiile sectoriale respective, cât și autorităților competente, inclusiv punctului unic de contact și CSIRT, după caz, responsabile de sarcinile în materie de securitate cibernetică prevăzute în prezenta directivă, sau un mecanism care să asigure schimbul sistematic și imediat de informații și cooperarea între autoritățile relevante și CSIRT în ceea ce privește gestionarea unor astfel de notificări. În scopul simplificării raportării și al punerii în aplicare a mecanismului de raportare comun, automat și direct, statele membre pot utiliza, în conformitate cu legislațiile sectoriale specifice, punctul de intrare unic pe care îl instituie în conformitate cu articolul 11 alineatul (5a) din prezenta directivă. Pentru a asigura armonizarea, obligațiile de raportare prevăzute de actele juridice sectoriale ale Uniunii ar trebui să fie aliniate cu cele specificate în prezenta directivă. Statele membre pot stabili că autoritățile competente în temeiul prezentei directive sau CSIRT naționale sunt destinatarii raportării, în conformitate cu legislațiile sectoriale.

(13) În ceea ce privește entitățile din sectorul financiar, Regulamentul XXXX/XXXX al Parlamentului European și al Consiliului ar trebui considerat un act juridic sectorial al Uniunii în legătură cu prezenta directivă. Dispozițiile Regulamentului XXXX/XXXX referitoare la măsurile de gestionare a riscurilor legate de tehnologia informației și comunicațiilor (TIC), la gestionarea incidentelor legate de TIC și, în special, la raportarea incidentelor, precum și cele referitoare la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscul asociat furnizorilor terți de servicii TIC ar trebui să se aplice în locul celor [...] **prevăzute** în prezenta directivă. Prin urmare, în cazul entităților financiare care intră sub incidența Regulamentului XXXX/XXXX, statele membre nu ar trebui să aplice dispozițiile prezentei directive privind obligațiile de gestionare și raportare a riscurilor în materie de securitate cibernetică [...], supravegherea și asigurarea respectării legii. În același timp, este important ca, în temeiul prezentei directive, să se mențină o relație puternică cu sectorul financiar și să se facă un schimb de informații cu acesta. Astfel, în temeiul Regulamentului XXXX/XXXX, [...] autoritățile europene de supraveghere (AES) pentru sectorul financiar și autoritățile naționale competente în temeiul Regulamentului XXXX/XXXX[...] pot participa la [...] **lucrările** Grupului de cooperare, pot face schimb de informații și pot coopera cu punctele unice de contact desemnate în temeiul prezentei directive**, precum** și cu CSIRT naționale. Autoritățile competente în temeiul Regulamentului XXXX/XXXX ar trebui să transmită detaliile incidentelor majore legate de TIC **și ale amenințărilor cibernetice semnificative** și punctelor unice de contact**, autorităților competente sau CSIRT naționale** desemnate în temeiul prezentei directive. **Acest lucru poate fi realizat prin transmiterea automată și directă a notificărilor incidentelor sau prin intermediul unei platforme comune de raportare.** În plus, statele membre ar trebui să includă în continuare sectorul financiar în strategiile lor de securitate cibernetică, iar CSIRT naționale pot acoperi sectorul financiar în activitățile lor.

(13a) Pentru a evita lacunele și suprapunerile obligațiilor în materie de securitate cibernetică impuse entităților din sectorul aviației menționate la punctul 2 litera (a) din anexa I, autoritățile naționale desemnate în temeiul Regulamentelor (CE) nr. 300/2008[16] și (UE) 2018/1139[17] ale Parlamentului European și ale Consiliului și autoritățile competente în temeiul prezentei directive ar trebui să coopereze în ceea ce privește punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și supravegherea măsurilor respective la nivel național. Respectarea de către o entitate a măsurilor de gestionare a riscurilor în materie de securitate cibernetică prevăzute în prezenta directivă ar putea fi considerată de autoritățile naționale desemnate în temeiul Regulamentelor (CE) nr. 300/2008 și (UE) 2018/1139 ca fiind conformă cu cerințele prevăzute în regulamentele respective și în actele delegate și de punere în aplicare relevante adoptate în temeiul lor.

---

16 **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 (JO L 97, 9.4.2008, p. 72).**

17 **Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).**

(14) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) XXX/XXX a Parlamentului European și a Consiliului și prezenta directivă. În acest scop, statele membre ar trebui să se asigure că, în temeiul Directivei (UE) XXX/XXX, entitățile critice **[**și entitățile echivalente**]** sunt considerate entități esențiale în temeiul prezentei directive. Statele membre ar trebui, de asemenea, să se asigure că strategiile lor în materie de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată între autoritatea competentă în temeiul prezentei directive și cea competentă în temeiul Directivei (UE) XXX/XXX în contextul schimbului de informații privind incidentele și amenințările cibernetice și al exercitării sarcinilor de supraveghere. Autoritățile **competente** în temeiul acestor două directive ar trebui să coopereze și să facă schimb de informații, în special în ceea ce privește identificarea entităților critice, amenințările cibernetice, riscurile în materie de securitate cibernetică, incidentele, **precum și riscurile, amenințările și incidentele de altă natură decât cibernetică** ce afectează entitățile critice **[**sau **entități echivalente cu entitățile critice]**, [...] **inclusiv** măsurile de securitate **fizică** și cibernetică adoptate de entitățile critice și rezultatele activităților de supraveghere desfășurate în raport cu astfel de entități. **În plus, pentru a simplifica activitățile de supraveghere între autoritățile competente desemnate în temeiul ambelor directive și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și procesele de supraveghere.** [...] **După caz,** autoritățile competente în temeiul Directivei (UE) XXX/XXX[...] **pot solicita** autorităților competente în temeiul prezentei directive [...] să își exercite competențele de supraveghere și de asigurare a respectării legii [...] **în raport cu** o entitate esențială identificată ca fiind critică. [...]

(14a) Entitățile care aparțin sectorului infrastructurii digitale se bazează, în esență, pe rețele și sisteme informatice și, prin urmare, obligațiile impuse acestor entități prin prezenta directivă ar trebui să abordeze în mod cuprinzător securitatea fizică a acestor sisteme, ca parte a obligațiilor lor de raportare și de gestionare a riscurilor în materie de securitate cibernetică. Întrucât aceste aspecte sunt reglementate de prezenta directivă, obligațiile prevăzute în capitolele III-VI din Directiva (UE) XXX/XXX [CER] nu se aplică acestor entități.

(15) Respectarea și menținerea unui sistem fiabil, rezilient și sigur de nume de domenii (DNS) este un factor-cheie pentru menținerea integrității internetului, esențial pentru funcționarea sa continuă și stabilă, de care depind economia digitală și societatea. Prin urmare, prezenta directivă ar trebui să se aplice furnizorilor de servicii DNS de-a lungul lanțului de furnizare și rezolvare a DNS care prezintă importanță pentru piața internă, inclusiv [...] registrelor cu nume de domeniu de prim nivel (TLD) [...], entităților care prestează servicii de înregistrare a numelor de domenii, operatorilor de servere de nume cu autoritate pentru nume de domenii și operatorilor de rezolvere recursive. **Termenul „furnizor de servicii DNS” nu ar trebui să se aplice serviciilor DNS operate în scopurile proprii ale entității în cauză și ale entităților sale afiliate. Obligațiile în materie de securitate cibernetică ce decurg din prezenta directivă pentru această categorie de furnizori sunt strict limitate la măsurile de gestionare a riscurilor în materie de securitate cibernetică și la raportare, prin urmare, nu aduc atingere guvernanței sistemului DNS mondial de către comunitatea multiparticipativă.**

(16) Serviciile de cloud computing ar trebui să acopere serviciile care permit, la cerere, accesul larg de la distanță la un bazin elastic și redimensionabil de resurse informatice care pot fi puse în comun și distribuite. Noțiunea de „resurse informatice” include resurse precum rețelele, serverele sau alte infrastructuri, sistemele de operare, software-urile, stocarea, aplicațiile și serviciile. **Modelele de servicii de cloud computing includ, printre altele, infrastructura ca serviciu (IaaS), platforma ca serviciu (PaaS), software-ul ca serviciu (SaaS) și rețeaua ca serviciu (NaaS).** Modelele de implementare a cloud computingului ar trebui să includă tehnologiile de tip cloud private, comunitare, publice și hibride. Modelele de servicii și de implementare menționate anterior au același înțeles ca și termenii modelelor de servicii și de implementare definiți în standardul ISO/IEC 17788:2014. Capacitatea utilizatorului de cloud computing de a furniza în mod unilateral capacități de calcul autonome, cum ar fi ora serverului sau stocarea în rețea, fără nicio interacțiune umană din partea furnizorului de servicii de cloud computing, ar putea fi descrisă ca administrare la cerere. Termenul „acces larg la distanță” este utilizat pentru a descrie faptul că aceste capacități de cloud sunt furnizate prin rețea și accesate prin mecanisme care promovează utilizarea unor platforme eterogene, subțiri sau groase pentru clienți (inclusiv telefoane mobile, tablete, laptopuri, stații de lucru).

Termenul „redimensionabil” se referă la resursele informatice care se alocă flexibil de către furnizorul de servicii cloud, indiferent de poziția geografică a resurselor, pentru a administra fluctuațiile de cerere. Termenul „bazin elastic” se referă la acele resurse informatice care sunt atribuite și transferate în funcție de cerere, pentru a înmulți și a reduce rapid resursele disponibile în conformitate cu volumul de lucru. Sintagma „care pot fi puse în comun” descrie acele resurse informatice care sunt furnizate mai multor utilizatori care au acces comun la serviciu, dar tratamentul se efectuează separat pentru fiecare utilizator, deși serviciul este furnizat de același echipament electronic. Termenul „distribuit” se referă la acele resurse informatice care sunt situate pe diferite calculatoare sau dispozitive în rețea și care comunică și se coordonează între ele prin transmiterea de mesaje.

(17) Având în vedere apariția unor tehnologii inovatoare și a unor noi modele de afaceri, se preconizează că pe piață vor apărea noi modele de implementare și de servicii de cloud computing ca răspuns la evoluția nevoilor clienților. În acest context, serviciile de cloud computing pot fi furnizate într-o formă foarte distribuită, chiar mai aproape de locul în care datele sunt generate sau colectate, trecând astfel de la modelul tradițional la unul foarte distribuit („tehnica de calcul la margine”).

(18) Este posibil ca serviciile oferite de furnizorii de servicii de centre de date să nu fie întotdeauna furnizate sub formă de servicii de cloud computing. În consecință, este posibil ca centrele de date să nu constituie întotdeauna o parte a infrastructurii de cloud computing. Pentru a gestiona toate riscurile la adresa securității rețelelor și a sistemelor informatice, prezenta directivă ar trebui să vizeze și furnizorii de astfel de servicii de centre de date care nu sunt servicii de cloud computing. În sensul prezentei directive, termenul „serviciu de centru de date” ar trebui să includă furnizarea unui serviciu care cuprinde structuri sau grupuri de structuri dedicate instalării centralizate, interconectării și funcționării tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului. Termenul „serviciu de centre de date” nu se aplică centrelor de date interne, corporative deținute și operate în scopuri proprii entității în cauză.

(19) Furnizorii de servicii poștale în sensul Directivei 97/67/CE a Parlamentului European și a Consiliului[18], [...] **inclusiv** furnizorii de servicii de curierat[...] ar trebui să facă obiectul prezentei directive în cazul în care asigură cel puțin una dintre etapele lanțului de distribuție poștală, în special ridicarea, sortarea sau distribuția, inclusiv serviciile de preluare. Serviciile de transport care nu sunt efectuate împreună cu una dintre aceste etape nu ar trebui să intre în domeniul de aplicare al serviciilor poștale.

---

18 Directiva 97/67/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind normele comune pentru dezvoltarea pieței interne a serviciilor poștale ale Comunității și îmbunătățirea calității serviciului (JO L 15, 21.1.1998, p. 14).

(20) Aceste interdependențe din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de furnizare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu acoperă, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programelor sale spațiale. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. Pandemia de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere.

(**20a**) **În scopul atingerii și menținerii unui nivel ridicat de securitate cibernetică, strategiile naționale în materie de securitate cibernetică impuse de prezenta directivă ar trebui să constea în cadre coerente care să prevadă o guvernanță în domeniul securității cibernetice. Aceste strategii pot fi compuse din unul sau mai multe documente legislative sau fără caracter legislativ.**

(21) Având în vedere diferențele dintre structurile naționale de guvernanță și pentru a salvgarda acordurile sectoriale sau organismele de supraveghere și de reglementare ale Uniunii deja existente, statele membre ar trebui să fie capabile să desemneze mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale entităților importante în temeiul prezentei directive. Statele membre ar trebui să fie capabile să atribuie acest rol unei autorități existente.

(22) Pentru a facilita cooperarea și comunicarea transfrontalieră între autorități și pentru a permite aplicarea efectivă a prezentei directive, este necesar ca fiecare stat membru să desemneze un punct unic de contact la nivel național responsabil cu coordonarea aspectelor legate de securitatea rețelelor și a sistemelor informatice și cu cooperarea transfrontalieră la nivelul Uniunii.

(23) Autoritățile competente sau CSIRT-urile ar trebui să primească de la entități notificări ale incidentelor într-un mod eficace și eficient**, inclusiv pentru a facilita, după caz, o reacție promptă la incidente și pentru a oferi un răspuns entității notificatoare**. Punctele unice de contact ar trebui să aibă sarcina de a transmite notificările incidentelor către punctele unice de contact ale altor state membre afectate. [...]

(23a) Actele juridice sectoriale ale Uniunii care impun măsuri de gestionare a riscurilor în materie de securitate cibernetică sau obligații de raportare cu efect cel puțin echivalent cu cele prevăzute în prezenta directivă ar putea prevedea ca autoritățile competente desemnate să își exercite competențele de supraveghere și de asigurare a respectării legii în raport cu astfel de măsuri sau obligații, cu sprijinul autorităților competente desemnate în conformitate cu prezenta directivă. Autoritățile competente în cauză ar putea stabili acorduri de cooperare în acest scop. Astfel de acorduri de cooperare ar putea specifica, printre altele, procedurile privind coordonarea activităților de supraveghere, inclusiv procedurile de investigație și de inspecție la fața locului în conformitate cu legislația națională, precum și un mecanism pentru schimbul de informații relevante între autoritățile competente în materie de supraveghere și asigurare a respectării legii, inclusiv accesul la informațiile legate de domeniul cibernetic solicitate de autoritățile competente desemnate în conformitate cu prezenta directivă.

(24) Statele membre ar trebui să fie echipate în mod adecvat, din punct de vedere al capacității atât tehnice, cât și organizatorice, pentru a preveni, a detecta, a combate și a atenua incidentele și riscurile la care sunt supuse rețelele și sistemele informatice. Prin urmare, statele membre ar trebui să se asigure că dețin CSIRT care funcționează corespunzător, cunoscute și drept echipe de intervenție în caz de urgență informatică („CERT”), care respectă cerințele esențiale pentru a garanta existența capacităților eficace și compatibile care să administreze incidentele și riscurile și să asigure o cooperare eficientă la nivelul Uniunii. În vederea consolidării relației de încredere dintre entități și CSIRT, în cazurile în care o echipă CSIRT face parte din autoritatea competentă, statele membre [...] **pot** să aibă în vedere separarea funcțională între sarcinile operaționale furnizate de CSIRT, în special în ceea ce privește schimbul de informații și sprijinul acordat entităților, și activitățile de supraveghere ale autorităților competente.

(25) În ceea ce privește datele cu caracter personal, CSIRT ar trebui să poată furniza, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[19], în ceea ce privește datele cu caracter personal, în numele și la cererea unei entități în temeiul prezentei directive, o scanare proactivă a rețelei și a sistemelor informatice utilizate pentru furnizarea serviciilor lor. **După caz,** statele membre ar trebui să vizeze asigurarea unui nivel egal al capacităților tehnice pentru toate CSIRT-urile sectoriale. Statele membre pot solicita asistența Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) la dezvoltarea echipelor CSIRT naționale.

(26) Având în vedere importanța cooperării internaționale în privința securității cibernetice, CSIRT ar trebui să aibă posibilitatea să participe la rețele de cooperare internațională, în plus față de rețeaua CSIRT instituită prin prezenta directivă. **Prin urmare, CSIRT-urile și autoritățile competente ar putea face schimb de informații, inclusiv de date cu caracter personal, cu CSIRT-uri din țări terțe sau cu autoritățile acestora, în scopul îndeplinirii sarcinilor care le revin în conformitate cu Regulamentul (UE) 2016/679. În absența unei decizii privind caracterul adecvat al nivelului de protecție adoptate în conformitate cu articolul 45 din Regulamentul (UE) 2016/679 sau a unor garanții adecvate în temeiul articolului 46 din același regulament, schimbul de date cu caracter personal care este considerat necesar în scopul atenuării amenințărilor cibernetice semnificative și al asigurării răspunsului la un incident semnificativ în desfășurare ar putea fi considerat un considerent important de interes public în sensul articolului 49 alineatul (1) litera (d) din Regulamentul (UE) 2016/679.**

[19] 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 (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

(27) În conformitate cu anexa la Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („Blueprint”)[20], un incident de mare anvergură ar trebui să însemne un incident cu un impact semnificativ asupra a cel puțin două state membre sau care provoacă o perturbare ce depășește capacitatea unui stat membru de a reacționa la acesta. În funcție de cauza și de impactul lor, incidentele de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne. Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune.

(28) Întrucât exploatarea vulnerabilităților din cadrul rețelelor și al sistemelor informatice poate provoca perturbări și prejudicii semnificative, identificarea și remedierea rapidă a acestor vulnerabilități reprezintă un factor important în reducerea riscului de securitate cibernetică. Entitățile care dezvoltă **sau administrează** astfel de sisteme ar trebui, prin urmare, să stabilească proceduri adecvate de gestionare a vulnerabilităților atunci când acestea sunt descoperite. Întrucât vulnerabilitățile sunt adesea descoperite și raportate (divulgate) de părți terțe (entități raportoare), producătorul ori furnizorul de produse sau servicii TIC ar trebui, de asemenea, să instituie procedurile necesare pentru a primi de la terți informații privind vulnerabilitatea. În acest sens, standardele internaționale ISO/IEC 30111 și ISO/IEC [...] **29147** oferă orientări privind gestionarea vulnerabilităților și, respectiv, divulgarea vulnerabilităților. În ceea ce privește divulgarea vulnerabilităților, coordonarea dintre entitățile raportoare și producătorii ori furnizorii de produse sau servicii TIC este deosebit de importantă. Divulgarea coordonată a vulnerabilităților presupune un proces structurat prin care vulnerabilitățile sunt raportate organizațiilor într-un mod care să permită organizației să diagnosticheze și să remedieze vulnerabilitățile înainte ca informațiile detaliate privind vulnerabilitățile să fie divulgate terților sau publicului. Divulgarea coordonată a vulnerabilităților ar trebui să includă, de asemenea, coordonarea dintre entitatea raportoare și organizație în ceea ce privește calendarul de remediere și publicare a vulnerabilităților.

---

[20] Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

(29) Prin urmare, statele membre ar trebui să ia măsuri pentru a facilita divulgarea coordonată a vulnerabilităților prin stabilirea unei politici naționale relevante. **Ca parte a politicii lor naționale, statele membre ar trebui să își propună să abordeze, în măsura posibilului, provocările cu care se confruntă analiștii de vulnerabilități, inclusiv expunerea potențială a acestora la răspunderea penală, în conformitate cu ordinea lor juridică națională.** [...] Statele membre ar trebui să desemneze o echipă CSIRT care să preia rolul de „coordonator”, acționând ca intermediar între entitățile raportoare și producătorii ori furnizorii de produse sau servicii TIC, dacă este necesar. Sarcinile coordonatorului CSIRT ar trebui să includă, în special, identificarea și contactarea entităților vizate, sprijinirea entităților raportoare, negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe organizații (divulgarea **coordonată a** vulnerabilităților mai multor părți). Atunci când vulnerabilitatea **raportată ar putea avea un impact semnificativ asupra entităților** [...] în mai multe state membre, CSIRT desemnate din fiecare dintre statele membre afectate ar trebui să coopereze în cadrul rețelei CSIRT**, dacă este cazul**.

(30) Accesul la informații corecte și în timp util cu privire la vulnerabilitățile care afectează produsele și serviciile TIC contribuie la o mai bună gestionare a riscurilor în materie de securitate cibernetică. În această privință, sursele de informații accesibile publicului cu privire la vulnerabilități reprezintă un instrument important atât pentru entități și utilizatorii acestora, cât și pentru autoritățile naționale competente și CSIRT. Din acest motiv, ENISA ar trebui să creeze un registru al vulnerabilităților în care entitățile esențiale și importante și furnizorii acestora, precum și entitățile care nu intră în domeniul de aplicare al prezentei directive **sau CSIRT desemnate** pot, în mod voluntar, să divulge vulnerabilitățile și să furnizeze informații privind vulnerabilitățile, astfel încât utilizatorii să ia măsuri de atenuare adecvate.

(31) Deși există registre ale vulnerabilităților sau baze de date similare, acestea sunt găzduite și întreținute de entități care nu sunt stabilite în Uniune. Un registru european al vulnerabilităților gestionat de ENISA ar oferi o mai mare transparență în ceea ce privește procesul de publicare înainte de dezvăluirea oficială a vulnerabilității, precum și reziliența în caz de perturbări sau întreruperi ale furnizării de servicii similare. Pentru a evita dublarea eforturilor și pentru a căuta complementaritatea în măsura posibilului, ENISA ar trebui să analizeze posibilitatea de a încheia acorduri de cooperare structurată cu registre similare în jurisdicții din țări terțe. **În special, ENISA ar trebui să analizeze posibilitatea unei cooperări strânse cu operatorii sistemului de vulnerabilități și expuneri comune (Common Vulnerabilities and Exposures – CVE), inclusiv posibilitatea de a deveni o autoritate de numerotare rădăcină a CVE.**

(32) **Grupul de cooperare ar trebui să sprijine și să faciliteze în continuare cooperarea strategică și schimbul de informații, precum și să consolideze încrederea între statele membre.** Grupul de cooperare ar trebui să stabilească, o dată la doi ani, un program de lucru care să includă acțiunile ce urmează să fie întreprinse de grup în vederea punerii în aplicare a obiectivelor și sarcinilor sale. Calendarul primului program adoptat în temeiul prezentei directive ar trebui să fie aliniat la calendarul ultimului program adoptat în temeiul Directivei (UE) 2016/1148, pentru a se evita eventualele perturbări ale activității grupului.

(33) Atunci când elaborează documente de orientare, Grupul de cooperare ar trebui ca, în mod consecvent, să identifice soluțiile și experiențele naționale, să evalueze impactul rezultatelor Grupului de cooperare asupra abordărilor naționale, să discute provocările legate de punerea în aplicare și să formuleze recomandări specifice care să fie abordate printr-o mai bună punere în aplicare a normelor existente.

(34) Grupul de cooperare ar trebui să rămână un forum flexibil, care să poată reacționa la prioritățile și provocările noi și în schimbare în materie de politici, ținând seama, în același timp, de disponibilitatea resurselor. Acesta ar trebui să organizeze reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară grupul și pentru a colecta informații cu privire la provocările emergente în materie de politici. Pentru a consolida cooperarea la nivelul Uniunii, grupul ar trebui să invite să participe la lucrările sale organismele și agențiile Uniunii implicate în politica de securitate cibernetică, cum ar fi Centrul european de combatere a criminalității informatice (EC3), Agenția Uniunii Europene pentru Siguranța Aviației (AESA) și Agenția Uniunii Europene pentru Programul spațial (EUSPA).

(35) Autoritățile competente și CSIRT ar trebui să aibă posibilitatea să participe la programe de schimb pentru funcționari din alte state membre în vederea îmbunătățirii cooperării. Autoritățile competente ar trebui să ia măsurile necesare ca funcționari din alte state membre să poată juca un rol efectiv în activitățile autorității competente gazdă.

(35a) Rețeaua CSIRT ar trebui să contribuie în continuare la consolidarea încrederii și la promovarea unei cooperări operaționale rapide și eficace între statele membre. Pentru a consolida cooperarea operațională la nivelul Uniunii, rețeaua CSIRT ar trebui să aibă în vedere invitarea organismelor și agențiilor Uniunii implicate în politica de securitate cibernetică, cum ar fi Europol, să participe la activitatea sa.

(36) [...]

(36a) Pentru a facilita punerea în aplicare eficace a dispozițiilor prezentei directive, cum ar fi gestionarea vulnerabilităților, gestionarea riscurilor în materie de securitate cibernetică, măsurile de raportare și acordurile privind schimbul de informații, statele membre pot coopera cu țări terțe și pot desfășura activități considerate adecvate acestui scop, inclusiv schimburi de informații cu privire la amenințări, incidente, vulnerabilități, instrumente și metode, tactici, tehnici și proceduri, pregătire și exerciții pentru gestionarea crizelor cibernetice, instruire, consolidarea încrederii și mecanisme structurate de schimb de informații. Astfel de acorduri de cooperare ar trebui să respecte dreptul Uniunii privind protecția datelor.

(37) Statele membre ar trebui să contribuie la instituirea cadrului UE de răspuns la crizele de securitate cibernetică prevăzut în Recomandarea (UE) 2017/1584 prin intermediul rețelelor de cooperare existente, în special prin rețeaua Organizației **europene** de legătură în caz de criză cibernetică (EU-CyCLONe), rețeaua CSIRT și Grupul de cooperare. EU-CyCLONe și rețeaua CSIRT ar trebui să coopereze pe baza modalităților procedurale care definesc modalitățile acestei cooperări **și să evite orice suprapunere a sarcinilor**. Regulamentul de procedură al EU-CyCLONe ar trebui să precizeze în detaliu modalitățile prin care ar trebui să funcționeze rețeaua, inclusiv, dar fără a se limita la acestea, rolurile, modurile de cooperare, interacțiunile cu alți actori relevanți și modelele pentru schimbul de informații, precum și mijloacele de comunicare. Pentru gestionarea crizelor la nivelul **politic al** Uniunii, părțile relevante ar trebui să se bazeze pe mecanismul integrat pentru un răspuns politic la crize (IPCR). În acest scop, Comisia ar trebui să utilizeze procesul ARGUS de coordonare transsectorială la nivel înalt în situații de criză. În cazul în care criza are o importantă dimensiune externă sau de politică de securitate și apărare comună (PSAC), ar trebui activat mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă (SEAE).

(37a) EU-CyCLONe ar trebui să funcționeze ca o rețea intermediară între nivelul tehnic și cel politic în timpul incidentelor și crizelor de securitate cibernetică de mare amploare. Aceasta ar trebui să consolideze cooperarea la nivel operațional, bazându-se pe constatările rețelei CSIRT și utilizând propriile capacități pentru a crea o analiză de impact a incidentelor și crizelor de mare amploare și pentru a sprijini procesul decizional la nivel politic. Instituțiile, organele și agențiile UE ar trebui să desemneze o autoritate competentă responsabilă cu gestionarea incidentelor și crizelor de securitate de mare amploare care să devină membră a EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Responsabilitatea asigurării securității rețelelor și a sistemelor informatice revine în mare măsură entităților esențiale și importante. Ar trebui să se promoveze și să se dezvolte o cultură a gestionării riscurilor, care să implice evaluarea riscurilor și aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate.

(40) Măsurile de gestionare a riscurilor ar trebui **să țină seama de gradul de dependență al entității de rețelele și sistemele informatice și** să includă măsuri de identificare a oricăror riscuri de incidente, de prevenire, detectare și administrare a incidentelor și de diminuare a impactului acestora Securitatea rețelelor și a sistemelor informatice ar trebui să cuprindă securitatea datelor stocate, transmise și prelucrate.

(40a) Întrucât amenințările la adresa securității rețelelor și a sistemelor informatice pot avea origini diferite, prezenta directivă aplică o abordare bazată pe „toate pericolele”, care include protecția rețelelor și a sistemelor informatice și a mediului lor fizic în fața oricărui eveniment, cum ar fi furt, incendiu, inundație, defecțiuni la nivelul telecomunicațiilor sau al alimentării cu energie, sau în cazul oricărui acces fizic neautorizat și al avarierii și intruziunii la nivelul echipamentelor de prelucrare a informațiilor ale entității, care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora. Prin urmare, măsurile de gestionare a riscurilor ar trebui să abordeze, de asemenea, securitatea fizică și a mediului prin includerea unor măsuri de protejare a rețelelor și a sistemelor informatice ale entității împotriva defecțiunilor de sistem, a erorilor umane, a acțiunilor răuvoitoare sau a fenomenelor naturale, în conformitate cu standardele europene sau recunoscute la nivel internațional, cum ar fi cele incluse în seria ISO 27000. În acest sens, entitățile ar trebui, în cadrul măsurilor lor de gestionare a riscurilor, să abordeze și securitatea resurselor umane și să dispună de politici adecvate de control al accesului. Măsurile respective ar trebui să fie coerente cu Directiva XXXX [Directiva CER].

(40b) În absența unor sisteme europene adecvate de certificare de securitate cibernetică adoptate în conformitate cu Regulamentul (UE) 2019/881, statele membre ar putea impune entităților să utilizeze produse, servicii și procese TIC certificate sau să obțină un certificat în cadrul sistemelor naționale de securitate cibernetică disponibile, în scopul respectării cerințelor de gestionare a riscurilor de securitate cibernetică prevăzute în prezenta directivă.

(41) Pentru a se evita impunerea unei sarcini financiare și administrative disproporționate asupra entităților esențiale și importante, cerințele de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri **și de costul implementării lor**. **De asemenea, ar trebui să se țină seama în mod corespunzător de dimensiunea entității, precum și de probabilitatea apariției incidentelor și de gravitatea acestora.**

(41a) În vederea reducerii sarcinilor de reglementare, cerințele pentru punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică pentru entitățile mijlocii, mici sau microentități ar trebui, în principiu, să fie mai puțin stricte, cu excepția cazului în care criteriile de criticitate sau evaluările naționale ale riscurilor ar justifica cerințe mai stricte, îndeosebi în ceea ce privește entitățile care îndeplinesc criteriile legate de criticitate prevăzute în prezenta directivă.

(42) Entitățile esențiale și importante ar trebui să asigure securitatea rețelelor și a sistemelor informatice pe care le utilizează pentru a-și desfășura activitatea. Acestea sunt în principal rețele și sisteme informatice private, gestionarea securității lor fiind efectuată de către personalul IT intern sau externalizată. Cerințele de raportare și de gestionare a riscurilor în materie de securitate cibernetică în temeiul prezentei directive ar trebui să se aplice entităților esențiale și importante relevante, indiferent dacă acestea efectuează la nivel intern întreținerea rețelelor și a sistemelor lor informatice sau dacă le externalizează.

(42aa) Având în vedere caracterul lor transfrontalier, furnizorii de servicii DNS, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de distribuție de conținut, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate ar trebui să facă obiectul unui grad mai ridicat de armonizare la nivelul Uniunii. Prin urmare, implementarea măsurilor de securitate cibernetică ar trebui facilitată printr-un act de punere în aplicare.

(43) Abordarea riscurilor în materie de securitate cibernetică care decurg din lanțul de aprovizionare al unei entități și din relația acesteia cu furnizorii săi este deosebit de importantă, având în vedere prevalența incidentelor în care entitățile au căzut victime atacurilor cibernetice și în care actori răuvoitori au fost în măsură să compromită securitatea rețelelor și a sistemelor informatice ale unei entități prin exploatarea vulnerabilităților care afectează produsele și serviciile părții terțe. Prin urmare, entitățile ar trebui să evalueze și să țină seama de calitatea generală a produselor și de practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor lor de servicii, inclusiv de procedurile lor de dezvoltare sigure.

(44) În rândul furnizorilor de servicii, furnizorii de servicii de securitate administrați (*managed security services providers* – MSSP) în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de important în sprijinirea entităților în eforturile lor de a detecta și de a reacționa la incidente. Totuși, și aceste MSSP-uri au fost ținte ale atacurilor cibernetice și, prin integrarea lor strânsă în operațiunile operatorilor, prezintă un risc deosebit în materie de securitate cibernetică. Prin urmare, entitățile ar trebui să dea dovadă de o diligență sporită în selectarea unui MSSP.

(44a) Autoritățile naționale competente, în contextul sarcinilor lor de supraveghere, pot beneficia, de asemenea, de servicii de securitate cibernetică, cum ar fi audituri de securitate și testarea penetrării sau răspunsul la incidente. Pentru a asista entitățile, precum și autoritățile naționale competente, la selectarea unor furnizori de servicii de securitate cibernetică calificați și de încredere, Comisia, cu sprijinul Grupului de cooperare și al ENISA, ar trebui să aibă în vedere posibilitatea de a solicita sisteme europene de certificare a securității cibernetice, în conformitate cu articolul 48 din Regulamentul (UE) 2019/881.

(45) Entitățile ar trebui, de asemenea, să abordeze riscurile de securitate cibernetică care decurg din interacțiunile și din relațiile lor cu alte părți interesate în cadrul unui ecosistem mai larg. În special, entitățile ar trebui să ia măsurile adecvate pentru a se asigura că activitatea lor de cooperare cu instituțiile academice și de cercetare se desfășoară în conformitate cu politicile lor în materie de securitate cibernetică și respectă bunele practici în ceea ce privește accesul și diseminarea în condiții de siguranță a informațiilor, în general, și protecția proprietății intelectuale, în special. În mod similar, având în vedere importanța și valoarea datelor pentru activitățile pe care le desfășoară entitățile, atunci când se bazează pe servicii de transformare și de analiză a datelor furnizate de terți, entitățile ar trebui să ia toate măsurile care se impun în materie de securitate cibernetică.

(46) Pentru a aborda în continuare principalele riscuri din cadrul lanțului de aprovizionare și pentru a oferi asistență entităților care își desfășoară activitatea în sectoarele reglementate de prezenta directivă în gestionarea adecvată a riscurilor în materie de securitate cibernetică legate de lanțul de aprovizionare și de furnizori, Grupul de cooperare, la care participă autoritățile naționale relevante, ar trebui să efectueze, în cooperare cu Comisia și ENISA, evaluări sectoriale coordonate ale riscurilor la nivelul lanțului de aprovizionare, astfel cum s-a procedat deja în cazul rețelelor 5G ca urmare a Recomandării (UE) 2019/534 privind securitatea cibernetică a rețelelor 5G[21], cu scopul de a identifica, pentru fiecare sector în parte, care sunt serviciile, sistemele sau produsele TIC critice, amenințările și vulnerabilitățile relevante.

[21] Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 Securitatea cibernetică a rețelelor 5G (JO L 88, 29.3.2019, p. 42).

(47) Evaluările riscurilor din cadrul lanțului de aprovizionare, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor, ar trebui să se țină seama de următoarele criterii: (i) în ce măsură entitățile esențiale și importante utilizează și se bazează pe servicii, sisteme sau produse TIC critice specifice; (ii) relevanța serviciilor, a sistemelor sau a produselor TIC critice specifice pentru îndeplinirea funcțiilor critice sau sensibile, printre care se numără și prelucrarea datelor cu caracter personal; (iii) disponibilitatea unor servicii, sisteme sau produse TIC alternative; (iv) reziliența întregului lanț de aprovizionare cu servicii, sisteme sau produse TIC împotriva evenimentelor perturbatoare și (v) pentru serviciile, sistemele sau produsele TIC emergente, potențiala lor importanță pentru activitățile pe care le vor desfășura entitățile în viitor.

(48) Pentru a raționaliza obligațiile juridice impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului și furnizorilor de servicii de asigurare a încrederii în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorităților competente ale acestora să beneficieze de cadrul juridic instituit prin prezenta directivă (inclusiv desemnarea CSIRT responsabile de gestionarea riscurilor și de administrarea incidentelor, participarea autorităților și a organismelor competente la lucrările grupului de cooperare și ale rețelei CSIRT), acestea ar trebui incluse în domeniul de aplicare al prezentei directive. Prin urmare, dispozițiile corespunzătoare prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[22] și în Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului[23] referitoare la impunerea **obligațiilor** de securitate și de notificare pentru aceste tipuri de entități ar trebui abrogate.

---

[22] 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 (JO L 257, 28.8.2014, p. 73).

[23] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

(48a) Obligațiile în materie de securitate prevăzute în prezenta directivă ar trebui considerate complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul Regulamentului (UE) nr. 910/2014 (Regulamentul e-IDAS). Prestatorilor de servicii de încredere ar trebui să li se impună să ia toate măsurile adecvate și proporționale pentru a gestiona riscurile la care sunt expuse serviciile lor, inclusiv în ceea ce privește clienții și beneficiarii terți, și să raporteze incidentele de securitate în temeiul prezentei directive. Aceste obligații în materie de securitate și raportare ar trebui să vizeze, de asemenea, protecția fizică a serviciului prestat. Articolul 24 din Regulamentul (UE) nr. 910/2014 continuă să se aplice.

(48aa) Statele membre pot atribui rolul de autorități competente pentru serviciile de încredere organismelor de supraveghere ale eIDAS, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite odată cu aplicarea Regulamentului eIDAS. În cazul în care rolul respectiv este atribuit unui alt organism, autoritățile naționale competente în temeiul prezentei directive ar trebui să coopereze îndeaproape, în timp util, prin schimburi de informații relevante, pentru a asigura supravegherea eficace și conformitatea prestatorilor de servicii de încredere cu cerințele prevăzute în prezenta directivă și în Regulamentul [XXXX/XXXX].

Dacă este cazul, autoritatea națională competentă în temeiul prezentei directive ar trebui să informeze imediat organismul de supraveghere al eIDAS cu privire la orice amenințare cibernetică semnificativă notificată sau incident cu impact asupra serviciilor de încredere, precum și cu privire la orice nerespectare de către un prestator de servicii de încredere a cerințelor prevăzute în prezenta directivă. În scopul raportării, statele membre pot utiliza, după caz, punctul de intrare unic instituit, pentru a realiza o raportare automată și comună a incidentelor atât către organismul de supraveghere al eIDAS, cât și către autoritatea competentă în temeiul prezentei directive. Normele privind obligațiile de raportare nu ar trebui să aducă atingere nici Regulamentului (UE) 2016/679, nici Directivei 2002/58/CE a Parlamentului European și a Consiliului[24].

[24] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

(49) După caz și pentru a evita perturbările inutile, orientările naționale existente[...] adoptate pentru transpunerea normelor referitoare la măsurile de securitate prevăzute la **articolele** 40[...] și 41 din Directiva (UE) 2018/1972[...] **ar trebui să fie luate în considerare în cadrul măsurilor de transpunere puse în aplicare de statele membre în legătură cu prezenta directivă, valorificând astfel cunoștințele și competențele dobândite în temeiul Directivei (UE) 2018/1972 în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate și notificările incidentelor. De asemenea, ENISA poate elabora orientări privind cerințele de securitate și de raportare pentru furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, pentru a facilita armonizarea și tranziția și pentru a reduce la minimum perturbările. Statele membre pot atribui rolul de autorități competente pentru comunicațiile electronice autorităților de reglementare naționale, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite odată cu aplicarea Directivei (UE) 2018/1972.**

(50) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe numere, este necesar să se asigure că aceste servicii fac, de asemenea, obiectul unor cerințe corespunzătoare în materie de securitate, în conformitate cu natura lor specifică și cu importanța lor economică. Furnizorii unor astfel de servicii ar trebui, prin urmare, să asigure și un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului prezentat. Având în vedere faptul că furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere nu exercită în mod normal un control efectiv asupra transmiterii semnalelor în rețea, gradul de risc aferent unor astfel de servicii poate fi considerat, în unele privințe, mai redus decât în cazul serviciilor tradiționale de comunicații electronice. Același lucru este valabil și pentru serviciile de comunicații interpersonale care utilizează numere și care nu exercită un control efectiv asupra transmiterii semnalului.

(51) Piața internă depinde mai mult decât oricând de funcționarea internetului. Aproape toate serviciile entităților esențiale și importante depind de serviciile furnizate pe internet. Pentru a asigura furnizarea fără probleme a serviciilor asigurate de entități esențiale și importante, este important ca rețelele publice de comunicații electronice, cum ar fi, de exemplu, magistralele de internet sau cablurile de comunicații submarine, să dispună de măsuri adecvate în materie de securitate cibernetică și să raporteze incidentele legate de aceasta.

(52) După caz, entitățile ar trebui să își informeze destinatarii serviciilor cu privire la [...] măsurile specifice pe care le pot lua pentru a atenua riscurile pentru ei înșiși **asociate unei amenințări cibernetice semnificative**. **Entitățile ar trebui, atunci când este cazul și mai ales în situațiile în care amenințarea cibernetică semnificativă se poate materializa, să notifice, de asemenea, amenințarea în sine și destinatarilor serviciilor lor, în paralel cu notificarea acesteia autorităților competente sau echipelor CSIRT.** Cerința de a informa destinatarii cu privire la astfel de amenințări nu ar trebui să scutească entitățile de obligația de a lua, pe cheltuiala proprie, măsuri adecvate și imediate pentru a preveni sau remedia orice amenințare cibernetică și pentru a restabili nivelul normal de securitate al serviciului. Furnizarea unor astfel de informații privind amenințările [...] **cibernetice** destinatarilor ar trebui să fie gratuită.

(53) În special, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui să îi informeze pe destinatarii serviciilor cu privire la amenințările cibernetice specifice și semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare.

(54) Pentru a se garanta securitatea rețelelor și a serviciilor de comunicații electronice, ar trebui promovată utilizarea criptării, în special a criptării de la un capăt la altul și, dacă este necesar, acest tip de criptare ar trebui să fie obligatoriu pentru furnizorii de astfel de servicii și rețele, în conformitate cu principiile securității și protecției vieții private în mod implicit și începând cu momentul conceperii, în sensul articolului 18. Utilizarea criptării de la un capăt la altul ar trebui să fie reconciliată cu competențele statelor membre de a asigura protecția intereselor lor esențiale în materie de securitate și de siguranță publică și de a permite investigarea, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii. Soluțiile pentru accesul legal la informații în comunicațiile criptate de la un capăt la altul ar trebui să mențină eficacitatea criptării în ceea ce privește protecția vieții private și securitatea comunicațiilor, oferind, în același timp, un răspuns eficace la criminalitate.

(55) Prezenta directivă stabilește o abordare în două etape a raportării incidentelor pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor și le permite entităților să solicite sprijin și, pe de altă parte, raportarea aprofundată, care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența întreprinderilor individuale și a unor sectoare întregi la amenințările cibernetice. Atunci când entitățile descoperă că a aut loc un incident, acestea ar trebui să aibă obligația de a transmite o notificare inițială în termen de 24 de ore, urmată de un raport final în termen de cel mult o lună de la incidentul respectiv. Notificarea inițială ar trebui să includă numai informațiile strict necesare pentru a informa autoritățile competente cu privire la incident și pentru a putea solicita asistență, dacă este necesar. O astfel de notificare, după caz, ar trebui să indice dacă incidentul pare să fie cauzat de acțiuni ilegale sau răuvoitoare. Statele membre ar trebui să se asigure că cerința de transmitere a acestei notificări inițiale nu deviază resursele entității raportoare de la activitățile legate de administrarea incidentelor care ar trebui să aibă prioritate. Pentru a preveni și mai mult situațiile în care obligațiile de raportare a incidentelor fie deviază resursele de la gestionarea răspunsului la incidente, fie compromit eforturile depuse de entități în acest sens, statele membre ar trebui să prevadă, de asemenea, că, în cazuri justificate în mod corespunzător și cu acordul autorităților competente sau al CSIRT, entitatea în cauză se poate abate de la termenul de 24 de ore pentru notificarea inițială și de o lună pentru raportul final.

(55a) O abordare proactivă a amenințărilor cibernetice este o componentă vitală a gestionării riscurilor în materie de securitate cibernetică, care ar trebui să permită autorităților competente să prevină în mod eficace materializarea amenințărilor cibernetice în incidente reale care pot cauza pierderi materiale sau nemateriale considerabile. În acest scop, notificarea amenințărilor cibernetice semnificative prezintă o importanță majoră.

(56) Entitățile esențiale și importante se află adesea într-o situație în care, din cauza caracteristicilor sale, un anumit incident trebuie raportat mai multor autorități ca urmare a obligațiilor de notificare incluse în diferite instrumente juridice. Astfel de cazuri creează sarcini suplimentare și pot conduce, de asemenea, la incertitudini în ceea ce privește formatul unor asemenea notificări și procedurile aferente acestora. Având în vedere cele de mai sus și în scopul simplificării raportării incidentelor de securitate, statele membre ar [...] **putea** să instituie *un punct de intrare unic* pentru toate notificările efectuate în temeiul prezentei directive și, de asemenea, în temeiul altor acte legislative ale Uniunii, cum ar fi Regulamentul (UE) 2016/679 și Directiva 2002/58/CE. ENISA, în cooperare cu Grupul de cooperare, ar trebui să instituie modele comune de notificare prin intermediul unor orientări care să simplifice și să raționalizeze informațiile de raportare solicitate de dreptul Uniunii și să reducă sarcinile impuse întreprinderilor.

(57) Atunci când există suspiciuni că un incident ar fi legat de activități infracționale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze entitățile esențiale și importante, pe baza normelor aplicabile în materie de proceduri penale în conformitate cu dreptul Uniunii, să raporteze autorităților de aplicare a legii incidentele despre care există suspiciuni că ar avea un caracter infracțional grav. După caz și fără a aduce atingere normelor de protecție a datelor cu caracter personal aplicabile Europol, este de dorit ca procesul de coordonare dintre autoritățile competente și autoritățile de aplicare a legii din diferite state membre să fie facilitată de EC3 și de ENISA.

(58) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile de protecție a datelor și cu autoritățile de supraveghere, în temeiul Directivei 2002/58/CE.

(59) Menținerea unor baze de date exacte și complete conținând numele de domenii și datele de înregistrare (așa-numitele „date WHOIS”) și furnizarea unui acces legal la astfel de date sunt aspecte esențiale pentru a asigura securitatea, stabilitatea și reziliența DNS, sistem care, la rândul său, contribuie la un nivel comun ridicat de securitate cibernetică în Uniune. Atunci când prelucrarea include date cu caracter personal, această prelucrare respectă legislația Uniunii în materie de protecție a datelor.

(60) Disponibilitatea și accesibilitatea în timp util a acestor date pentru autoritățile publice, inclusiv pentru autoritățile competente în temeiul dreptului Uniunii sau al dreptului intern pentru prevenirea, investigarea sau urmărirea penală a infracțiunilor, CERT, [...]CSIRT și, în ceea ce privește datele clienților lor, pentru furnizorii de rețele și servicii de comunicații electronice și pentru furnizorii de tehnologii și servicii de securitate cibernetică care acționează în numele clienților respectivi, sunt aspecte esențiale pentru prevenirea și combaterea abuzurilor din sistemul de nume de domenii, în special pentru prevenirea, detectarea și combaterea incidentelor de securitate cibernetică. Acest tip de acces ar trebui să respecte legislația Uniunii în materie de protecție a datelor în măsura în care este legat de date cu caracter personal.

(61) Pentru a asigura disponibilitatea unor date exacte și complete de înregistrare a numelor de domeniu, registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD (operatorii de registru) ar trebui să colecteze și să garanteze integritatea și disponibilitatea datelor de înregistrare a numelor de domenii. **În ceea ce privește datele de înregistrare, entitățile ar trebui să verifice în special numele și adresa de e-mail ale solicitantului înregistrării.** [...] Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui să stabilească politici și proceduri pentru colectarea și păstrarea unor date de înregistrare exacte și complete, precum și pentru prevenirea și corectarea datelor de înregistrare inexacte, în conformitate cu normele Uniunii privind protecția datelor.

(62) Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului date de înregistrare a numelor de domenii care nu intră în domeniul de aplicare al normelor Uniunii privind protecția datelor, cum ar fi datele care se referă la persoanele juridice[25]. Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui, de asemenea, să le permită solicitanților legitimi de acces, în conformitate cu legislația Uniunii privind protecția datelor, accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să se asigure că registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii răspund fără întârzieri nejustificate solicitărilor de divulgare a datelor de înregistrare a numelor de domenii formulate de solicitanții legitimi de acces**, cum ar fi autoritățile competente în temeiul dreptului Uniunii sau al dreptului intern în domeniul securității naționale și al justiției penale, sau CSIRT**. Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Procedura de acces poate include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. **Statele membre ar trebui să se asigure că orice tip de acces la datele de înregistrare a domeniilor (atât datele cu caracter personal, cât și datele fără caracter personal) este gratuit.** În vederea promovării unor practici armonizate pe piața internă, Comisia poate adopta orientări cu privire la aceste proceduri fără a aduce atingere competențelor Comitetului european pentru protecția datelor**, în conformitate cu standardele internaționale elaborate de comunitatea multipartită și complementare acestora**.

---

25 Considerentul 14 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului, care prevede: „Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.”

(63) [...] Entitățile esențiale și importante vizate de prezenta directivă ar trebui considerate ca fiind sub jurisdicția statului membru în care își prestează serviciile. **Entitățile menționate la punctele 1-7 și 10 din anexa I, prestatorii de servicii de încredere și furnizorii de internet exchange point menționați la punctul 8 din anexa I și la punctele 1-5 din anexa II la prezenta directivă ar trebui să intre sub jurisdicția statului membru în care au sediul.** În cazul în care entitatea furnizează servicii **sau are sediu** în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre aceste state membre. Autoritățile competente din aceste state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere. **În cazul în care statele membre decid să își exercite competența, acestea ar trebui să evite sancționarea aceluiași comportament de mai multe ori pentru încălcarea obligațiilor prevăzute în prezenta directivă.**

(64) Pentru a ține seama de caracterul transfrontalier al serviciilor și al operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, **ale entităților care furnizează servicii de înregistrare a numelor de domenii pentru TLD,** ale furnizorilor de rețele de distribuție de conținut, ale furnizorilor de servicii de cloud computing, ale furnizorilor de servicii de centre de date și ale furnizorilor digitali, un singur stat membru ar trebui să aibă jurisdicție asupra acestor entități. Competența ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

Respectarea acestui criteriu nu ar trebui să depindă de situarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui să fie locul în care sunt luate **în mod predominant** deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Aceasta va corespunde, de regulă, locului în care se află administrația centrală a întreprinderilor din Uniune. În cazul în care **nu poate fi stabilit locul în care astfel de decizii sunt luate în mod predominant sau dacă** astfel de decizii nu sunt luate în Uniune, se consideră că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. În cazul în care serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

(64a) În cazul în care un serviciu DNS recurent este furnizat de un furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului numai ca parte a serviciului de acces la internet, entitatea ar trebui să fie considerată a se afla sub jurisdicția tuturor statelor membre în care sunt furnizate serviciile sale.

(64aa) Pentru a asigura o imagine de ansamblu clară a furnizorilor de servicii DNS, a registrelor de nume TLD, a entităților care furnizează servicii de înregistrare a numelor de domenii pentru TLD, a furnizorilor de rețele de distribuție de conținut, a furnizorilor de servicii de cloud computing, a furnizorilor de servicii de centre de date și a furnizorilor de servicii digitale din întreaga Uniune care intră în domeniul de aplicare al prezentei directive, ENISA ar trebui să creeze și să mențină un registru pentru astfel de entități, pe baza notificărilor primite de statele membre, dacă este cazul, prin intermediul mecanismelor lor naționale de autonotificare. Pentru a asigura acuratețea și exhaustivitatea informațiilor care ar trebui incluse în acest registru, statele membre ar trebui să transmită către ENISA informațiile disponibile în registrele lor naționale cu privire la aceste entități. ENISA și statele membre ar trebui să ia măsuri pentru a facilita interoperabilitatea acestor registre, asigurând, în același timp, protecția informațiilor confidențiale sau clasificate.

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

(66) În cazul în care se face schimb de informații considerate clasificate în conformitate cu legislația națională sau a Uniunii ori astfel de informații sunt raportate sau partajate în alt mod în temeiul dispozițiilor prezentei directive, ar trebui să se aplice normele specifice corespunzătoare privind tratarea informațiilor clasificate.

(67) Amenințările cibernetice devenind tot mai complexe și mai sofisticate, eficacitatea măsurilor de detectare și prevenire depinde în mare măsură de schimbul regulat de informații privind amenințările și vulnerabilitățile care are loc între entități. Schimbul de informații contribuie la creșterea gradului de sensibilizare cu privire la amenințările cibernetice, ceea ce, la rândul său, consolidează capacitatea entităților de a preveni materializarea amenințărilor în incidente reale și le permite entităților să controleze mai bine efectele incidentelor și să se redreseze mai eficient. În absența unor orientări la nivelul Uniunii, mai mulți factori par să fi împiedicat un astfel de schimb de informații, în special incertitudinea cu privire la compatibilitatea cu normele în materie de concurență și răspundere.

(68) Entitățile ar trebui încurajate să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, pentru a-și consolida capacitățile de evaluare și de monitorizare a amenințărilor cibernetice, de apărare împotriva acestora și de răspuns în mod adecvat la asemenea amenințări. Prin urmare, este necesar să se permită apariția, la nivelul Uniunii, a unor mecanisme de schimb voluntar de informații. În acest scop, statele membre ar trebui să sprijine și să încurajeze în mod activ și entitățile relevante care nu intră în domeniul de aplicare al prezentei directive să participe la astfel de mecanisme de schimb de informații. Mecanismele respective ar trebui să se desfășoare în deplină conformitate cu normele Uniunii în materie de concurență, precum și cu normele Uniunii în materie de protecție a datelor.

(69) [...] În măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, **prelucrarea datelor cu caracter personal**de către entitățile **esențiale și importante** [...] și de către furnizorii de tehnologii și servicii de securitate **ar putea fi considerată necesară pentru respectarea unei obligații legale sau ar putea**[...] constitui un interes legitim al operatorului de date în cauză**[...]**, astfel cum se menționează în Regulamentul (UE) 2016/679. Aceasta ar putea [...] să includă măsuri legate de prevenirea, detectarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate, precum și schimbul voluntar de informații cu privire la incidentele respective, [...] la amenințările și vulnerabilitățile cibernetice, la indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare. Astfel de măsuri pot necesita prelucrarea [...] **a diferite** tipuri de date cu caracter personal**, cum ar fi**: adrese IP, localizatoare uniforme de resurse (URL), nume de domenii și adrese de e-mail. **Prelucrarea datelor cu caracter personal de către autorități competente, SPOC și CSIRT ar trebui să fie prevăzută în dreptul intern și considerată necesară pentru respectarea unei obligații legale sau pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul de date, astfel cum se menționează la articolul 6 alineatul (1) literele (c) sau (e) din Regulamentul (UE) 2016/679.**

(69a) Legislațiile statelor membre pot stabili norme care să permită autorităților competente, SPOC și CSIRT, în măsura în care acest lucru este strict necesar și proporțional cu scopul asigurării securității rețelelor și a sistemelor informatice ale entităților esențiale și importante, să prelucreze categorii speciale de date cu caracter personal în conformitate cu articolul 9 [...] din Regulamentul (UE) 2016/679, în special prin prevederea unor măsuri adecvate și specifice care să protejeze drepturile și interesele fundamentale ale persoanelor fizice, inclusiv limitări tehnice privind reutilizarea unor astfel de date și aplicarea unor măsuri de securitate și de păstrare a confidențialității de ultimă generație, cum ar fi pseudonimizarea sau criptarea, atunci când anonimizarea poate afecta semnificativ scopul urmărit.

(70) Pentru a consolida competențele și acțiunile de supraveghere care contribuie la asigurarea respectării efective, prezenta directivă ar trebui să prevadă o listă minimă de acțiuni și mijloace de supraveghere prin care autoritățile competente să poată supraveghea entitățile esențiale și importante. În plus, prezenta directivă ar trebui să stabilească o diferențiere între regimul de supraveghere al entităților esențiale și cel al entităților importante, în vederea asigurării unui echilibru echitabil al obligațiilor atât pentru entități, cât și pentru autoritățile competente. Astfel, entitățile esențiale ar trebui să facă obiectul unui regim de supraveghere complet (*ex ante* și *ex post*), în timp ce entitățile importante ar trebui să facă obiectul unui regim de supraveghere moderat, doar *ex post*. Pentru cele din urmă, acest lucru înseamnă că entitățile importante nu ar trebui să **fie obligate să** documenteze în mod sistematic respectarea cerințelor de gestionare a riscurilor în materie de securitate cibernetică, în timp ce autoritățile competente ar trebui să pună în aplicare o abordare reactivă *ex post* a supravegherii și, prin urmare, să nu aibă o obligație generală de a supraveghea entitățile respective. **În cazul entităților importante, supravegherea *ex post* poate fi declanșată de dovezi sau de orice indicație sau informație adusă la cunoștința autorităților competente despre care aceste autorități consideră că sugerează o potențială nerespectare a obligațiilor prevăzute în prezenta directivă. De exemplu, astfel de dovezi, indicații sau informații ar putea fi de tipul celor furnizate autorităților competente de către alte autorități, entități, de cetățeni, de mass-media sau de alte surse, informații aflate la dispoziția publicului, sau pot rezulta din alte activități desfășurate de autoritățile competente în îndeplinirea sarcinilor lor.**

(70a) În exercitarea supravegherii *ex ante*, autoritățile competente ar trebui să fie în măsură să decidă cu privire la ierarhizarea importanței utilizării acțiunilor și mijloacelor de supraveghere de care dispun, în mod proporțional. Acest lucru implică faptul că autoritățile competente pot decide cu privire la o astfel de ierarhizare a priorităților pe baza metodologiilor de supraveghere care ar trebui să urmeze o abordare bazată pe riscuri. Mai precis, astfel de metodologii ar putea include criterii sau valori de referință pentru clasificarea entităților esențiale în categorii de risc, alături de acțiuni de supraveghere corespunzătoare și mijloace recomandate pentru fiecare categorie de risc, cum ar fi utilizarea, frecvența sau tipul inspecțiilor la fața locului sau al auditurilor de securitate specifice sau al scanărilor de securitate, tipul de informații care trebuie solicitate și nivelul de detaliere al informațiilor respective. Astfel de metodologii de supraveghere pot fi, de asemenea, însoțite de programe de lucru și pot fi evaluate și revizuite periodic, inclusiv cu privire la aspecte precum alocarea resurselor și nevoile.

(70bisa) În ceea ce privește entitățile administrației publice, competențele de supraveghere ar trebui exercitate în conformitate cu cadrele naționale și cu ordinea juridică. Statele membre ar trebui să poată decide impunerea unor măsuri adecvate, proporționale și eficace de supraveghere și de asigurare a respectării legii în ceea ce privește aceste entități.

(70bisaa) Pentru a demonstra conformitatea cu anumite măsuri de gestionare a riscurilor în materie de securitate cibernetică, statele membre ar putea solicita entităților esențiale și importante să utilizeze servicii de încredere calificate sau sisteme de identificare electronică notificate în temeiul Regulamentului (UE) nr. 910/2014.

(71) Pentru ca asigurarea respectării să fie eficace, ar trebui stabilită o listă minimă de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscurilor de securitate cibernetică și de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru astfel de sancțiuni în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de natura, gravitatea și durata încălcării, de daunele reale cauzate sau de pierderile suferite ori de daunele sau pierderile potențiale care ar fi putut fi declanșate, de caracterul intenționat sau din neglijență al încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul și/sau pierderile suferite, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv al unei protecții judiciare eficiente și al unui proces echitabil.

(71a) Dispozițiile referitoare la răspunderea persoanelor fizice care au anumite responsabilități în cadrul unei entități pentru încălcarea obligației lor de a asigura respectarea obligațiilor prevăzute în prezenta directivă nu impun statelor membre să asigure urmărirea penală sau răspunderea civilă pentru prejudiciile cauzate terților prin astfel de încălcări.

(72) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezenta directivă, fiecare autoritate competentă ar trebui să aibă competența de a impune sau de a solicita impunerea de amenzi administrative.

(73) În cazul în care amenzile administrative sunt impuse unei întreprinderi, acest termen ar trebui înțeles ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative nu afectează exercitarea altor competențe de către autoritățile competente sau aplicarea altor sancțiuni prevăzute în normele naționale de transpunere a prezentei directive.

(74) Statele membre [...] **pot** stabili norme privind sancțiunile penale pentru încălcarea normelor naționale de transpunere a prezentei directive. Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale acestor norme de drept intern și de sancțiuni administrative conexe nu ar trebui să ducă la încălcarea principiului *ne bis in idem*, astfel cum a fost interpretat de Curtea de Justiție.

(75) În cazul în care prezenta directivă nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale obligațiilor prevăzute în prezenta directivă, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni eficace, proporționale și disuasive. Natura unor astfel de sancțiuni, penale sau administrative, ar trebui stabilită în legislația statelor membre.

(76) Pentru a consolida și mai mult eficacitatea și caracterul disuasiv al sancțiunilor aplicabile în cazul încălcării obligațiilor prevăzute în temeiul prezentei directive, autoritățile competente ar trebui să fie împuternicite să aplice sancțiuni constând în suspendarea unei certificări sau a unei autorizații privind o parte din serviciile furnizate de o entitate esențială sau toate aceste servicii și impunerea unei interdicții temporare de a exercita funcții de conducere de către o persoană fizică. Având în vedere gravitatea și impactul lor asupra activităților entităților și, în cele din urmă, asupra consumatorilor acestora, aceste sancțiuni ar trebui aplicate numai proporțional cu gravitatea încălcării și ținând seama de circumstanțele specifice fiecărui caz, inclusiv de caracterul intenționat sau din neglijență al încălcării, de măsurile luate pentru a preveni sau a atenua prejudiciul și/sau de pierderile suferite. Astfel de sancțiuni ar trebui aplicate doar în ultimă instanță, adică numai după ce celelalte măsuri relevante de asigurare a respectării legislației prevăzute de prezenta directivă au fost epuizate și numai până în momentul în care entitățile cărora li se aplică iau măsurile necesare pentru a remedia deficiențele sau pentru a se conforma cerințelor autorității competente pentru care au fost aplicate aceste sancțiuni. Impunerea unor astfel de sancțiuni face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv protecția jurisdicțională efectivă, respectarea garanțiilor procedurale, prezumția de nevinovăție și dreptul la apărare.

(76a) Pentru a asigura eficacitatea supravegherii și a asigurării respectării legii, îndeosebi în cazurile cu o dimensiune transfrontalieră, statele membre care au primit o cerere de asistență reciprocă ar trebui, în măsura în care li s-a cerut acest lucru, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în ceea ce privește entitatea în cauză care furnizează servicii sau care deține rețeaua și sistemul informatic pe teritoriul lor.

(77) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente și autoritățile de supraveghere în conformitate cu Regulamentul (UE) 2016/679 pentru tratarea cazurilor de încălcare a normelor în materie de date cu caracter personal.

(78) Prezenta directivă ar trebui să vizeze asigurarea unui nivel ridicat de responsabilitate pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare la nivelul organizațiilor. Din aceste motive, organele de conducere ale entităților care intră în domeniul de aplicare al prezentei directive ar trebui să aprobe măsurile privind riscurile la adresa securității cibernetice și să supravegheze punerea lor în aplicare.

(79) Ar trebui introdus un [...] **sistem** de [...] **învățare *inter pares* pentru a contribui la consolidarea** încrederii **reciproce și la învățarea din bunele practici și experiențe**, care să permită [...] **schimburi reciproce între** experții desemnați de statele membre **cu privire la**[...] punerea în aplicare a politicilor în materie de securitate cibernetică[...]. **La implementarea sistemului de învățare *inter pares*, ar trebui să se acorde o atenție deosebită asigurării faptului că acesta nu creează sarcini inutile sau disproporționate pentru autoritățile relevante ale statelor membre. Comisia ar trebui să exploreze toate posibilitățile de a garanta, în mod potențial, acoperirea financiară a costurilor care ar putea rezulta din organizarea de misiuni de învățare *inter pares*. În plus, sistemul de învățare *inter pares* ar trebui să țină seama de rezultatele unor mecanisme similare, cum ar fi sistemul de evaluare *inter pares* al rețelei CSIRT, să aducă valoare adăugată și să evite suprapunerile. Implementarea sistemului de învățare *inter pares* nu ar trebui să aducă atingere dreptului intern sau dreptului Uniunii privind protecția informațiilor confidențiale și clasificate. Înainte de începerea rundelor de învățare *inter pares*, statele membre pot efectua o autoevaluare a aspectelor relevante. La cererea grupului de cooperare, ENISA poate oferi orientări privind autoevaluarea și modele relevante, dacă este necesar. Statele membre ar putea decide să își pună rapoartele respective la dispoziția publicului.**

(80) [...]

(81) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a dispozițiilor relevante ale prezentei directive în ceea ce privește dispozițiile procedurale necesare pentru funcționarea grupului de cooperare, elementele tehnice legate de măsurile de gestionare a riscurilor sau tipul de informații, formatul și procedura de notificare a incidentelor, **categoriile de entități care sunt obligate să utilizeze anumite produse, servicii și procese TIC certificate**, Comisiei ar trebui să i se confere competențe de executare. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[26].

(82) Comisia ar trebui să revizuiască periodic prezenta directivă, consultându-se cu părțile interesate, în special pentru a stabili dacă este necesară efectuarea unor modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață.

[26] Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

(83) Întrucât obiectivul prezentei directive, și anume obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, nu poate fi suficient realizat de către statele membre ci, datorită efectelor acțiunii, poate fi realizat mai bine la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității stabilit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

(84) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiect

(1) Prezenta directivă stabilește măsuri în vederea asigurării unui nivel comun ridicat de securitate cibernetică în Uniune**, astfel încât să se îmbunătățească funcționarea pieței interne**.

(2) În acest scop, prezenta directivă:

(a) stabilește obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică, de a desemna autorități naționale competente, puncte unice de contact și echipe de intervenție în caz de incidente de securitate informatică (CSIRT);

(b) stabilește obligațiile de gestionare și de raportare a riscurilor în materie de securitate cibernetică pentru entitățile de tipul celor menționate [...] în **anexele I și II**[...];

(c) stabilește **norme și** obligații privind schimbul de informații în materie de securitate cibernetică.

Articolul 2

Domeniul de aplicare

(1) Prezenta directivă se aplică entităților publice și private de tipul celor **enumerate**[...] în [...] **anexele I și II** [...] **care ating sau depășesc plafoanele pentru întreprinderile mijlocii** [...] în sensul Recomandării 2003/361/CE a Comisiei[27]. **Articolul 3 alineatul (4) și articolul 6 alineatul (2) al doilea și al treilea paragraf din anexa la recomandarea respectivă nu se aplică în sensul prezentei directive.**

(2) [...] Indiferent de dimensiunea [...] **entităților menționate la alineatul (1)**, prezenta directivă se aplică, de asemenea, în cazul în care: [...]

(a) serviciile sunt furnizate de una dintre următoarele entități:

(i) **furnizorii de** rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, menționate la punctul 8 din anexa I;

(ii) **prestatorii de servicii de încredere calificați menționați la punctul XX din anexa I;**

(iii) **prestatorii de servicii de încredere necalificați menționați la punctul XX din anexa I;**

(iv) registrele de nume de domenii de prim nivel [...] menționate la punctul 8 din anexa I;

(b) [...]

---

27 Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

(c) entitatea este singurul furnizor **dintr-un stat membru** al unui serviciu [...] **care este esențial pentru susținerea unor activități societale și economice critice**;

(d) o eventuală perturbare a serviciului furnizat de entitate ar putea avea un impact **semnificativ** asupra siguranței publice, a securității publice sau a sănătății publice;

(e) o eventuală perturbare a serviciului furnizat de entitate ar putea genera riscuri sistemice **semnificative**, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

(f) [...];

(g) entitatea este identificată ca fiind o entitate critică în temeiul Directivei (UE) XXXX/XXXX a Parlamentului European și a Consiliului[28] [Directiva privind reziliența entităților critice] **[**sau o entitate echivalentă cu o entitate critică în temeiul articolului 7 din directiva respectivă**]**.

(2a) **Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților administrației publice din administrația centrală recunoscute ca atare într-un stat membru în conformitate cu dreptul intern și menționate la punctul 9 din anexa I. Statele membre pot stabili că prezenta directivă se aplică și entităților administrației publice de la nivel regional și local.**

28 [a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]

(3) [...]

Prezenta directivă nu aduce atingere responsabilităților statelor membre de a proteja securitatea națională sau competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.

(3a) (1) Prezenta directivă nu se aplică:

(a) entităților care nu intră în domeniul de aplicare al dreptului Uniunii și, în orice caz, niciuneia dintre entitățile care desfășoară în principal activități în domeniul apărării, securității naționale, siguranței publice sau al asigurării respectării legii, indiferent de entitatea care desfășoară aceste activități și indiferent dacă este o entitate publică sau o entitate privată, fără a se aduce atingere punctului (2);

(b) entităților care desfășoară activități în domeniul judiciar, al parlamentelor și al băncilor centrale.[...]

(2) În cazul în care entitățile administrației publice desfășoară activități în aceste domenii numai ca parte a activităților lor generale, ele sunt excluse în totalitate din domeniul de aplicare al prezentei directive.

(3aa) Prezenta directivă nu se aplică:

(i) activităților entităților care nu intră în domeniul de aplicare al dreptului Uniunii și, în orice caz, niciuneia dintre activitățile din domeniile securității naționale sau apărării, indiferent de entitatea care desfășoară aceste activități și indiferent dacă este o entitate publică sau o entitate privată;

(ii) activităților entităților din sistemul judiciar, parlamentelor, băncilor centrale și din domeniul securității publice, inclusiv ale entităților administrației publice care desfășoară activități de asigurare a respectării legii în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor.

(3aaa) Obligațiile prevăzute în prezenta directivă nu implică furnizarea de informații a căror divulgare contravine intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(**3aaaa) Prezenta directivă nu aduce atingere dreptului Uniunii privind protecția datelor cu caracter personal, în special Regulamentului (UE) 2016/679 și Directivei 2002/58/CE.**

(3b) Prezenta directivă nu se aplică entităților care sunt exceptate de la aplicarea Regulamentului (UE) XXXX/XXXX al Parlamentului European și al Consiliului [Regulamentul DORA] în conformitate cu articolul 2 alineatul (4) din Regulamentul DORA.

(4) Prezenta directivă se aplică fără a aduce atingere [...][29] Directivelor 2011/93/UE[30] și 2013/40/UE[31] ale Parlamentului European și ale Consiliului.

(5) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii și cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante **conform prezentei directive** numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante și proporționale cu scopul urmărit. Schimbul de informații păstrează confidențialitatea informațiilor respective și protejează securitatea și interesele comerciale ale entităților esențiale sau importante.

---

29 [...]

30 Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

31 Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

Articolul 2a

Entități esențiale și importante

(1) Dintre entitățile cărora li se aplică prezenta directivă, următoarele entități sunt considerate esențiale:

(i) entitățile de tipul celor prevăzute la punctele 1-8a și 10 din anexa I la prezenta directivă care depășesc plafoanele pentru întreprinderile mijlocii, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei;

(ii) entitățile mijlocii menționate la articolul 2 alineatul (2) litera (a) punctul (i);

(iii) entitățile menționate la articolul 2 alineatul (2) litera (a) punctele (ii) și (iv) din prezenta directivă, indiferent de dimensiune;

(iv) entitățile menționate la articolul 2 alineatul (2) litera (g) și la articolul 2 alineatul (2a) din prezenta directivă, indiferent de dimensiune;

(v) în cazul în care sunt înființate de statele membre, entitățile pe care statele membre le-au identificat înainte de intrarea în vigoare a prezentei directive ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 sau cu dreptul intern;

(vi) entitățile care depășesc plafoanele pentru întreprinderile mijlocii, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei, de tipul prevăzut în anexa II, pe care statele membre le clasifică drept esențiale pe baza criteriilor menționate la articolul 2 alineatul (2) literele (c)-(e);

(vii) entitățile mijlocii în sensul Recomandării 2003/361/CE a Comisiei, pe care statele membre le clasifică drept esențiale pe baza criteriilor menționate la articolul 2 alineatul (2) literele (c)-(e);

(viii) microentitățile sau entitățile mici în sensul Recomandării 2003/361/CE a Comisiei, menționate la alineatul (2) litera (a) punctul (i) sau identificate în temeiul alineatului (2) literele (c)-(e) din prezentul articol, pe care statele membre le clasifică drept esențiale pe baza evaluărilor naționale ale riscurilor.

(2) Dintre entitățile cărora li se aplică prezenta directivă, următoarele entități sunt considerate importante:

(i) entitățile de tipul celor prevăzute în anexa I la prezenta directivă care se califică drept întreprinderi mijlocii în sensul Recomandării 2003/361/CE a Comisiei și entitățile de tipul celor prevăzute în anexa II care ating sau depășesc plafoanele pentru întreprinderile mijlocii în sensul Recomandării 2003/361/CE a Comisiei[32];

(ii) entitățile menționate la articolul 2 alineatul (2) punctul (iii) din prezenta directivă, indiferent de dimensiune;

(iii) entitățile mici și microentitățile menționate la articolul 2 alineatul (2) litera (a) punctul (i);

(iv) entitățile mici și microentitățile pe care statele membre le clasifică drept entități importante în temeiul articolului 2 alineatul (2) literele (c)-(e).

---

32 **Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntrerinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).**

Articolul 2a

Mecanisme de notificare

(1) **Statele membre pot institui un mecanism național de autonotificare care să impună tuturor entităților care fac obiectul prezentei directive să transmită cel puțin numele, adresa și datele lor de contact, precum și sectorul în care își desfășoară activitatea sau tipul de serviciu pe care îl furnizează și, după caz, lista statelor membre în care entitățile furnizează serviciile vizate de prezenta directivă autorităților competente în temeiul prezentei directive sau organismelor desemnate în acest scop de către statele membre.**

(2) Statele membre [...] transmit Comisiei**, în legătură cu entitățile pe care le-au identificat în temeiul articolului 2 alineatul (2) literele (b)-(e), cel puțin informațiile relevante privind numărul entităților identificate, sectorul din care fac parte sau tipul de servicii pe care le furnizează conform anexelor, precum și dispoziția (dispozițiile) specifică (specifice) de la articolul 2 alineatul (2) pe baza cărora au fost identificate, până la [12 luni de la termenul de transpunere a prezentei directive].** Statele membre revizuiesc [...] **aceste informații** în mod periodic și, ulterior, cel puțin o dată la doi ani și, dacă este cazul, [...] le actualizează.

Articolul 2b

Acte sectoriale ale Uniunii

(1) În cazul în care [...] actele **juridice sectoriale ale Uniunii** impun entităților esențiale sau importante [...] să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele sau amenințările cibernetice **semnificative**, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta directivă, dispozițiile relevante ale prezentei directive, **inclusiv dispozițiile privind supravegherea și asigurarea respectării legii prevăzute în capitolul VI,** nu se aplică **acestor entități**. **În cazul în care actele juridice sectoriale ale Uniunii nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive se aplică în continuare entităților care nu fac obiectul dispozițiilor sectoriale respective.**

(2) Cerințele menționate la alineatul (1) de la prezentul articol sunt considerate ca având un efect echivalent cu obligațiile prevăzute în prezenta directivă dacă actul sectorial respectiv al Uniunii prevede că autoritățile competente în temeiul prezentei directive sau echipele CSIRT desemnate au un acces imediat, după caz automat și direct, la notificările incidentelor și dacă:

(a) măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente ca efect cu cele prevăzute la articolul 18 alineatele (1) și (2) din prezenta directivă; sau

(b) cerințele de notificare a incidentelor semnificative au efecte cel puțin echivalente cu cele prevăzute la articolul 20 alineatele (1)-(6).

(3) Comisia revizuiește periodic aplicarea cerințelor privind efectul echivalent prevăzute la alineatele (1) și (2) de la prezentul articol în legătură cu dispozițiile sectoriale ale actelor juridice ale Uniunii. Comisia consultă grupul de cooperare și ENISA atunci când pregătește aceste revizuiri periodice.

Articolul 3

Armonizarea minimă

Fără a aduce atingere celorlalte obligații care le revin în temeiul dreptului Uniunii, statele membre pot [...] să adopte sau să mențină dispoziții care să asigure un nivel mai ridicat de securitate cibernetică **în domeniile vizate de prezenta directivă**.

Articolul 4

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

1. „rețea și sistem informatic” înseamnă:

   (a) o rețea de comunicații electronice în sensul articolului 2 punctul 1 din Directiva (UE) 2018/1972;

   (b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale;

   (c) datele digitale stocate, prelucrate, recuperate sau transmise de elemente reglementate în temeiul literelor (a) și (b) în vederea funcționării, utilizării, protejării și întreținerii lor;

2. „securitatea rețelelor și a sistemelor informatice” înseamnă capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, **oricărui eveniment** care **poate** compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor **[...]** oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

2a. „servicii de comunicații electronice” înseamnă servicii de comunicații [...] electronice în sensul articolului 2 punctul 4 din Directiva (UE) 2018/1972;

3. „securitate cibernetică” înseamnă securitate cibernetică în sensul articolului 2 punctul 1 din Regulamentul (UE) nr. 2019/881 al Parlamentului European și al Consiliului[33];

4. „strategie națională **de securitate cibernetică**” înseamnă un cadru coerent al unui stat membru care prevede o guvernanță pentru realizarea de obiective și priorități strategice [...] **în domeniul** securității cibernetice [...] în statul membru respectiv;

5. „incident” înseamnă orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor [...] oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

5a. „incident de securitate cibernetică de mare amploare” înseamnă un incident care are un impact semnificativ asupra a cel puțin două state membre sau care provoacă o perturbare ce depășește capacitatea unui stat membru de a reacționa la acesta.

---

33 Regulamentul (UE) nr. 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

6. „administrarea incidentelor” înseamnă toate acțiunile și procedurile care vizează detectarea, analizarea și limitarea unui incident, precum și răspunsul la acesta;

6a. „risc” înseamnă potențialele pierderi sau perturbări cauzate de un incident și este exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului respectiv.

7. „amenințare cibernetică” înseamnă amenințare cibernetică în sensul articolului 2 punctul 8 din Regulamentul (UE) 2019/881;

7**a** **„amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei entități sau ale utilizatorilor acesteia, cauzând pierderi materiale sau nemateriale considerabile;**

8. „vulnerabilitate” înseamnă un punct slab, o susceptibilitate sau o deficiență a unui activ TIC sau a unui sistem [...] care poate fi exploatată de o amenințare cibernetică;

8a. „incident evitat la limită” înseamnă un eveniment care ar fi putut cauza prejudicii rețelei și sistemelor informatice ale unei entități sau ale utilizatorilor acesteia, dar a cărui desfășurare până la capăt a fost împiedicată cu succes;

9. „reprezentant” înseamnă orice persoană fizică sau juridică stabilită în Uniune care este desemnată în mod explicit să acționeze în numele i) unui furnizor de servicii DNS, al unui registru de nume de domenii de prim nivel (TLD), al unui furnizor de servicii de cloud computing, al unui furnizor de servicii de centre de date, al unui furnizor de rețele de furnizare de conținut, astfel cum se menționează la punctul 8 din anexa I sau ii) al entităților menționate la punctul [...] **6** din anexa II care nu sunt stabilite în Uniune, căreia i se poate adresa o autoritate națională competentă sau o CSIRT în locul entității în ceea ce privește obligațiile entității respective în temeiul prezentei directive;

10. „standard” înseamnă un standard în sensul articolului 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[34];

11. „specificație tehnică” înseamnă o specificație tehnică în sensul articolului 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

12. „internet exchange point (IXP)” înseamnă o structură de rețea care permite interconectarea a mai mult de două rețele independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet; un IXP furnizează interconectare doar pentru sisteme autonome; un IXP nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre o pereche oarecare de sisteme autonome participante și nici nu modifică sau afectează într-un alt mod acest trafic;

13. „sistem de nume de domenii (DNS)” înseamnă un sistem ierarhic și distribuit de atribuire de nume care le permite utilizatorilor finali să acceseze servicii și resurse pe internet;

14. „furnizor de servicii DNS” înseamnă o entitate care furnizează servicii de rezolvare a numelor de domenii recursive sau cu autoritate **pentru** [...] **a fi utilizate de către terți, cu excepția serverelor de nume rădăcină** [...];

---

34 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 (JO L 316, 14.11.2012, p. 12).

15. „registru de nume de domenii de prim nivel” înseamnă o entitate căreia i s-a delegat un anumit domeniu de prim nivel (*top–level domain* –TLD) și care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului și cu exploatarea tehnică a TLD-ului, în special cu exploatarea serverelor sale de nume, cu întreținerea bazelor sale de date și cu distribuirea fișierelor zonale TLD între serverele de nume**, excluzând în același timp situațiile în care numele de domenii de prim nivel sunt utilizate de un registru exclusiv pentru uz propriu**;

15a. „entități care furnizează servicii de înregistrare a numelor de domenii pentru TLD” înseamnă registre de nume TLD, operatori de registru pentru TLD și agenți ai operatorilor de registru, cum ar fi revânzătorii și furnizorii de servicii de proxy;

16. „serviciu digital” înseamnă un serviciu în sensul articolului 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului[35];

16a. „servicii de încredere” înseamnă servicii de încredere în sensul articolului 3 punctul 16 din Regulamentul (UE) nr. 910/2014;

[35] Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

16b. „prestator de servicii de încredere calificat” înseamnă un prestator de servicii de încredere calificat în sensul articolului 3 punctul 20 din Regulamentul (UE) nr. 910/2014;

17. „piață online” înseamnă un serviciu digital în sensul articolului 2 litera (n) din Directiva 2005/29/CE a Parlamentului European și a Consiliului[36];

18. „motor de căutare online” înseamnă un serviciu digital în sensul articolului 2 alineatul (5) din Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului[37];

19. „serviciu de cloud computing” înseamnă un serviciu digital care permite administrarea la cerere și accesul amplu la distanță la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun și distribuite**, inclusiv atunci când acestea sunt distribuite în mai multe locuri**;

20. „serviciu de centre de date” înseamnă un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului;

---

36 Directiva 2005/29/CE a Parlamentului European și a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori și de modificare a Directivei 84/450/CEE a Consiliului, a Directivelor 97/7/CE, 98/27/CE și 2002/65/CE ale Parlamentului European și ale Consiliului și a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului („Directiva privind practicile comerciale neloiale”) (JO L 149, 11.6.2005, p. 22).

37 Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului din 20 iunie 2019 privind promovarea echității și a transparenței pentru întreprinderile utilizatoare de servicii de intermediere online (JO L 186, 11.7.2019, p. 57).

21. „rețea de furnizare de conținut” înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;

22. „platformă de servicii de socializare în rețea” înseamnă o platformă care le permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul mai multor dispozitive, în special prin chat, postări, materiale video și recomandări[...];

23. „entitate a administrației publice” înseamnă o entitate, **recunoscută ca atare într-un stat membru în conformitate cu dreptul intern**, [...] care îndeplinește următoarele criterii:

    (a) a fost înființată în scopul satisfacerii unor nevoi de interes general și nu are caracter industrial sau comercial;

    (b) are personalitate juridică **sau este abilitată prin lege să acționeze în numele unei alte entități cu personalitate juridică**;

    (c) este finanțată, în cea mai mare parte, de stat, de autoritatea regională sau de alte organisme de drept public; sau face obiectul unui control de gestiune din partea autorităților sau a organismelor respective; sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de stat, de autoritățile regionale sau de alte organisme de drept public;

    (d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor.

24. „entitate” înseamnă orice persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;

25. „entitate esențială” înseamnă orice entitate de un tip [...] **prevăzut în anexa I și desemnată ca fiind „esențială” în conformitate cu articolul 2a alineatul (1)**;

26. „entitate importantă” înseamnă orice entitate de un tip [...] **prevăzut în anexele I și II și desemnată ca fiind „importantă” în conformitate cu articolul 2a alineatul (2);**

26a. „produs TIC” înseamnă un produs TIC în sensul articolului 2 punctul 12 din Regulamentul (UE) 2019/881;

26aa. „serviciu TIC” înseamnă un serviciu TIC în sensul articolului 2 punctul 13 din Regulamentul (UE) 2019/881;

26ab. „proces TIC” înseamnă un proces TIC în sensul articolului 2 punctul 14 din Regulamentul (UE) 2019/881;

26ac. „furnizor de servicii gestionate” înseamnă orice entitate care furnizează servicii, cum ar fi rețea, aplicație, infrastructură și securitate, prin gestionare permanentă și periodică, sprijin și administrare activă la sediile clienților, în centrul de date al propriului lor MSP (găzduire) sau într-un centru de date terț;

26ad. „furnizor de servicii de securitate gestionate” înseamnă orice entitate care furnizează monitorizarea și gestionarea externalizate ale dispozitivelor și sistemelor de securitate. Printre serviciile obișnuite se numără serviciile gestionate de „firewall”, de detectare a intruziunilor, rețelele private virtuale, serviciile de scanare a vulnerabilităților și serviciile antivirale.

Sunt incluse, de asemenea, utilizarea centrelor operaționale de securitate de mare disponibilitate (fie din propriile lor instalații, fie de la alți furnizori de centre de date) pentru a furniza servicii în regim 24/7 menite să reducă personalul operațional de securitate pe care o întreprindere trebuie să îl angajeze, să îl formeze și să îl păstreze pentru a menține o situație de securitate acceptabilă.

CAPITOLUL II

Cadre de reglementare coordonate în materie de securitate cibernetică

Articolul 5

Strategia națională de securitate cibernetică

(1) Fiecare stat membru adoptă o strategie națională de securitate cibernetică care definește obiectivele strategice și măsurile de politică și de reglementare adecvate, în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică include, în special, următoarele elemente:

(a) [...] obiectivele și prioritățile strategiei statului membru privind securitatea cibernetică;

(b) un cadru de guvernanță pentru realizarea acestor obiective și priorități, inclusiv politicile menționate la alineatul (2) și rolurile și responsabilitățile diferitelor autorități și ale diferiților actori care participă la punerea în aplicare a strategiei [...];

(c) [...] **orientări** menite să identifice activele și **să evalueze** riscurile în materie de securitate cibernetică relevante din statul membru respectiv[...];

(d) o identificare a măsurilor de asigurare a pregătirii pentru incidente, a răspunsului la acestea și a redresării în urma acestora, inclusiv cooperarea dintre sectorul public și cel privat;

(e) [...]

(f) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei directive și al Directivei (UE) XXXX/XXXX a Parlamentului European și a Consiliului[38] [Directiva privind reziliența entităților critice] în scopul schimbului de informații privind **riscurile în materie de securitate cibernetică**, [...] amenințările și incidentele cibernetice, **precum și riscurile, amenințările și incidentele de altă natură decât cibernetică,** și al exercitării sarcinilor de supraveghere**, după caz**;

(fa) un cadru de politică pentru coordonarea și cooperarea dintre autoritățile competente în temeiul prezentei directive și autoritățile competente desemnate în temeiul legislației sectoriale.

(2) În cadrul strategiei naționale de securitate cibernetică, statele membre adoptă în special următoarele politici:

(a) o politică ce abordează securitatea cibernetică în lanțul de aprovizionare pentru produsele și serviciile TIC utilizate de entități [...] pentru furnizarea serviciilor lor;

(b) **o politică**[...] privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele și serviciile TIC în cadrul achizițiilor publice**, inclusiv certificarea securității cibernetice**;

(c) o politică **privind gestionarea vulnerabilităților, care să cuprindă promovarea și facilitarea** [...] divulgării coordonate **voluntare** a vulnerabilităților în sensul articolului 6 **alineatul (1)**;

(d) o politică legată de menținerea disponibilității, [...] a integrității **și a confidențialității** generale a nucleului public al internetului deschis;

(e) o politică de promovare și dezvoltare a inițiativelor privind competențele, **educația și formarea,** sensibilizarea și cercetarea și dezvoltarea în materie de securitate cibernetică;

---

38 *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]*

(f) o politică de sprijinire a instituțiilor academice și de cercetare în vederea dezvoltării unor instrumente de securitate cibernetică și a unei infrastructuri de rețea securizate;

(g) o politică, proceduri relevante și instrumente adecvate de schimb de informații care să sprijine schimbul voluntar de informații în materie de securitate cibernetică între întreprinderi, în conformitate cu dreptul Uniunii;

(h) o politică care răspunde nevoilor specifice ale IMM-urilor, în special ale celor excluse din domeniul de aplicare al prezentei directive, în ceea ce privește orientările și sprijinul pentru îmbunătățirea rezilienței acestora la amenințările [...]cibernetice.

(3) Statele membre notifică Comisiei strategiile lor naționale de securitate cibernetică în termen de trei luni de la adoptarea acestora. **În cadrul acestui proces,** statele membre pot exclude **elemente ale strategiei care au legătură cu** [...] securitatea națională.

(4) Statele membre își evaluează periodic strategiile naționale de securitate cibernetică cel puțin o dată la [...] **cinci** ani pe baza indicatorilor-cheie de performanță și, dacă este necesar, le modifică. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sprijină statele membre, la cererea **acestora**, în elaborarea unei strategii naționale și a unor indicatori-cheie de performanță pentru evaluarea strategiei.

Articolul 6

Divulgarea coordonată a vulnerabilităților și registrul european al vulnerabilităților

(1) Fiecare stat membru desemnează una dintre echipele sale CSIRT, astfel cum se menționează la articolul 9, drept coordonator în scopul divulgării coordonate a vulnerabilităților. CSIRT desemnată acționează ca intermediar de încredere, facilitând, dacă este necesar, interacțiunea dintre entitatea raportoare**, potențialul proprietar al vulnerabilității** și producătorul sau furnizorul de produse TIC sau servicii TIC. **Orice persoană fizică sau juridică poate raporta către echipa CSIRT desemnată, eventual în mod anonim, o vulnerabilitate menționată la articolul 4 alineatul (8). CSIRT desemnată asigură o monitorizare atentă a raportării și confidențialitatea identității persoanei care raportează vulnerabilitatea.** În cazul în care vulnerabilitatea raportată [...] **ar putea avea un impact semnificativ asupra entităților în mai multe state membre**, CSIRT desemnată din fiecare stat membru în cauză**, dacă este cazul,** cooperează cu **alte CSIRT desemnate din cadrul** rețelei CSIRT.

(2) ENISA creează și menține un registru european al vulnerabilităților**, în consultare cu Grupul de cooperare**. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate, în special pentru a permite entităților importante și esențiale și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze **în mod voluntar** vulnerabilitățile **cunoscute public** prezente în produsele TIC sau serviciile TIC, precum și să ofere acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în registru. Registrul include, în special, informații care descriu vulnerabilitatea, produsul TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată, disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări **emise de autoritățile naționale competente sau de CSIRT** adresate utilizatorilor de produse și servicii vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate. **ENISA se asigură că registrul european al vulnerabilităților utilizează o infrastructură de comunicații și informații sigură și rezilientă.**

Articolul 7

Cadrele naționale de gestionare a crizelor în materie de securitate cibernetică

(1) Fiecare stat membru desemnează una sau mai multe autorități competente responsabile cu gestionarea incidentelor și a crizelor **de securitate cibernetică** de mare amploare. Statele membre se asigură că autoritățile competente dispun de resurse adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le-au fost încredințate. **Statele membre asigură coerența cu cadrele existente pentru gestionarea generală a crizelor.**

(2) Fiecare stat membru identifică capacitățile, mijloacele și procedurile care pot fi utilizate în caz de criză în sensul prezentei directive.

(3) Fiecare stat membru adoptă un plan național de răspuns la incidente și crize de securitate cibernetică în care sunt stabilite obiective și modalități de gestionare a incidentelor și a crizelor de securitate cibernetică de mare amploare. Planul stabilește, în special, următoarele:

(a) obiectivele măsurilor și ale activităților naționale de pregătire;

(b) sarcinile și responsabilitățile autorităților naționale competente;

(c) procedurile de gestionare a crizelor**, inclusiv integrarea acestora în cadrul național general de gestionare a crizelor** și canalele de schimb de informații;

(d) măsurile de pregătire, inclusiv exerciții și activități de formare periodice;

(e) părțile [...] relevante din sectorul public și privat și infrastructura implicată;

(f) procedurile și mecanismele naționale dintre autoritățile și organismele naționale relevante menite să asigure participarea efectivă a statului membru la gestionarea coordonată a incidentelor și a crizelor de securitate cibernetică de mare amploare la nivelul Uniunii și sprijinul acordat de acesta.

(4) Statele membre [...] **informează** Comisia **cu privire la** desemnarea autorităților lor competente menționate la alineatul (1) și transmit **informațiile relevante referitoare la cerințele prevăzute la alineatul (3) de la prezentul articol cu privire la** planurile naționale de răspuns la incidente și crize în materie de securitate cibernetică [...] în termen de trei luni de la desemnarea autorităților și adoptarea planurilor respective. Statele membre pot exclude [...] anumite informații în cazul și în măsura în care acest lucru este [...] necesar pentru securitatea lor națională**, siguranța publică sau apărare**.

Articolul 8

Autoritățile naționale competente și punctele unice de contact

(1) Fiecare stat membru desemnează una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VI din prezenta directivă. Statele membre pot desemna în acest scop o autoritate existentă sau autorități existente.

(2) Autoritățile competente menționate la alineatul (1) monitorizează aplicarea prezentei directive la nivel național.

(3) Fiecare stat membru desemnează un punct unic de contact național în materie de securitate cibernetică („punct unic de contact”). În cazul în care un stat membru desemnează o singură autoritate competentă, aceasta servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.

(4) Fiecare punct unic de contact exercită o funcție de legătură menită să asigure cooperarea transfrontalieră a autorităților din statul său membru cu autoritățile relevante din alte state membre și să asigure cooperarea transsectorială cu alte autorități naționale competente din statul său membru.

(5) Statele membre se asigură că autoritățile competente menționate la alineatul (1) și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod eficace și eficient sarcinile care le-au fost atribuite și a realiza astfel obiectivele prezentei directive. Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților desemnați în grupul de cooperare menționat la articolul 12.

(6) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei desemnarea autorității competente menționate la alineatul (1) și a punctului unic de contact menționat la alineatul (3), sarcinile acestora și orice modificare ulterioară a acestora. Fiecare stat membru face publică desemnarea lor. Comisia publică lista punctelor unice de contact desemnate.

Articolul 9

Echipele de intervenție în caz de incidente de securitate informatică („echipe CSIRT")

(1) Fiecare stat membru desemnează una sau mai multe echipe CSIRT care respectă cerințele stabilite la articolul 10 alineatul (1) și care acoperă cel puțin sectoarele, subsectoarele sau entitățile menționate în anexele I și II; acestea sunt responsabile de administrarea incidentelor în conformitate cu o procedură bine definită. O echipă CSIRT poate fi înființată în cadrul unei autorități competente menționate la articolul 8.

(2) Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-și îndeplini efectiv sarcinile stabilite la articolul 10 alineatul (2). **Atunci când îndeplinesc aceste sarcini, CSIRT pot acorda prioritate furnizării anumitor servicii către entități conform unei abordări bazate pe riscuri.**

(3) Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și rezilientă pentru a face schimb de informații cu entitățile esențiale și importante și cu alte părți interesate relevante. În acest scop, statele membre se asigură că echipele CSIRT contribuie la implementarea unor instrumente securizate de schimb de informații.

(4) Echipele CSIRT cooperează și, după caz, fac schimb de informații relevante în conformitate cu articolul 26 cu comunități sectoriale sau transsectoriale de încredere formate din entități esențiale și importante.

(5) Echipele CSIRT participă la [...] **sesiunile de învățare** *inter pares* organizate în conformitate cu articolul 16.

(6) Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT menționate la articolul 13.

(7) Statele membre comunică fără întârzieri nejustificate Comisiei echipele CSIRT desemnate în conformitate cu alineatul (1), coordonatorul CSIRT desemnat în conformitate cu articolul 6 alineatul (1) și sarcinile acestora prevăzute în legătură cu entitățile menționate în anexele I și II.

(8) Statele membre pot solicita asistența ENISA pentru instituirea echipelor CSIRT naționale.

Articolul 10

Cerințe și sarcini pentru echipele CSIRT

(1) Echipele CSIRT respectă următoarele cerințe:

(a) echipele CSIRT asigură o disponibilitate ridicată a [...] **canalelor** lor de comunicare evitând punctele unice de defecțiune și dispun de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment. Echipele CSIRT specifică în mod clar canalele de comunicare și le aduc la cunoștința utilizatorilor și a partenerilor de cooperare;

(b) localurile echipelor CSIRT și sistemele informatice de suport sunt situate pe amplasamente securizate;

(c) echipele CSIRT dispun de un sistem adecvat de gestionare și rutare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;

(d) echipele CSIRT dispun de personal adecvat pentru a asigura o disponibilitate permanentă;

(e) echipele CSIRT sunt echipate cu sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor;

(f) echipele CSIRT au posibilitatea de a participa la rețele internaționale de cooperare.

(2) Echipelor CSIRT le revin următoarele sarcini:

(a) monitorizarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național;

(b) asigurarea unor mecanisme de avertizare timpurie, alerte, anunțuri și diseminare de informații către entitățile esențiale și importante, precum și către **autoritățile competente și** alte părți interesate relevante cu privire la amenințările cibernetice, vulnerabilități și incidente;

(c) răspunsul la incidente;

(d) colectarea și analizarea datelor criminalistice și furnizarea de analize dinamice de risc și de incident și conștientizarea situației în materie de securitate cibernetică;

(e) furnizarea **[...]** unei scanări proactive a rețelei și a sistemelor informatice [...] **pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, cu condițiaca, în cazul în care nu există consimțământul entității respective, rețeaua și sistemele informatice să nu fie perturbate și funcționarea lor să nu fie afectată în mod negativ;**

(f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă **în funcție de capacitățile și competențele lor** altor membri ai rețelei, la cererea acestora.

(fa) după caz, asumarea rolului de coordonator în scopul procesului coordonat de divulgare a vulnerabilităților în temeiul articolului 6 alineatul (1), care include, în special, facilitarea interacțiunii dintre entitățile raportoare, proprietarul vulnerabilității potențiale și producătorul sau furnizorul de produse TIC sau de servicii TIC în cazurile în care acest lucru este necesar, identificarea și contactarea entităților vizate, sprijinirea entităților raportoare, negocierea termenelor pentru divulgarea informațiilor și gestionarea vulnerabilităților care afectează mai multe organizații (divulgarea coordonată multipartită a vulnerabilităților).

(3) Echipele CSIRT stabilesc relații de cooperare cu actorii relevanți din sectorul privat, în vederea unei mai bune îndepliniri a obiectivelor directivei.

(3a) Echipele CSIRT pot stabili relații de cooperare cu echipe CSIRT naționale din țări terțe. În cadrul acestei cooperări, ale pot face schimb de informații relevante, inclusiv de date cu caracter personal, în conformitate cu dreptul Uniunii privind protecția datelor.

(4) Pentru a facilita cooperarea, echipele CSIRT promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu următoarele:

(a) procedurile de administrare a incidentelor;

(b) gestionarea crizelor în materie de securitate cibernetică;

(c) divulgarea coordonată a vulnerabilităților.

Articolul 11

Cooperarea la nivel național

(1) Atunci când sunt separate, autoritățile competente menționate la articolul 8, punctul unic de contact și echipele (echipa) CSIRT ale aceluiași stat membru cooperează între ele pentru îndeplinirea obligațiilor ce le revin în temeiul prezentei directive.

(2) Statele membre se asigură că fie autoritățile lor competente, fie echipele lor CSIRT primesc notificări privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită comunicate în temeiul prezentei directive. În cazul în care un stat membru decide ca echipele sale CSIRT să nu primească notificări, acestora li se acordă, în măsura necesară pentru a-și îndeplini atribuțiile, acces la datele privind incidentele notificate de entitățile esențiale sau importante, în temeiul articolului 20.

(3) Fiecare stat membru se asigură că autoritățile sale competente sau echipele sale CSIRT informează punctul său unic de contact cu privire la notificările privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită comunicate în temeiul prezentei directive.

(4) În măsura în care este necesar pentru a îndeplini în mod eficace sarcinile și obligațiile prevăzute în prezenta directivă, statele membre asigură o cooperare adecvată între autoritățile competente**, CSIRT**, punctele unice de contact și autoritățile de aplicare a legii, autoritățile pentru protecția datelor și autoritățile **competente desemnate** [...] în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice[...]], **autoritățile competente în temeiul Regulamentului de punere în aplicare 2019/1583 al Comisiei, autoritățile naționale de reglementare desemnate în conformitate cu Directiva (UE) 2018/1972, autoritățile naționale desemnate în temeiul articolului 17 din Regulamentul (UE) nr. 910/2014,** [...] autoritățile financiare naționale desemnate în conformitate cu Regulamentul (UE) XXXX/XXXX al Parlamentului European și al Consiliului [Regulamentul DORA]**, precum și autoritățile competente desemnate în baza altor acte juridice sectoriale ale Uniunii** din statul membru respectiv.

(5) Statele membre se asigură că autoritățile lor competente **în temeiul prezentei directive și autoritățile competente desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] fac schimburi** periodice **de** informații [...] cu privire la **identificarea entităților critice,** riscurile de securitate cibernetică, amenințările și incidentele **cibernetice, precum și cu privire la riscurile, amenințările și incidentele de altă natură decât cibernetică** ce afectează entitățile esențiale identificate ca fiind critice **[**sau ca fiind entități echivalente cu entitățile critice,**]** în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice], precum și cu privire la măsurile luate [...] ca răspuns la aceste riscuri și incidente. **De asemenea, statele membre se asigură că autoritățile competente în temeiul prezentei directive** [...] **și autoritățile competente desemnate în temeiul Regulamentului XXXX/XXXX [Regulamentul DORA], al Directivei 2018/1972 și al Regulamentului (UE) 910/2014 efectuează schimburi periodice de informații relevante.**

În ceea ce privește prestatorii de servicii de încredere și [...] în special, [...] în cazurile în care rolul de supraveghere în temeiul prezentei directive este atribuit unui alt organism decât organismele de supraveghere desemnate în temeiul Regulamentului (UE) nr. 910/2014, autoritățile naționale competente în temeiul prezentei directive cooperează îndeaproape, în timp util, prin schimburi de informații relevante, pentru a asigura supravegherea eficace și conformitatea prestatorilor de servicii de încredere cu cerințele prevăzute în prezenta directivă și în Regulamentul [XXXX/XXXX] **și, după caz, autoritatea națională competentă în temeiul prezentei directive informează fără întârzieri nejustificate organismul de supraveghere al eIDAS cu privire la orice incident sau amenințare cibernetică semnificativă notificată cu impact asupra serviciilor de încredere.**

(5a) În scopul [...] simplificării raportării incidentelor, statele membre pot să instituie un punct de intrare unic pentru toate notificările impuse în temeiul prezentei directive, precum și în temeiul Regulamentului (UE) 2016/679 și al Directivei 2002/58/CE, după caz. Statele membre pot utiliza punctul de intrare unic pentru notificările impuse în temeiul altor acte juridice sectoriale ale Uniunii. Acest punct de intrare unic nu aduce atingere aplicării dispozițiilor Regulamentului (UE) 2016/679 și ale Directivei 2002/58/CE, în special a celor referitoare la autoritățile de supraveghere independente.

CAPITOLUL III

*Cooperarea **în UE***

Articolul 12

Grupul de cooperare

(1) Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații între statele membre [...] **și pentru a consolida încrederea**, se instituie un grup de cooperare.

(2) Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (6).

(3) Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) **și autoritățile competente desemnate în temeiul** Regulamentului (UE) XXXX/XXXX [Regulamentul DORA] [...] pot participa la activitățile grupului de cooperare **în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) XXXX/XXXX [Regulamentul DORA].**

După caz, grupul de cooperare poate invita să participe la lucrările sale reprezentanți ai părților interesate relevante.

Comisia asigură secretariatul.

(4) Grupului de cooperare îi revin următoarele sarcini:

(a) furnizarea de orientări autorităților competente în legătură cu transpunerea și punerea în aplicare a prezentei directive**;**

(aa) furnizarea de orientări în legătură cu elaborarea și punerea în aplicare a politicilor privind divulgarea coordonată a vulnerabilităților, astfel cum se menționează la articolul 5 alineatul (2) litera (c) și la articolul 6 alineatul (1);

(b) schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentei directive, inclusiv în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, incidentele evitate la limită, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, precum și standardele și specificațiile tehnice;

(c) schimbul de opinii și cooperarea cu Comisia cu privire la inițiativele emergente de politică în materie de securitate cibernetică;

(d) schimbul de opinii și cooperarea cu Comisia cu privire la proiectele de acte de punere în aplicare [...] ale Comisiei adoptate în temeiul prezentei directive;

(e) schimbul de bune practici și de informații cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii;

(ea) schimbul de opinii cu privire la punerea în aplicare a legislației sectoriale pentru aspecte legate de securitatea cibernetică;

(f) discutarea rapoartelor privind [...] **învățarea** *inter pares* menționată la articolul 16 alineatul (7);

(g) discutarea [...] **experiențelor asociate** activităților de supraveghere comună în cazurile transfrontaliere, astfel cum se menționează la articolul 34;

(h) furnizarea de orientări strategice rețelei CSIRT **și UE-CyCLONe** cu privire la aspecte emergente specifice;

(ha) schimbul de opinii cu privire la monitorizarea politicilor în cazul incidentelor de securitate cibernetică de mare amploare, pe baza lecțiilor învățate din rețeaua CSIRT și UE-CyCLONe;

(i) contribuția la capacitățile în materie de securitate cibernetică în întreaga Uniune prin facilitarea schimbului de funcționari naționali prin intermediul unui program de consolidare a capacităților care implică personal din cadrul autorităților competente ale statelor membre sau al CSIRT;

(j) organizarea de reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară grupul și pentru a colecta informații cu privire la noile dificultăți în materie de politici;

(k) discutarea activității desfășurate în legătură cu exercițiile de securitate cibernetică, inclusiv a activității desfășurate de ENISA**;**

(ka) instituirea mecanismului de învățare *inter pares* în conformitate cu articolul 16 din prezenta directivă.

(5) Grupul de cooperare poate solicita rețelei CSIRT un raport tehnic pe anumite teme.

(6) Până la ... [24 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, o dată la doi ani, grupul de cooperare stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și a sarcinilor sale. Calendarul primului program adoptat în temeiul prezentei directive este aliniat la calendarul ultimului program adoptat în temeiul Directivei (UE) 2016/1148.

(7) Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea grupului de cooperare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2).

(8) Grupul de cooperare se reunește periodic și cel puțin o dată pe an cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] pentru a promova cooperarea strategică și **a facilita** schimbul de informații.

Articolul 13

Rețeaua CSIRT

(1) Pentru a contribui la dezvoltarea încrederii și pentru a promova cooperarea operațională rapidă și eficace între statele membre, se stabilește o rețea a echipelor CSIRT naționale.

(2) Rețeaua CSIRT este formată din reprezentanți ai echipelor CSIRT ale statelor membre **desemnate în conformitate cu articolul 9** și ai CERT-UE. Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și sprijină activ cooperarea între echipele CSIRT.

(3) Rețelei CSIRT îi revin următoarele sarcini:

(a) schimbul de informații privind capacitățile CSIRT;

(b) schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile;

(ba) schimbul de informații în ceea ce privește publicațiile și recomandările în materie de securitate cibernetică;

(bb) schimbul de soluții tehnice care să faciliteze gestionarea tehnică a incidentelor;

(bc) schimbul de bune practici, de instrumente și de procese în ceea ce privește sarcinile echipelor CSIRT;

(c) la cererea unui [...] **membru** al rețelei CSIRT care ar putea fi afectat de un incident, schimbul de informații și discutarea informațiilor cu privire la incidentul respectiv și la amenințările cibernetice, riscurile și vulnerabilitățile conexe;

(d) la cererea unui [...] **membru** al rețelei CSIRT, discutarea și, după caz, punerea în aplicare a unui răspuns coordonat la un incident care a fost identificat în jurisdicția statului membru respectiv;

(e) furnizarea de sprijin statelor membre în abordarea incidentelor transfrontaliere în temeiul prezentei directive;

(f) cooperarea**, schimbul de bune practici** și furnizarea de asistență echipelor CSIRT desemnate menționate la articolul 6 în ceea ce privește gestionarea divulgării coordonate multipartite a vulnerabilităților care afectează mai mulți producători sau furnizori de produse TIC, servicii TIC și procese TIC stabiliți în diferite state membre;

(g) discutarea și identificarea de noi forme de cooperare operațională, inclusiv în legătură cu:

(i) categoriile de amenințări cibernetice și incidente;

(ii) alertele timpurii;

(iii) asistența reciprocă;

(iv) principiile și modalitățile de coordonare, ca răspuns la riscuri și incidente transfrontaliere;

(v) contribuția la planul național de răspuns la incidente și crize de securitate cibernetică menționat la articolul 7 alineatul (3)**, la solicitarea unui stat membru**;

(h) informarea grupului de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în temeiul literei (g) **și,** după caz, solicitarea de orientări în acest sens;

(i) bilanțul exercițiilor de securitate cibernetică, inclusiv al celor organizate de ENISA;

(j) la cererea unei anumite echipe CSIRT, analizarea capacităților și a nivelului de pregătire al echipei CSIRT respective;

(k) cooperarea și schimbul de informații cu centrele de operațiuni de securitate la nivel regional și la nivelul Uniunii pentru a îmbunătăți conștientizarea comună a situației cu privire la incidentele și amenințările din întreaga Uniune;

(l) discutarea rapoartelor privind [...] **învățarea** *inter pares* menționate la articolul 16 alineatul (7);

(m) emiterea de orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentului articol referitoare la cooperarea operațională.

(4) În scopul revizuirii menționate la articolul 35 și în termen de [24 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, la fiecare doi ani, rețeaua CSIRT evaluează progresele înregistrate în ceea ce privește cooperarea operațională și întocmește un raport. Raportul formulează, în special, concluzii cu privire la rezultatele [...] **învățării** *inter pares*menționate la articolul 16, efectuate în legătură cu echipele CSIRT naționale, inclusiv concluzii și recomandări, în temeiul articolului respectiv. Raportul se transmite, de asemenea, grupului de cooperare.

(5) Rețeaua CSIRT își adoptă propriul regulament de procedură.

(6) Rețeaua CSIRT cooperează cu UE-CyCLONe pe baza modalităților procedurale convenite.

Articolul 14

Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (UE - CyCLONe)

(1) Pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor și a crizelor de securitate cibernetică de mare amploare și pentru a asigura schimbul periodic de informații între statele membre și instituțiile, organele și agențiile Uniunii, se înființează Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (UE - CyCLONe).

(2) UE-CyCLONe este formată din reprezentanți ai autorităților de gestionare a crizelor **cibernetice** din statele membre desemnați în conformitate cu articolul 7[...]. **Comisia participă la activitățile rețelei în calitate de observator.** ENISA asigură secretariatul rețelei și sprijină schimbul securizat de informații**; de asemenea, furnizează instrumentele necesare pentru sprijinirea cooperării dintre statele membre, asigurând schimbul securizat de informații.**

După caz, UE-CyCLONe poate invita să participe la lucrările sale reprezentanți ai părților interesate relevante.

(3) UE - CyCLONe are următoarele sarcini:

(a) consolidarea nivelului de pregătire pentru gestionarea incidentelor și a crizelor **de securitate cibernetică** de mare amploare;

(b) dezvoltarea unei conștientizări comune a situației, în ceea ce privește [...] incidentele și crizele de mare amploare în materie de securitate cibernetică;

(ba) evaluarea consecințelor și a impactului incidentelor de securitate cibernetică de mare amploare relevante și propunerea unor posibile măsuri de atenuare;

(c) coordonarea gestionării incidentelor și a crizelor **de securitate cibernetică** de mare amploare și sprijinirea procesului decizional la nivel politic în legătură cu astfel de incidente și crize;

(d) **la solicitarea unui stat membru,** discutarea planurilor **sale** naționale de răspuns la incidente și crize în materie de securitate cibernetică menționate la articolul 7 alineatul (**3**[...])**;**[...]

(4) UE-CyCLONe își adoptă regulamentul de procedură.

(5) UE-CyCLONe prezintă periodic rapoarte grupului de cooperare cu privire la **gestionarea incidentelor și crizelor de securitate cibernetică de mare amploare**, concentrându-se în special pe impactul acestora asupra entităților esențiale și importante.

(6) UE-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite.

(7) UE-CyCLONe prezintă Parlamentului European și Consiliului un raport de evaluare a activității sale până la [24 luni de la data intrării în vigoare a prezentei directive].

Articolul 14a

Cooperarea internațională

Dacă este cazul, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau cu organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT și ale UE-CyCLONe, în conformitate cu dreptul Uniunii privind protecția datelor.

Articolul 15

Raportul privind situația în materie de securitate cibernetică în Uniune

(1) ENISA elaborează, în cooperare cu Comisia **și cu Grupul de cooperare**, un raport bienal privind situația în materie de securitate cibernetică în Uniune. **În special,** [...] raportul [...] include [...] următoarele elemente:

(aa) o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, ținând seama de situația amenințărilor;

(a) [...] **o evaluare a** dezvoltării capacităților în materie de securitate cibernetică **în sectorul public și cel privat** în întreaga Uniune;

(b) [...]

(c) **o evaluare agregată pe baza unor indicatori calitativi și cantitativi** în materie de securitate cibernetică [...] care să [...] **ofere o imagine de ansamblu asupra** nivelului de maturitate al capacităților în materie de securitate cibernetică**, inclusiv al capacităților sectoriale**.

(2) Raportul include recomandări de politică specifice pentru îmbunătățirea nivelului de securitate cibernetică în întreaga Uniune și un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situația tehnică în materie de securitate cibernetică ale agenției, emise de ENISA în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881.

Articolul 16

Învățare *inter pares*

(1) **În vederea consolidării încrederii reciproce, a atingerii unui nivel comun ridicat de securitate cibernetică, precum și a consolidării capacităților și politicilor statelor membre în materie de securitate cibernetică necesare pentru punerea în aplicare eficace a prezentei directive, Grupul de cooperare**[...] [...] stabilește, **cu sprijinul Comisiei și** după consultarea [...] ENISA**, și, după caz, a rețelei CSIRT,** și în termen de cel mult **24 [...] de** luni de la intrarea în vigoare a prezentei directive, metodologia [...] **pentru un sistem de învățare** *inter pares* **obiectiv, nediscriminatoriu și echitabil în ceea ce privește [...] punerea în aplicare a prezentei directive de către** statele membre [...]. **Participarea la învățarea *inter pares* este voluntară. Sistemul constă în runde de evaluare**[...] efectuate de experți [...] în materie de securitate cibernetică din [...] statele membre și acoperă [...] **unul sau mai multe dintre** următoarele elemente:

(i) [...] punerea în aplicare a cerințelor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare menționate la articolele 18 și 20;

(ii) [...] capacitățile, inclusiv resursele [...] disponibile, și [...] exercitarea sarcinilor autorităților naționale competente **menționate la articolul 8 și ale CSIRT menționate la articolul 9**;

[...]

(i**ii**[...]) [...] **implementarea** asistenței reciproce menționate la articolul 34;

(**iv**) [...] **implementarea** cadrului privind schimbul de informații, menționat la articolul 26 [...].

(2) **Criteriile pe baza cărora statele membre desemnează experți eligibili să participe la rundele de învățare *inter pares* sunt**[...] obiective, nediscriminatorii, echitabile și transparente [...] **și sunt incluse în metodologia menționată la alineatul (1)**. ENISA și Comisia [...] **pot** desemna experți care să participe în calitate de observatori la [...] **rundele de învățare*inter pares*** . [...]

(3) [...] .

(3a) Înainte de începerea rundelor de învățare *inter pares*, statele membre pot efectua o autoevaluare a aspectelor vizate de respectiva rundă de învățare *inter pares* și pot furniza autoevaluarea respectivă experților desemnați menționați la alineatul (2).

(4) [...] **Învățarea** *inter pares* **poate să** implice vizite la fața locului [...] **fizice** sau virtuale și schimburi *ex situ*. Având în vedere principiul bunei cooperări, statele membre care [...] **participă la învățarea *inter pares*** furnizează experților desemnați informațiile [...] necesare pentru [...]**evaluare, fără a aduce atingere dreptului intern sau al Uniunii privind protecția informațiilor confidențiale sau clasificate sau protejării funcțiilor esențiale ale statului, cum ar fi securitatea națională.** Orice informație obținută prin intermediul procesului de [...]**învățare** *inter pares* este utilizată exclusiv în acest scop. Experții care participă la [...]**învățarea** *inter pares* nu divulgă terților nicio informație sensibilă sau confidențială obținută în [...] **acest context**. **Statul membru care participă la învățarea *inter pares* se poate opune desemnării anumitor experți din motive justificate corespunzător, comunicate Grupului de cooperare.**

(5) Odată **supuse unei runde de învățare *inter pares*** [...], aceleași aspecte nu fac obiectul unor noi [...]**runde de învățare** *inter pares* [...] **pentru statele membre participante** timp de [...] **patru** ani de la încheierea **respectivei runde de învățare** [...] *inter pares*, **cu excepția cazului în care statul membru în cauză solicită acest lucru sau își exprimă acordul la propunerea**[...] **Grupului de cooperare[...]**.

(6) [...]

(7) Experții care participă la [...]**runde de învățare** *inter pares* elaborează rapoarte cu privire la constatările și concluziile evaluărilor. **Statelor membre li se permite să formuleze observații cu privire la proiectele de rapoarte ale acestora, care se anexează la raport.** Rapoartele **finale** sunt prezentate[...] Grupului de cooperare[...]. **Statele membre pot decide să își pună rapoartele respective la dispoziția publicului.**

CAPITOLUL IV

Gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare

SECȚIUNEA I

Gestionarea și raportarea riscurilor în materie de securitate cibernetică

Articolul 17

Guvernanța

(1) Statele membre se asigură că organele de conducere ale entităților esențiale și importante aprobă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate de entitățile respective pentru a se conforma articolului 18, supraveghează punerea în aplicare a acestuia și **pot fi trase la răspundere** pentru nerespectarea de către entități a obligațiilor care le revin în temeiul prezentului articol.

Aplicarea prezentului alineat nu aduce atingere dreptului intern al statului membru în ceea ce privește normele privind răspunderea în instituțiile publice, precum și răspunderea funcționarilor publici și a funcționarilor aleși și numiți.

(2) Statele membre se asigură că **membrii organului de conducere au obligația să** urmeze, în mod regulat, cursuri de formare [...] pentru a dobândi suficiente cunoștințe și competențe în vederea identificării și a evaluării riscurilor și a practicilor de gestionare în materie de securitate cibernetică, precum și a impactului acestora asupra operațiunilor pe care le desfășoară entitatea.

Articolul 18

Măsuri de gestionare a riscurilor în materie de securitate cibernetică

(1a) **Prezenta directivă aplică o abordare bazată pe „toate pericolele”, care include protecția rețelelor și a sistemelor informatice și a mediului lor fizic în fața oricărui eveniment care poate compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele sau de sistemele informatice sau accesibile prin intermediul acestora.**

(1) Statele membre se asigură că entitățile esențiale și importante iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează pentru a furniza servicii. Ținând seama de cele mai avansate cunoștințe în domeniu **și de costurile implementării**, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului prezentat. **Atunci când se evaluează proporționalitatea acestor măsuri, trebuie să se țină seama în mod corespunzător de gradul de expunere a entității la riscuri, de dimensiunea acesteia, de probabilitatea apariției incidentelor și de gravitatea acestora. Ținându-se cont de nivelul și tipul riscului pentru societate în cazul unor incidente care afectează entități esențiale sau importante, măsurile de gestionare a riscurilor în materie de securitate cibernetică impuse entităților importante pot fi mai puțin stricte decât cele impuse entităților esențiale.**

(2) Măsurile menționate la alineatul (1) includ cel puțin următoarele:

(a) analiza riscurilor și politicile de securitate a sistemelor informatice;

(b) administrarea incidentelor (prevenirea și detectarea incidentelor, [...] răspunsul la acestea **și redresarea în urma acestora**);

(c) continuitatea activității și gestionarea crizelor;

(d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi de servicii **direcți**, cum ar fi furnizorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate;

(e) securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora;

(f) politici și proceduri [...] pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;

(g) **politica privind** utilizarea criptografiei și a criptării;

(ga) securitatea resurselor umane, politicile de control al accesului și gestionarea activelor.

(3) Statele membre se asigură că, atunci când au în vedere luarea măsurilor adecvate menționate la alineatul (2) litera (d), entitățile [...] **au obligația de a lua** în considerare vulnerabilitățile specifice fiecărui prestator și furnizor **direct**de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare. **Statele membre se asigură, de asemenea, că, atunci când au în vedere luarea măsurilor adecvate menționate la alineatul (2) litera (d), entitățile au obligația de a ține seama de rezultatele evaluărilor coordonate ale riscurilor efectuate în conformitate cu articolul 19 alineatul (1).**

(4) Statele membre se asigură că, în cazul în care o entitate constată că serviciile sau sarcinile sale nu sunt în conformitate cu cerințele prevăzute la alineatul (2), aceasta ia, fără întârzieri nejustificate, toate măsurile corective necesare pentru a asigura conformitatea serviciului respectiv.

(5) Comisia poate adopta acte de punere în aplicare pentru a stabili specificațiile tehnice și metodologice**, precum și aspecte cu specific sectorial, dacă este necesar,** ale elementelor menționate la alineatul (2) **de la prezentul articol**. **Comisia adoptă, până la [18 luni de la intrarea în vigoare a prezentei directive], acte de punere în aplicare pentru a stabili specificațiile tehnice și metodologice pentru entitățile menționate la articolul 24 alineatul (1) și pentru prestatorii de servicii de încredere menționați în anexa I punctul 8. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2).** Atunci când pregătește **astfel de** acte [...] **de punere în aplicare**, Comisia [...] urmează, în cea mai mare măsură posibilă, standardele internaționale și europene, precum și specificațiile tehnice relevante **și face schimb de opinii cu Grupul de cooperare și cu ENISA cu privire la proiectul de act de punere în aplicare, în conformitate cu articolul 12 alineatul (4) litera (d)**.

(6) [...]

Articolul 19

Evaluări coordonate la nivelul UE ale riscurilor legate de lanțurile de aprovizionare critice

(1) Grupul de cooperare, în cooperare cu Comisia și ENISA, poate efectua evaluări coordonate ale riscurilor în materie de securitate ale anumitor lanțuri de aprovizionare ale serviciilor, sistemelor sau produselor TIC critice, ținând seama de factorii de risc de natură tehnică și, după caz, care nu sunt de natură tehnică.

(2) Comisia, după consultarea grupului de cooperare și a ENISA, identifică serviciile, sistemele sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor menționate la alineatul (1).

Articolul 20

Obligații de raportare

(1) Statele membre se asigură că entitățile esențiale și importante notifică, fără întârzieri nejustificate, autorităților competente sau CSIRT, în conformitate cu alineatele (3) și (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor. Dacă este cazul, entitățile respective notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor **aceste** incidente care ar putea afecta în mod negativ prestarea serviciului respectiv. Statele membre se asigură că entitățile respective raportează, printre altele, orice informație care să le permită autorităților competente sau CSIRT să stabilească dacă incidentul are un impact transfrontalier. **Actul de notificare în sine nu expune entitatea notificatoare unei răspunderi sporite.**

(2) [...]

Dacă este cazul, entitățile [...] **esențiale și importante** notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă măsurile sau măsurile corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, entitățile le notifică, de asemenea, destinatarilor în cauză amenințarea propriu-zisă. **Actul de** notificare **în sine** nu expune entitatea notificatoare unei răspunderi sporite.

(3) Un incident este considerat semnificativ dacă:

(a) incidentul a provocat sau are potențialul de a provoca perturbări operaționale [...] **grave ale serviciului** sau pierderi financiare substanțiale pentru entitatea în cauză;

(b) incidentul a afectat sau are potențialul de a afecta alte persoane fizice sau juridice, cauzând pierderi materiale sau morale considerabile.

(4) Statele membre se asigură că, în scopul notificării prevăzute la alineatul (1), entitățile în cauză transmit autorităților competente sau CSIRT:

(a) fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incident, o notificare inițială **sub forma unei alerte timpurii** care, după caz, indică dacă există suspiciuni că incidentul a fost cauzat de acțiuni ilegale sau răuvoitoare;

(b) la cererea unei autorități competente sau a unei CSIRT, un raport intermediar privind actualizarea relevantă a situației;

(c) un raport **final**, în termen de cel mult o lună de la transmiterea [...] **notificării inițiale** menționate la litera (a), care să includă cel puțin următoarele elemente:

(i) o descriere detaliată a incidentului, a gravității și a impactului acestuia;

(ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs.

Statele membre se asigură că, în cazuri justificate în mod corespunzător și în acord cu autoritățile competente sau cu CSIRT, entitatea în cauză se poate abate de la termenele prevăzute la literele (a) și (c). **În special, o abatere de la termenul menționat la litera (c) poate fi justificată în cazurile în care incidentul este încă în desfășurare.**

(5) Autoritățile naționale competente sau CSIRT furnizează, [...] **fără întârzieri nejustificate după** primirea notificării inițiale menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incident și, la cererea entității, orientări privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care CSIRT nu a primit notificarea menționată la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu CSIRT. CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, autoritățile naționale competente sau CSIRT furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii.

(6) După caz, mai ales dacă incidentul menționat la alineatul (1) implică două sau mai multe state membre, autoritatea competentă, CSIRT sau **punctul unic de contact** informează celelalte state membre afectate și ENISA cu privire la incident. **Aceste informații conțin cel puțin elementele prevăzute la alineatul (4) de la prezentul articol.** Astfel, autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea informațiilor furnizate.

(7) În cazul în care sensibilizarea publicului este necesară pentru a preveni un incident sau pentru a face față unui incident în curs sau în cazul în care divulgarea incidentului este în alt mod în interesul public, autoritatea competentă sau CSIRT și, după caz, autoritățile sau echipele CSIRT din alte state membre vizate pot, după consultarea entității în cauză, să informeze publicul cu privire la incident sau să solicite entității să facă acest lucru.

(8) La cererea autorității competente sau a echipei CSIRT, punctul unic de contact transmite notificările primite în temeiul alineatului [...] (1) [...] punctelor unice de contact din celelalte state membre afectate.

(9) Punctul unic de contact transmite ENISA [...] **o dată la șase luni** un raport de sinteză care include date anonimizate și agregate privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu alineatul [...] (1) [...] și în conformitate cu articolul 27. Pentru a contribui la furnizarea de informații comparabile, ENISA poate emite orientări tehnice cu privire la parametrii informațiilor incluse în raportul de sinteză. **ENISA informează semestrial Grupul de cooperare și rețeaua CSIRT cu privire la constatările sale referitoare la notificările primite.**

(10) Autoritățile competente furnizează autorităților competente desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] informații cu privire la incidentele și amenințările cibernetice notificate în conformitate cu alineatele (1) și (2) de către entitățile esențiale identificate ca fiind entități critice **[**sau ca fiind entități echivalente cu entitățile critice**]**, în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice].

(11) Comisia poate adopta acte de punere în aplicare pentru a preciza mai în detaliu tipul de informații, formatul și procedura referitoare la o notificare transmisă în temeiul alineatelor (1) și (2). Comisia poate adopta, de asemenea, acte de punere în aplicare pentru a preciza mai în detaliu cazurile în care un incident este considerat semnificativ, astfel cum se menționează la alineatul (3). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2).

Articolul 21

Utilizarea sistemelor europene de certificare a securității cibernetice

(1) Pentru a demonstra conformitatea cu anumite cerințe de la articolul 18, **statele membre le pot solicita entităților să utilizeze anumite produse** [...], **servicii** [...] **și procese TIC certificate** în cadrul sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. Produsele, serviciile și procesele **TIC** care fac obiectul certificării pot fi elaborate de o entitate esențială sau importantă sau achiziționate de la terți.

(2) Comisia poate [...] să adopte [...] acte de punere în aplicare pentru a preciza ce categorii de entități esențiale sau importante au obligația de a utiliza anumite produse, servicii sau procese TIC certificate sau de a obține un certificat [...] în cadrul [...] sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.[...] Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2). **Atunci când pregătește astfel de acte de punere în aplicare, Comisia, în conformitate cu articolul 56 din Regulamentul (UE) 2019/881:**

(i) ia în considerare impactul măsurilor asupra producătorilor sau furnizorilor de astfel de produse, servicii sau procese TIC, precum și asupra utilizatorilor în ceea ce privește costul măsurilor respective, avantajele societale sau economice care decurg din nivelul sporit de securitate preconizat pentru produsele, serviciile sau procesele TIC vizate, precum și alternativele acestora disponibile pe piață;

(ii) desfășoară un proces de consultare deschis, transparent și incluziv cu toate părțile interesate relevante și cu statele membre;

(iii) **ia în considerare termenele de punere în aplicare, precum și măsurile și perioadele de tranziție, în special în ceea ce privește impactul posibil al măsurilor asupra producătorilor sau a furnizorilor de produse, servicii sau procese TIC sau asupra utilizatorilor acestora, îndeosebi asupra IMM-urilor;**

(iv) **ține seama de existența și de punerea în aplicare a legislației relevante a statelor membre.**

(3) Comisia poate solicita ENISA să pregătească o propunere de sistem **sau să revizuiască un sistem european de certificare a securității cibernetice** în temeiul articolului 48 alineatul (2) din Regulamentul (UE) 2019/881 în cazurile în care nu este disponibil niciun sistem european adecvat de certificare a securității cibernetice în sensul alineatului (2) **de la prezentul articol**.

Articolul 22

Standardizarea

(1) Pentru promovarea punerii în aplicare convergente a articolului 18 alineatele (1) și (2), statele membre, fără a impune sau a crea discriminare în favoarea utilizării unui anumit tip de tehnologie, încurajează utilizarea standardelor și a specificațiilor europene sau a celor acceptate la nivel internațional relevante pentru securitatea rețelelor și a sistemelor informatice.

(2) ENISA, în colaborare cu statele membre, elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale ale statelor membre, care ar permite reglementarea acestor domenii.

Articolul 23

Bazele de date cu numele de domenii și datele de înregistrare

(1) Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre se asigură că registrele **de nume** TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD colectează și mențin date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, **în conformitate cu** [...] legislația Uniunii în materie de protecție a datelor cu caracter personal.

(2) Statele membre se asigură că bazele de date cu datele de înregistrare a numelor de domenii menționate la alineatul (1) conțin informații relevante pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor**, inclusiv cel puțin următoarele date:**

a) numele de domeniu

b) data înregistrării

c) datele solicitantului înregistrării, inclusiv:

(i) pentru persoane fizice – nume, prenume și adresă de e-mail;

(ii) pentru persoane juridice – nume și adresă de e-mail.

(3) Statele membre se asigură că registrele **de nume** TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD dispun de politici și proceduri care să asigure că bazele de date conțin informații exacte și complete. Statele membre se asigură că aceste politici și proceduri sunt puse la dispoziția publicului.

(4) Statele membre se asigură că registrele **de nume** TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD publică, fără întârzieri nejustificate după înregistrarea unui nume de domeniu, date de înregistrare a domeniului care nu sunt date cu caracter personal.

(5) Statele membre se asigură că registrele **de nume** TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD oferă acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu legislația Uniunii în materie de protecție a datelor. Statele membre se asigură că registrele **de nume** TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD răspund fără întârzieri nejustificate **și, în orice caz, în termen de 72 de ore** la toate cererile de acces. Statele membre se asigură că politicile și procedurile de divulgare a unor astfel de date sunt puse la dispoziția publicului.

Secțiunea II

Jurisdicție și înregistrare

Articolul 24

Jurisdicție și teritorialitate

(1a) Se consideră că entitățile care fac obiectul prezentei directive se află sub jurisdicția statului membru în care își prestează serviciile. Se consideră că entitățile menționate la punctele 1-7 și 10 din anexa I, prestatorii de servicii de încredere și furnizorii de internet exchange point-uri menționați la punctul 8 din anexa I și la punctele 1-5 din anexa II se află sub jurisdicția statului membru pe teritoriul căruia își au sediul.

(1) Se consideră că furnizorii de servicii DNS, registrele de nume TLD **și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD**, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, [...] furnizorii de rețele de distribuție de conținut**, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate** menționați la punctul 8 **și la punctul 8a** din anexa I, precum și furnizorii digitali menționați la punctul 6 din anexa II se află sub jurisdicția statului membru în care își au sediul principal din Uniune.

(2) În sensul prezentei directive, se consideră că entitățile menționate la alineatul (1) își au sediul principal din Uniune în statul membru în care se iau **în mod predominant** deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. În cazul în care **nu poate fi stabilit locul în care astfel de decizii sunt luate în mod predominant sau dacă** astfel de decizii nu se iau în niciun sediu din Uniune, se consideră că sediul principal este în statul membru în care entitățile au sediul cu cel mai mare număr de angajați din Uniune. **În cazul în care serviciile sunt furnizate de un grup de întreprinderi, se consideră că sediul principal este sediul principal al grupului de întreprinderi.**

(3) În cazul în care o entitate menționată la alineatul (1) nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant desemnat în Uniune în temeiul prezentului articol, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru nerespectarea obligațiilor care îi revin în temeiul prezentei directive.

(4) Desemnarea unui reprezentant de către o entitate menționată la alineatul (1) nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși.

(4a) Statele membre care au primit o cerere de asistență reciprocă în legătură cu entitățile menționate la alineatul (1) pot, în limitele cererii, să ia măsuri adecvate de supraveghere și de asigurare a respectării legislației în ceea ce privește entitatea în cauză care furnizează servicii sau care își are rețeaua și sistemul informatic pe teritoriul lor.

Articolul 25

Registrul pentru anumite entități de infrastructură digitală și furnizori digitali

(1) [...] **Statele membre se asigură că**[...] entitățile **menționate la articolul 24 alineatul (1) care își au sediul principal pe teritoriul lor sau, în cazul în care nu sunt stabilite în Uniune, care își au reprezentantul desemnat în Uniune stabilit pe teritoriul lor** [...] transmit **autorităților competente** următoarele informații [...] până la [cel târziu 12 luni de la intrarea în vigoare a directivei]:

(a) denumirea entității;

(aa) tipul de entitate în conformitate cu anexele I și II la prezenta directivă;

(b) adresa sediului său principal și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 24 alineatul (3);

(c) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale entităților **și ale reprezentanților lor;**

(d) statele membre în care entitatea furnizează serviciul.

După caz, aceste informații sunt transmise prin intermediul mecanismului național [...] de autonotificare menționat la articolul 2a.

(2) **Statele membre se asigură că** entitățile menționate la alineatul (1) notifică [...] **de asemenea** fără întârziere și, în orice caz, în termen de trei luni de la data la care a intrat în vigoare modificarea, [...] orice modificare a datelor pe care le-au transmis în temeiul alineatului (1).

(3) [...] Punctele unice de contact ale statelor membre transmit ENISA informațiile menționate la alineatele (1) și (2) [...]. [...]

(3a) Pe baza informațiilor primite în conformitate cu alineatul (3) de la prezentul articol, ENISA creează și menține un registru al entităților menționate la alineatul (1). La cererea statelor membre, ENISA permite accesul autorităților competente relevante la registru, asigurând în același timp garanțiile necesare pentru protejarea confidențialității informațiilor, după caz.

(4) [...]

CAPITOLUL V

Schimbul de informații

Articolul 26

Acorduri privind schimbul de informații în materie de securitate cibernetică

(1) [...] Statele membre se asigură că entitățile esențiale și importante pot, **în mod voluntar,** face schimb de informații relevante în materie de securitate cibernetică, inclusiv de informații referitoare la amenințări cibernetice, **incidente evitate la limită,** vulnerabilități, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în cazul în care un astfel de schimb de informații:

(a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau atenuarea acestora;

(b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea răspândirii amenințărilor cibernetice, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare.

(2) Statele membre se asigură că schimbul de informații are loc în cadrul unor comunități [...] ale entităților esențiale și importante. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informații, ținând seama de caracterul potențial sensibil al informațiilor partajate [...].

(3) Statele membre **pot** stabili norme care să specifice procedura, elementele operaționale (inclusiv utilizarea platformelor TIC dedicate), conținutul și condițiile acordurilor privind schimbul de informații menționate la alineatul (2). Aceste norme **pot** stabili, de asemenea, detaliile implicării autorităților publice în astfel de acorduri, precum și elementele operaționale, inclusiv utilizarea platformelor informatice dedicate. Statele membre oferă sprijin pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menționate la articolul 5 alineatul (2) litera (g).

(4) Entitățile esențiale și importante informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații menționate la alineatul (2), odată cu încheierea unor astfel de acorduri sau, după caz, cu retragerea din astfel de acorduri, după ce retragerea intră în vigoare.

(5) [...] ENISA sprijină instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) oferind bune practici și orientări.

Articolul 27

Notificarea voluntară a informațiilor relevante

(1) Fără a aduce atingere articolului 20, statele membre se asigură că entitățile esențiale și importante pot notifica, în mod voluntar, autorităților competente sau echipelor CSIRT orice incidente, amenințări cibernetice sau incidente evitate la limită relevante.

(2) Statele membre se asigură că, fără a aduce atingere articolului 3, entitățile care nu intră în domeniul de aplicare al prezentei directive pot transmite notificări, în mod voluntar, cu privire la incidente , amenințări cibernetice sau incidente evitate la limită semnificative. Atunci când tratează notificările, statele membre acționează în conformitate cu procedura prevăzută la articolul 20. Statele membre pot trata notificările obligatorii cu prioritate față de notificările voluntare. **Fără a aduce atingere măsurilor de depistare, investigare sau urmărire a infracțiunilor penale,** notificarea voluntară nu impune entității raportoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

(3) Notificările voluntare se tratează doar atunci când această prelucrare nu constituie o sarcină disproporționată sau neavenită asupra statului membru în cauză.

CAPITOLUL VI

Supravegherea și asigurarea respectării legislației

Articolul 28

Aspecte generale privind supravegherea și asigurarea respectării legislației

(1) Statele membre se asigură că autoritățile competente monitorizează în mod eficace și iau măsurile necesare pentru a asigura respectarea prezentei directive, în special a obligațiilor prevăzute la articolele 18**,** [...] 20 **și 23**. **Statele membre pot permite autorităților competente să acorde prioritate supravegherii, care se fondează pe o abordare bazată pe riscuri.**

(2) În cazul incidentelor de securitate cibernetică, autoritățile competente lucrează în strânsă cooperare cu autoritățile de protecție a datelor, **cu autoritățile competente desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice], cu organismele de supraveghere desemnate în temeiul Regulamentului (UE) nr. 910/2014 și cu alte autorități competente desemnate în temeiul anumitor acte juridice sectoriale ale Uniunii.** [...]

(3) Fără a aduce atingere cadrelor legislative și instituționale naționale, statele membre se asigură că, în ceea ce privește supravegherea conformității entităților administrației publice cu prezenta directivă și aplicarea sancțiunilor potențiale în caz de neconformitate, autoritățile competente au competențele corespunzătoare pentru a îndeplini astfel de sarcini cu independență operațională în raport cu entitățile supravegheate. Statele membre pot decide impunerea unor măsuri adecvate, proporționale și eficace de supraveghere și de asigurare a respectării legislației în ceea ce privește aceste entități, în conformitate cu cadrele naționale și cu ordinea juridică.

Articolul 29

Supravegherea și asigurarea respectării legislației pentru entitățile esențiale

(1) Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legislației impuse entităților esențiale în ceea ce privește obligațiile prevăzute în prezenta directivă sunt eficace, proporționale și disuasive, ținând seama de circumstanțele fiecărui caz în parte.

(2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, **urmează o abordare bazată pe riscuri și** au competența de a supune entitățile respective **cel puțin**:

(a) unor inspecții la fața locului și unei supravegheri ex situ, inclusiv unor verificări aleatorii;

(b) unor audituri **de securitate**;

(c) unor audituri de securitate specifice bazate pe evaluări ale riscurilor sau pe informații disponibile legate de riscuri;

(d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, **atunci când acest lucru este necesar din motive tehnice, cu cooperarea entității în cauză**;

(e) unor cereri de informații necesare pentru a evalua măsurile de securitate cibernetică adoptate de entitate, inclusiv politicile de securitate cibernetică documentate [...];

(f) unor cereri de acces la date, la documente sau la toate informațiile necesare pentru îndeplinirea sarcinilor lor de supraveghere;

(g) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și elementele de probă care stau la baza acestora.

(2a) Atunci când își exercită sarcinile de supraveghere prevăzute la alineatul (2) de la prezentul articol, autoritățile competente pot stabili metodologii de supraveghere care să permită stabilirea unei ordini de prioritate a acestor sarcini, urmând o abordare bazată pe riscuri.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (e) - (g), autoritățile competente precizează scopul solicitării și informațiile solicitate.

(4) Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legislației în ceea ce privește entitățile esențiale, autoritățile competente au competența **cel puțin**:

(a) de a emite avertismente cu privire la nerespectarea de către entități a obligațiilor prevăzute în prezenta directivă;

(b) de a emite instrucțiuni obligatorii sau un ordin prin care le solicită acestor entități să remedieze deficiențele identificate sau încălcările obligațiilor prevăzute în prezenta directivă;

(c) de a dispune ca entitățile respective să înceteze comportamentul care nu respectă obligațiile prevăzute în prezenta directivă și să se abțină de la repetarea comportamentului respectiv;

(d) de a dispune ca entitățile respective să asigure conformitatea măsurilor lor de gestionare a riscurilor și/sau a obligațiilor lor de raportare cu obligațiile prevăzute la articolele 18 și 20 într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile respective să informeze persoana (persoanele) fizică (fizice) sau juridică (juridice) căreia (cărora) îi (le) furnizează servicii sau activități care sunt potențial afectate de o amenințare cibernetică semnificativă **cu privire la caracterul amenințării, precum și** cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoana (persoanele) fizică (fizice) sau juridică (juridice) în cauză ca răspuns la amenințarea respectivă;

(f) de a dispune ca entitățile respective să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(g) [...]

(h) de a dispune ca entitățile respective să facă publice într-un anumit mod aspectele legate de nerespectarea obligațiilor prevăzute în prezenta directivă**, în cazul în care o astfel de divulgare publică nu conduce la o expunere dăunătoare a entității respective**;

(i) [...]

(j) de a impune sau a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei amenzi administrative în temeiul articolului 31, în plus față de măsurile menționate la literele (a)-(i) de la prezentul alineat sau în locul acestora, în funcție de circumstanțele fiecărui caz în parte.

(5) În cazul în care măsurile de asigurare a respectării legislației adoptate în temeiul alineatului (4) literele (a)-(d) și (f) se dovedesc ineficiente, statele membre se asigură că autoritățile competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile competente au competența:

(a) să suspende sau să solicite unui organism de certificare sau de autorizare **ori instanțelor conform legislației naționale** suspendarea unei certificări sau a unei autorizații privind o parte sau toate serviciile sau activitățile furnizate de o entitate esențială;

(b) să impună sau să solicite impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială respectivă, precum și împotriva oricărei alte persoane fizice declarate responsabilă de încălcare.

Aceste sancțiuni se aplică numai până în momentul în care entitatea ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă în temeiul cărora au fost aplicate aceste sancțiuni.

Sancțiunile prevăzute la prezentul alineat nu se aplică entităților administrației publice vizate de prezenta directivă.

(6) Statele membre se asigură că orice persoană fizică responsabilă de o entitate esențială sau care acționează în calitate de reprezentant al acestei entități pe baza competenței de a o reprezenta, a autorității de a lua decizii în numele acesteia sau a autorității de a exercita controlul asupra acesteia are competența de a se asigura că aceasta respectă obligațiile prevăzute în prezenta directivă. Statele membre se asigură că aceste persoane fizice pot fi trase la răspundere pentru încălcarea obligațiilor care le revin de a asigura respectarea obligațiilor prevăzute în prezenta directivă. **În ceea ce privește entitățile administrației publice, prezenta dispoziție nu aduce atingere legislației statelor membre în ceea ce privește răspunderea funcționarilor publici și a funcționarilor aleși și numiți.**

(7) Atunci când iau măsuri de asigurare a respectării legislației sau aplică sancțiuni în temeiul alineatelor (4) și (5), autoritățile competente respectă dreptul la apărare, iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător cel puțin de:

(a) gravitatea încălcării și importanța dispozițiilor încălcate. Printre încălcările care ar trebui considerate grave se numără: încălcări repetate, neîndeplinirea obligației de notificare sau de remediere a incidentelor cu un efect perturbator semnificativ, neremedierea deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente, obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea competentă în urma constatării unei încălcări, furnizarea de informații false sau vădit denaturate în ceea ce privește cerințele de gestionare a riscurilor sau obligațiile de raportare prevăzute la articolele 18 și 20.

(b) durata încălcării, inclusiv caracterul repetitiv al încălcărilor;

(c) daunele reale cauzate sau pierderile suferite ori daunele sau pierderile potențiale care ar fi putut fi cauzate, în măsura în care acestea pot fi determinate. La evaluarea acestui aspect, se ține seama, printre altele, de pierderile financiare sau economice reale sau potențiale, de efectele asupra altor servicii și de numărul de utilizatori afectați sau potențial afectați;

(d) caracterul încălcării (intenționat sau din neglijență);

(e) măsurile luate de entitate pentru a preveni sau a atenua daunele și/sau pierderile;

(f) aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

(g) nivelul de cooperare al persoanei (persoanelor) fizice sau juridice considerate responsabile cu autoritățile competente.

(8) Autoritățile competente prezintă o motivare detaliată a deciziilor lor de asigurare a respectării legislației. Înainte de a lua astfel de decizii, autoritățile competente notifică entităților în cauză constatările lor preliminare și acordă entităților respective un termen rezonabil pentru prezentarea observațiilor**, cu excepția cazului în care există un pericol iminent**.

(9) Statele membre se asigură că autoritățile lor competente **în temeiul prezentei directive** informează autoritățile competente relevante din **același** stat membru [...] desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] atunci când își exercită competențele de supraveghere și de asigurare a respectării legislației menite să asigure conformitatea unei entități esențiale identificate ca fiind critică sau **[**ca fiind o entitate echivalentă cu o entitate critică**]**, în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] cu obligațiile care decurg din prezenta directivă. **După caz,** [...] autoritățile competente în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice][...] **pot solicita** autorităților competente **în temeiul prezentei directive**[...] să își exercite **competențele** de supraveghere și de asigurare a respectării legislației **în legătură cu** o entitate esențială care intră în domeniul de aplicare al prezentei directive și care este identificată, de asemenea, ca fiind critică **[**sau ca fiind o entitate echivalentă cu o entitate critică**] în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice].**

(10) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere în temeiul articolului 29 alineatul (1) din Regulamentul (UE) XXXX/XXXX [DORA] atunci când își exercită competențele de supraveghere și de asigurare a respectării legislației menite să asigure conformitatea unei entități esențiale desemnate drept furnizor terț de servicii TIC de importanță critică în temeiul articolului 28 din Regulamentul (UE) XXXX/XXXX [DORA] cu obligațiile care decurg din prezenta directivă.

(10a) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează autoritățile competente relevante desemnate în temeiul Regulamentului (UE) nr. 910/2014 atunci când își exercită competențele de supraveghere și de asigurare a respectării legislației menite să asigure respectarea de către o entitate desemnată drept prestator de servicii de încredere în temeiul Regulamentului (UE) nr. 910/2014 a obligațiilor care îi revin în temeiul prezentei directive.

Articolul 30

Supravegherea și asigurarea respectării legislației pentru entitățile importante

(1) Atunci când li se furnizează dovezi sau indicii **sau informații** că o entitate importantă nu **ar** respecta obligațiile prevăzute în prezenta directivă, în special la articolele 18 și 20, statele membre se asigură că autoritățile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere *ex post*.

(2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile importante, **urmează o abordare bazată pe riscuri și** au competența de a supune entitățile respective **cel puțin**:

(a) unor inspecții la fața locului și unei supravegheri ex situ ex post;

(b) unor audituri de securitate specifice bazate pe evaluări ale riscurilor sau pe informații disponibile legate de riscuri;

(c) unor scanări de securitate bazate pe criterii obiective, **nediscriminatorii,** echitabile și transparente de evaluare a riscurilor, **atunci când acest lucru este necesar din motive tehnice, cu cooperarea entității în cauză**;

(d) unor cereri de informații necesare pentru a evalua *ex post* măsurile de securitate cibernetică [...];

(e) unor cereri de acces la date, la documente și/sau la informații necesare pentru îndeplinirea sarcinilor de supraveghere;

(ea) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și elementele de probă care stau la baza acestora.

(2a) Atunci când își exercită sarcinile de supraveghere prevăzute la alineatul (2) de la prezentul articol, autoritățile competente pot stabili metodologii de supraveghere care să permită stabilirea unei ordini de prioritate a acestor sarcini, urmând o abordare bazată pe riscuri.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (d)**-(ea)**, autoritățile competente precizează scopul solicitării și informațiile solicitate.

(4) Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legislației în ceea ce privește entitățile importante, autoritățile competente au competența **cel puțin**:

(a) de a emite avertismente cu privire la nerespectarea de către entități a obligațiilor prevăzute în prezenta directivă;

(b) de a emite instrucțiuni obligatorii sau un ordin prin care le solicită acestor entități să remedieze deficiențele identificate sau încălcarea obligațiilor prevăzute în prezenta directivă;

(c) de a dispune ca entitățile respective să înceteze comportamentul care nu respectă obligațiile prevăzute în prezenta directivă și să se abțină de la repetarea comportamentului respectiv;

(d) de a dispune ca entitățile respective să asigure conformitatea măsurilor lor de gestionare a riscurilor sau a obligațiilor lor de raportare cu obligațiile prevăzute la articolele 18 și 20 într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile respective să informeze persoana (persoanele) fizică (fizice) sau juridică (juridice) căreia (cărora) îi (le) furnizează servicii sau activități care sunt potențial afectate de o amenințare cibernetică semnificativă **cu privire la caracterul amenințării, precum și** cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoana (persoanele) fizică (fizice) sau juridică (juridice) în cauză ca răspuns la amenințarea respectivă;

(f) de a dispune ca entitățile respective să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(g) de a dispune ca entitățile respective să facă publice într-un anumit mod aspectele legate de nerespectarea obligațiilor lor prevăzute în prezenta directivă**, în cazul în care o astfel de divulgare publică nu conduce la o expunere dăunătoare a entității respective**;

(h) [...]

(i) de a impune sau a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei amenzi administrative în temeiul articolului 31, în plus față de măsurile menționate la literele (a)-(h) de la prezentul alineat sau în locul acestora, în funcție de circumstanțele fiecărui caz în parte.

(5) Articolul 29 alineatele (6)-(8) se aplică, de asemenea, măsurilor de supraveghere și de asigurare a respectării legislației prevăzute la prezentul articol pentru entitățile importante [...].

Articolul 31

Condiții generale pentru impunerea de amenzi administrative entităților esențiale și importante

(1) Statele membre se asigură că impunerea de amenzi administrative entităților esențiale și importante în temeiul prezentului articol pentru încălcări ale obligațiilor prevăzute în prezenta directivă este, în fiecare caz în parte, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 29 alineatul (4) literele (a)-(i), la articolul 29 alineatul (5) și la articolul 30 alineatul (4) literele (a)(h).

(3) Atunci când se ia decizia de a impune o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită, cel puțin, elementelor prevăzute la articolul 29 alineatul (7).

(4) Statele membre se asigură că încălcările **de către entitățile esențiale ale** obligațiilor prevăzute la articolul 18 sau la articolul 20 fac obiectul, în conformitate cu alineatele (2) și (3) de la prezentul articol, unor amenzi administrative maxime de cel puțin **4**[...] 000 000 EUR sau**, în cazul unei persoane juridice,** 2 % din cifra de afaceri mondială totală anuală a întreprinderii căreia îi aparține entitatea esențială [...] în exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.

(4a) Statele membre se asigură că încălcările de către entitățile importante ale obligațiilor prevăzute la articolul 18 sau la articolul 20 fac obiectul, în conformitate cu alineatele (2) și (3) de la prezentul articol, unor amenzi administrative maxime de cel puțin 2 000 000 EUR sau, în cazul unei persoane juridice, 1 % din cifra de afaceri mondială totală anuală a întreprinderii căreia îi aparține entitatea importantă în exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.

(5) Statele membre pot prevedea competența de a impune penalități cu titlu cominatoriu pentru a obliga o entitate esențială sau importantă să înceteze o încălcare în conformitate cu o decizie prealabilă a autorității competente.

(6) Fără a aduce atingere competențelor autorităților competente menționate la articolele 29 și 30, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative entităților administrației publice menționate la articolul 4 punctul (23), sub rezerva obligațiilor prevăzute în prezenta directivă.

(6a) În cazul în care sistemul juridic al statului membru nu prevede amenzi administrative, statele membre se asigură că prezentul articol poate fi aplicat astfel încât amenda să fie inițiată de autoritatea competentă și impusă de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și că au un efect echivalent cu cel al amenzilor administrative impuse de autoritățile competente. În orice caz, amenzile impuse sunt eficace, proporționale și disuasive. Respectivele state membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la […], precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 32

Încălcări care implică o încălcare a securității datelor cu caracter personal

(1) În cazul în care**, în cursul supravegherii sau al asigurării respectării legislației,** autoritățile competente [...] **au luat cunoștință de faptul** că încălcarea de către o entitate esențială sau importantă a obligațiilor prevăzute la articolele 18 și 20 **din prezenta directivă poate** atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) nr. 2016/679, care este notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează **fără întârzieri nejustificate** autoritățile de supraveghere competente în temeiul articolelor 55 și 56 din regulamentul respectiv [...].

(2) În cazul în care autoritățile de supraveghere competente în conformitate cu articolele 55 și 56 din Regulamentul (UE) 2016/679 decid să își exercite competențele în temeiul articolului 58 **alineatul (2)** litera (i) din regulamentul respectiv și să impună o amendă administrativă, autoritățile competente **menționate la articolul 8 din prezenta directivă** nu impun o amendă administrativă pentru [...] **o** încălcare **care presupune aceeași faptă ca cea prevăzută la**[...] articolul 31 din prezenta directivă. Cu toate acestea, autoritățile competente pot aplica acțiuni de asigurare a respectării legislației sau pot exercita competențele de sancționare prevăzute la articolul 29 alineatul (4) literele (a)-(i), la articolul 29 alineatul (5) și la articolul 30 alineatul (4) literele (a)-(h) din prezenta directivă.

(3) În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este stabilită într-un alt stat membru decât autoritatea competentă, aceasta din urmă poate informa autoritatea de supraveghere stabilită în același stat membru.

Articolul 33

Sancțiuni

(1) Statele membre stabilesc regimul sancțiunilor aplicabile în cazurile de încălcare a dispozițiilor de drept intern adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare.

(2) În termen de [doi] ani de la intrarea în vigoare a prezentei directive, statele membre notifică Comisiei normele și măsurile respective, precum și, fără întârzieri nejustificate, orice modificare ulterioară a acestora.

Articolul 34

Asistență reciprocă

(1) Dacă o entitate esențială sau importantă furnizează servicii în mai multe state membre sau [...] **furnizează servicii în unul sau mai multe state membre**, dar rețelele și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, **autoritățile** competente ale **statelor membre în cauză** [...] cooperează și își oferă asistență reciprocă, după caz. Această cooperare implică cel puțin următoarele:

(a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legislației într-un stat membru informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legislației luate [...];

(b) o autoritate competentă poate solicita unei alte autorități competente să ia măsurile de supraveghere sau de asigurare a respectării legislației [...];

(c) la primirea unei cereri justificate din partea altei autorități competente, o autoritate competentă acordă asistență celeilalte autorități competente, **în mod proporțional cu resursele aflate la dispoziția sa,** astfel încât acțiunile de supraveghere sau de asigurare a respectării legislației [...] să poată fi puse în aplicare într-un mod eficace, eficient și consecvent. O astfel de asistență reciprocă poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri ex situ sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu poate refuza cererea respectivă, cu excepția cazului în care, în urma unui schimb cu celelalte autorități în cauză [...], se stabilește că [...] autoritatea nu are competența de a furniza asistența solicitată sau nu dispune de resursele necesare sau asistența solicitată nu este proporțională cu sarcinile de supraveghere desfășurate de autoritatea competentă [...] sau cererea se referă la informații sau implică activități care intră în conflict cu interesele statului membru respectiv în materie de securitate națională, siguranță publică sau apărare.

(2) Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere [...].

CAPITOLUL VII

Dispoziții tranzitorii și finale

Articolul 35

Revizuirea

Comisia revizuiește periodic funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța sectoarelor, a subsectoarelor, a dimensiunii și a tipului de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În [...] scopul **revizuirii** [...], Comisia ține cont de rapoartele [...] rețelei CSIRT privind experiența obținută la nivel [...] operațional. Primul raport se transmite până la… [54 de luni de la data intrării în vigoare a prezentei directive].

Articolul 36

[...]

[...]

[...]

Articolul 37

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

(3) În cazul în care avizul comitetului urmează să fie obținut prin procedură scrisă, respectiva procedură se încheie fără rezultat atunci când, în termenul stabilit pentru emiterea avizului, președintele comitetului decide în acest sens sau un membru al comitetului solicită acest lucru.

Articolul 38

Transpunere

(1) [...] **Până la**... [...]**24** de luni de la data intrării în vigoare a prezentei directive, statele membre adoptă și publică actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta. Statele membre aplică măsurile respective începând cu … [ziua următoare datei menționate la primul paragraf].

(2) Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.

Articolul 39

Modificarea Regulamentului (UE) nr. 910/2014

Articolul 19 din Regulamentul (UE) nr. 910/2014 se elimină **cu efect de la... [data termenului de transpunere a prezentei directive]**.

Articolul 40

Modificarea Directivei (UE) 2018/1972

Articolele 40 și 41 din Directiva (UE) 2018/1972 se elimină **cu efect de la... [data termenului de transpunere a prezentei directive]**.

Articolul 41

Abrogarea

Directiva (UE) 2016/1148 se abrogă cu efect de la... [data termenului de transpunere a directivei].

Trimiterile la Directiva (UE) 2016/1148 se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa II[...].

Articolul 42

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.

Articolul 43

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*

ANEXA I

SECTOARE, SUBSECTOARE ȘI TIPURI DE ENTITĂȚI

Sectorul	Subsectorul	Tipul de entitate
(1) Energie	(a) Electricitate	— Întreprinderile din domeniul energiei electrice menționate la articolul 2 punctul 57 din Directiva (UE) 2019/944 care îndeplinesc funcția de „furnizare” menționată la articolul 2 punctul 12 din directiva respectivă ([39])
		— Operatorii de distribuție menționați la articolul 2 punctul 29 din Directiva (UE) 2019/944
		— Operatorii de transport și de sistem menționați la articolul 2 punctul 35 din Directiva (UE) 2019/944
		— Producătorii menționați la articolul 2 punctul 38 din Directiva (UE) 2019/944
		— Operatorii pieței de energie electrică desemnați menționați la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 ([40])
		— Participanții la piață menționați la articolul 2 punctul 25 din Regulamentul (UE) 2019/943 care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie menționate la articolul 2 punctele 18, 20 și 59 din Directiva (UE) 2019/944

[39] Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).

[40] Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54).

	(b) Încălzire centralizată și răcire centralizată	— Încălzirea centralizată sau răcirea centralizată menționată la articolul 2 punctul 19 din Directiva (UE) 2018/2001 ([41]) privind promovarea utilizării energiei din surse regenerabile
	(c) 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
		— Entitățile centrale de stocare menționate la articolul 2 litera (f) din Directiva 2009/119/CE a Consiliului ([42])
	(d) Gaze	— Întreprinderile de furnizare menționate la articolul 2 punctul 8 din Directiva 2009/73/CE ([43])
		— Operatorii de distribuție menționați la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatorii de transport și de sistem menționați la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatorii de înmagazinare menționați la articolul 2 punctul 10 din Directiva 2009/73/CE

41 Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82).

42 Directiva 2009/119/CE a Consiliului din 14 septembrie 2009 privind obligația statelor membre de a menține un nivel minim de rezerve de țiței și/sau de produse petroliere (JO L 265, 9.10.2009, p. 9).

43 Directiva 2009/73/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă în sectorul gazelor naturale și de abrogare a Directivei 2003/55/CE (JO L 211, 14.8.2009, p. 94).

		— Operatorii de sistem GNL menționați la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderile din sectorul gazelor naturale, astfel cum sunt definite la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatori de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	Operatori de producție, stocare și transport de hidrogen
(2) Transporturi	(a) Transport aerian	— Transportatorii aerieni menționați la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008 ([44]) **utilizați în scop comercial**
		— Organele de administrare a aeroporturilor menționate la articolul 2 punctul 2 din Directiva 2009/12/CE ([45]), aeroporturile menționate la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 ([46]), precum și entități care operează instalații auxiliare în cadrul aeroporturilor
		— Operatorii de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC),

[44] 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 (JO L 97, 9.4.2008, p. 72).

[45] Directiva 2009/12/CE a Parlamentului European și a Consiliului din 11 martie 2009 privind tarifele de aeroport (JO L 70, 14.3.2009, p. 11).

[46] Regulamentul (CE) 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 (JO L 348, 20.12.2013, p. 1).

		astfel cum sunt menționate la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 ([47])
	(b) Transport feroviar	— Administratorii infrastructurii menționați la articolul 3 punctul 2 din Directiva 2012/34/UE ([48])
		— Întreprinderile feroviare menționate la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatorii unei infrastructuri de servicii menționați la articolul 3 punctul 12 din Directiva 2012/34/UE
	(c) Transport pe apă	— Companiile de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, menționate pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 ([49]), fără a include navele individuale operate de companiile respective
		— Organe de gestionare a porturilor menționate la articolul 3 punctul 1 din Directiva 2005/65/CE ([50]), inclusiv instalațiile portuare ale acestora menționate la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004 și entitățile care operează lucrări și echipamente în cadrul porturilor

[47] 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) (JO L 96, 31.3.2004, p. 1).

[48] Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (JO L 343, 14.12.2012, p. 32).

[49] Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare (JO L 129, 29.4.2004, p. 6).

[50] Directiva 2005/65/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind consolidarea securității portuare (JO L 310, 25.11.2005, p. 28).

		— Operatori de servicii de trafic maritim menționate la articolul 3 litera (o) din Directiva 2002/59/CE ([51])
	(d) Transport rutier	— Autoritățile rutiere menționate la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei ([52]) responsabile cu controlul gestionării traficului**, cu excepția entităților publice în cazul cărora gestionarea traficului sau operatorii de sisteme de transport inteligente reprezintă doar o parte neesențială a activității lor generale**
		— Operatori de sisteme de transport inteligente menționate la articolul 4 punctul 1 din Directiva 2010/40/UE ([53])
(3) Sectorul bancar		— Instituțiile de credit menționate la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 ([54])**, [cu excepția celor menționate la articolul 2 alineatul (5) punctul (8) din Directiva 2013/36/UE, care sunt exceptate în conformitate cu articolul 2 alineatul (4) din Regulamentul XX [DORA]]**

[51] Directiva 2002/59/CE a Parlamentului European și a Consiliului din 27 iunie 2002 de instituire a unui sistem comunitar de monitorizare și informare privind traficul navelor maritime și de abrogare a Directivei 93/75/CEE a Consiliului (JO L 208, 5.8.2002, p. 10).

[52] 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 (JO L 157, 23.6.2015, p. 21).

[53] Directiva 2010/40/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (JO L 207, 6.8.2010, p. 1).

[54] Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

(4) Infrastructuri ale pieței financiare		— Operatori de locuri de tranzacționare menționate la articolul 4 punctul 24 din Directiva 2014/65/UE ([55])
		— Contrapărțile centrale (CPC) menționate la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 ([56])
(5) Sănătate		— Furnizorii de servicii medicale menționați la articolul 3 litera (g) din Directiva 2011/24/UE ([57])
		— Laboratoarele de referință ale UE menționate la articolul 15 din Regulamentul XXXX/XXXX privind amenințările transfrontaliere grave pentru sănătate ([58])
		— Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor menționate la articolul 1 punctul 2 din Directiva 2001/83/CE ([59]) — Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 — Entitățile care fabrică dispozitive medicale considerate esențiale în contextul unei urgențe de sănătate

[55] 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 (JO L 173, 12.6.2014, p. 349).

[56] 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 (JO L 201, 27.7.2012, p. 1).

[57] Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

[58] [Regulamentul Parlamentului European și al Consiliului privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)727 final]

[59] Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).

		publică („lista dispozitivelor esențiale pentru urgența de sănătate publică”) menționate la articolul 20 din Regulamentul XXXX ([60])
(6) Apă potabilă		Furnizori și distribuitori de apă destinată consumului uman menționată la articolul 2 punctul 1 litera (a) din Directiva 98/83/CE a Consiliului ([61]), excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă doar o parte **neesențială** din activitatea lor generală de distribuție a altor produse de bază [...]
(7) Ape uzate		Întreprinderile care colectează, depozitează sau tratează ape urbane reziduale, ape menajere uzate și ape industriale uzate menționate la articolul 2 punctele 1-3 din Directiva 91/271/CEE a Consiliului ([62]) **cu excepția întreprinderilor pentru care colectarea, eliminarea sau tratarea apelor reziduale urbane, menajere și industriale reprezintă doar o parte neesențială a activității lor generale** [...]
(8) Infrastructură digitală		**—** Furnizori de IXP (internet exchange point)
		— Furnizori de servicii DNS**, cu excepția operatorilor de servere de nume rădăcină**
		— Registre de nume TLD
		— Furnizori de servicii de cloud

60 [Regulamentul Parlamentului European și al Consiliului privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)725 final]

61 Directiva 98/83/CE a Consiliului din 3 noiembrie 1998 privind calitatea apei destinate consumului uman (JO L 330, 5.12.1998, p. 32).

62 Directiva 91/271/CEE a Consiliului din 21 mai 1991 privind tratarea apelor urbane reziduale (JO L 135, 30.5.1991, p. 40).

		computing
		— Furnizori de servicii de centre de date
		— Furnizori de rețele de furnizare de conținut
		— Prestatorii de servicii de încredere menționați la articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014 ([63])
		— Furnizorii de rețele publice de comunicații electronice menționate la articolul 2 punctul 8 din Directiva (UE) 2018/1972 ([64]) sau furnizorii de servicii de comunicații electronice menționate la articolul 2 punctul 4 din Directiva (UE) 2018/1972 în cazul în care serviciile acestora sunt destinate publicului
8a. Gestionarea serviciilor TIC **(B2B)**		— **Furnizori de servicii gestionate (MSP)** — **Furnizori de servicii de securitate gestionate (MSSP)**

63 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 (JO L 257, 28.8.2014, p. 73).

64 Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

(9) **Entități de** administrație publică		— Entități de administrație publică din administrația centrală**, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern** — [...][65][...] — [...]
(10) Spațiu		— Operatori de infrastructură terestră deținută, gestionată și operată de statele membre sau de părți private, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice menționate la articolul 2 punctul 8 din Directiva (UE) 2018/1972

65 [...]

ANEXA II

SECTOARE, SUBSECTOARE ȘI TIPURI DE ENTITĂȚI

Sectorul	Subsectorul	Tipul de entitate
(1) Servicii poștale și de curierat		Furnizori de servicii poștale menționate la articolul 2 punctul 1 din Directiva 97/67/CE ([66]), **inclusiv** [...] furnizori de servicii de curierat
(2) Gestionarea deșeurilor		Întreprinderi care efectuează gestionarea deșeurilor menționată la articolul 3 punctul 9 din Directiva 2008/98/CE ([67]), cu excepția întreprinderilor pentru care gestionarea deșeurilor nu reprezintă principala activitate economică

[66] Directiva 97/67/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind normele comune pentru dezvoltarea pieței interne a serviciilor poștale ale Comunității și îmbunătățirea calității serviciului (JO L 15, 21.1.1998, p. 14)**, astfel cum a fost modificată prin Directiva 2008/6/CE a Parlamentului European și a Consiliului din 20 februarie 2008 de modificare a Directivei 97/67/CE cu privire la realizarea integrală a pieței interne a serviciilor poștale ale Comunității (JO L 52, 27.2.2008, p. 3)**.

[67] Directiva 2008/98/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind deșeurile și de abrogare a anumitor directive (JO L 312, 22.11.2008, p. 3).

(3) Fabricarea, producția și distribuția de substanțe chimice		Întreprinderi care efectuează fabricarea [...] și distribuția de substanțe și [...] **amestecuri** menționate la articolul 3 punctele ([...]), 9 și 14 din Regulamentul (CE) nr. 1907/2006 ([68]) **și întreprinderi care efectuează producția de articole menționate la articolul 3 punctul 3 din același regulament din substanțe și amestecuri**
(4) Producția, prelucrarea și distribuția de alimente		Întreprinderile cu profil alimentar menționate la articolul 3 punctul 2 din Regulamentul (CE) nr. 178/2002 ([69]) **care desfășoară activități de distribuție angro și de producție și prelucrare industrială**
(5) Fabricare	(a) Fabricarea de dispozitive medicale și de dispozitive medicale pentru diagnostic *in vitro*	Entități care fabrică dispozitive medicale menționate la articolul 2 punctul 1 din Regulamentul (UE) 2017/745 ([70]) și entități care fabrică dispozitive medicale pentru diagnostic *in vitro* menționate la articolul 2 punctul 2 din Regulamentul (UE) 2017/746 ([71]), cu excepția entităților care fabrică dispozitive medicale menționate în anexa 1 punctul 5.

68 Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

69 Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului din 28 ianuarie 2002 de stabilire a principiilor și a cerințelor generale ale legislației alimentare, de instituire a Autorității Europene pentru Siguranța Alimentară și de stabilire a procedurilor în domeniul siguranței produselor alimentare (JO L 31, 1.2.2002, p. 1).

70 Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1)

71 Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic *in vitro* și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

	(b) Fabricarea computerelor și a produselor electronice și optice	Întreprinderi care desfășoară una dintre activitățile economice menționate în secțiunea C diviziunea 26 din NACE Rev. 2
	(c) Fabricarea echipamentelor electrice	Întreprinderi care desfășoară una dintre activitățile economice menționate în secțiunea C diviziunea 27 din NACE Rev. 2
	(d) Fabricarea altor mașini și echipamente n.a.p.	Întreprinderi care desfășoară una dintre activitățile economice menționate în secțiunea C diviziunea 28 din NACE Rev. 2
	(e) Fabricarea autovehiculelor, remorcilor și semiremorcilor	Întreprinderi care desfășoară una dintre activitățile economice menționate în secțiunea C diviziunea 29 din NACE Rev. 2
	(f) Fabricarea altor echipamente de transport	Întreprinderi care desfășoară una dintre activitățile economice menționate în secțiunea C diviziunea 30 din NACE Rev. 2
(6) Furnizori digitali		— Furnizori de piețe online
		— Furnizori de motoare de căutare online
		— Furnizori de platforme de servicii de socializare în rețea