Avizul Comitetului Economic și Social European privind „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 2016/1148/UE și Propunerea de directivă a Parlamentului European și a Consiliului privind reziliența entităților critice”

[COM(2020) 823 final – 2020/0359 (COD) – COM(2020) 829 final – 2020/0365 (COD)]

(2021/C 286/28)

Raportor: **Maurizio MENSI**

Sesizare	Parlamentul European, 21.1.2021 – 11.2.2021
	Consiliu, 26.1.2021 – 19.2.2021
Baza procedurală	Articolul 114 din Tratatul privind funcționarea Uniunii Europene
Secțiunea responsabilă	Secțiunea pentru transporturi, energie, infrastructură și societatea informațională
Data adoptării în secțiune	14.4.2021
Data adoptării în sesiunea plenară	27.4.2021
Sesiunea plenară nr.	560
Rezultatul votului	
(voturi pentru/voturi împotrivă/abțineri)	243/0/5

1. **Concluzii și recomandări**

1.1. CESE salută efortul depus de Comisie pentru a spori reziliența entităților publice și private la amenințările ce decurg din atacuri și incidente cibernetice și fizice și este de acord cu necesitatea de a consolida industria și capacitatea de inovare a UE într-un mod favorabil incluziunii, în conformitate cu o strategie bazată pe patru piloni: protecția datelor, drepturile fundamentale, siguranța și securitatea cibernetică.

1.2. CESE observă însă că, date fiind relevanța și caracterul sensibil al obiectivelor urmărite de ambele propuneri, ar fi fost preferabil ca, în locul unei directive, să se opteze pentru un regulament. Cu toate acestea, nu există nicio indicație privind motivele pentru care Comisia nu a considerat această opțiune nici măcar demnă de a fi luată în considerare.

1.3. CESE observă că unele prevederi ale celor două propuneri de directivă se suprapun, dat fiind că sunt strâns legate și complementare, prima abordând mai ales profilurile de securitate cibernetică, iar cealaltă – securitatea fizică. Solicită, ca atare, să se analizeze dacă este posibil ca cele două propuneri să fie reunite într-un singur text, în vederea simplificării și a concentrării funcționale.

1.4. CESE salută propunerea de eliminare a distincției dintre operatorii de servicii esențiale și furnizorii de servicii digitale, prevăzută de Directiva NIS inițială. Cu toate acestea, în ceea ce privește domeniul de aplicare al directivei, Comitetul subliniază că sunt necesare orientări specifice și mai clare pentru identificarea celor care au obligații în temeiul acesteia. În special, criteriile de diferențiere între entități esențiale și importante și cerințele care trebuie îndeplinite ar trebui definite mai precis, pentru a evita abordări divergente la nivel național care să creeze obstacole în calea concurenței și a liberei circulații a bunurilor și serviciilor, cu riscul de a aduce atingere întreprinderilor și de a afecta schimburile comerciale.

1.5. Dată fiind complexitatea obiectivă a sistemului stabilit în cele două propuneri, CESE consideră că este important pentru Comisie să clarifice cu precizie domeniul de aplicare al celor două seturi de norme, mai ales atunci când diverse dispoziții contribuie la reglementarea aceleiași situații sau a aceleiași entități.

1.6. În opinia CESE, claritatea oricărei prevederi normative este un obiectiv esențial, alături de reducerea birocrației și a fragmentării prin simplificarea procedurilor, a cerințelor de siguranță și a cerințelor de raportare a incidentelor. Și din acest motiv, în beneficiul cetățenilor și al întreprinderilor, ar putea fi oportună fuzionarea celor două propuneri de directivă într-un singur text, evitând un exercițiu complicat de interpretare și aplicare.

1.7. CESE recunoaște rolul esențial (subliniat în propunerea de directivă) al organelor de conducere ale entităților esențiale și importante, ai căror membri trebuie să urmeze cursuri de formare specifice în mod regulat, astfel încât să dobândească cunoștințe și competențe suficiente pentru a cunoaște diversele riscuri cibernetice, a le gestiona și a evalua impactul lor. În acest sens, se consideră că propunerea ar trebui să indice conținutul minim al acestor cunoștințe și competențe, pentru a oferi orientări la nivel european cu privire la competențele de formare considerate adecvate și a evita ca cuprinsul diverselor cursuri de formare să difere de la o țară la alta.

1.8. CESE recunoaște importanța esențială a Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) în cadrul instituțional și operațional general al securității cibernetice la nivel european. Consideră, în acest sens, că, pe lângă raportul privind starea securității cibernetice în Uniune, o dată la doi ani, acest organism ar trebui să publice online informații periodice și actualizate despre incidentele de securitate cibernetică, pe lângă fișe informative sectoriale, pentru a oferi un instrument suplimentar de informare util care să le permită părților interesate afectate de NIS 2 să își protejeze mai bine întreprinderile.

1.9. CESE este de acord cu propunerea de a încredința Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) sarcina de a institui un registru european care să înregistreze vulnerabilități și consideră că raportarea lor și a incidentelor majore ar putea deveni obligatorie, mai degrabă decât voluntară, pentru a deveni un instrument util pentru entitățile contractante în cadrul procedurilor de achiziții publice la nivel european, inclusiv pentru produsele și tehnologiile 5G.

2. **Observații generale**

2.1. La 16 decembrie 2020 a fost prezentată noua Strategie de securitate cibernetică a UE, alături de două propuneri legislative: revizuirea Directivei (UE) 2016/1148 ([1]) privind securitatea rețelelor și a sistemelor informatice (NIS 2) și noua Directivă privind reziliența entităților critice (REC). Element-cheie al Comunicării intitulate „Conturarea viitorului digital al Europei" ([2]), al Planului european de redresare și al Strategiei UE privind o uniune a securității, strategia urmărește să consolideze reziliența colectivă a Europei la amenințările cibernetice și să garanteze că toți cetățenii și toate întreprinderile pot beneficia de servicii și instrumente digitale fiabile și sigure.

2.2. Trebuie actualizate măsurile existente la nivelul UE pentru protejarea serviciilor și infrastructurii critice împotriva riscurilor cibernetice și fizice. Riscurile în materie de securitate cibernetică continuă să evolueze, pe măsură ce crește ponderea digitalizării și a interconectării. Ca atare, este necesar să se revizuiască cadrul de reglementare existent, urmând logica Strategiei de securitate a UE și depășind dihotomia dintre online și offline și abordarea bazată pe o strictă compartimentare.

2.3. Cele două propuneri de directivă acoperă o vastă gamă de sectoare și abordează riscurile online și offline existente și potențiale, generate de atacuri cibernetice și infracționale, de dezastre naturale și alte accidente, inclusiv pe baza învățămintelor desprinse din actuala pandemie, care a evidențiat că societățile și economiile ce depind tot mai mult de mediul digital sunt vulnerabile și expuse unor amenințări cibernetice în continuă evoluție și în creștere, mai ales pentru grupurile expuse riscului de excluziune socială, cum ar fi persoanele cu handicap. Ca atare, UE propune acțiuni de protejare a unui spațiu cibernetic global și deschis, dar pe baza unor garanții solide de securitate, suveranitate tehnologică și leadership, prin dezvoltarea unor capacități operaționale de prevenire, de descurajare și de reacție consolidată la posibile amenințări, cu respectarea prerogativelor de securitate națională ce revin statelor membre.

3. **Propunerea de revizuire a Directivei privind securitatea rețelelor și a sistemelor informatice**

3.1. Directiva (UE) 2016/1148 (NIS), prim instrument „orizontal" al UE de reglementare a securității cibernetice, urmărea ameliorarea rezilienței rețelelor și a sistemelor informatice ale Uniunii împotriva riscurilor cibernetice. În pofida unor rezultate bune obținute, Directiva NIS a scos în evidență unele limitări, în condițiile în care transformarea digitală a societății, intensificată de criza COVID-19, a extins gama amenințărilor, accentuând vulnerabilitatea societăților noastre, tot

([1]) JO L 194, 19.7 2016, p. 1.
([2]) COM(2020) 67 final.

mai interdependente de riscuri relevante și neprevăzute. Au apărut noi provocări, ce necesită răspunsuri adecvate și inovatoare. Rezultatele consultării ample cu părțile interesate au evidențiat nivelul insuficient de securitate cibernetică al întreprinderilor europene, aplicarea inconsecventă de către statele membre a normelor în diverse sectoare și lipsă de înțelegere a principalelor amenințări și provocări.

3.2. Propunerea NIS 2 este strâns legată de alte două inițiative: propunerea de regulament privind sectorul finanțelor digitale (Actul privind reziliența operațională digitală a serviciilor financiare – DORA: Digital Operational Resilience Act) și propunerea de directivă privind entitățile critice (REC), care extinde la noi sectoare domeniul de aplicare a Directivei 2008/114/CE ([3]) (de exemplu, la sectorul sănătății și la entitățile care desfășoară activități de cercetare și de dezvoltare farmaceutică). Directiva REC, al cărei domeniu de aplicare sectorial este identic cu cel al Directivei NIS 2 pentru entitățile critice (anexa 1 la Directiva NIS 2), își mută atenția de la protecția activelor fizice la reziliența entităților care le gestionează și de la identificarea infrastructurii critice europene cu dimensiune transfrontalieră la identificarea infrastructurii critice existente la nivel național. NIS 2 se corelează și cu alte instrumente juridice existente, completându-le: Codul european al comunicațiilor electronice, Regulamentul general privind protecția datelor și Regulamentul e-IDAS privind identificarea electronică și serviciile de încredere.

3.3. În conformitate cu Programul privind o reglementare adecvată și funcțională (REFIT), propunerea de directivă NIS 2 urmărește să reducă sarcina de reglementare a autorităților competente și costurile de asigurare a conformității pentru entitățile publice și private și să modernizeze cadrul juridic de referință. Ea consolidează și cerințele de securitate impuse întreprinderilor, abordează securitatea lanțurilor de aprovizionare, simplifică cerințele de raportare, introduce măsuri de supraveghere mai stricte pentru autoritățile naționale și urmărește armonizarea regimurilor de sancțiuni din statele membre.

3.4. De asemenea, NIS 2 contribuie, la intensificarea schimbului de informații și a cooperării privind gestionarea crizelor cibernetice la nivel național și european. Este eliminată distincția dintre operatorii de servicii esențiale și furnizorii de servicii digitale în temeiul Directivei NIS. Domeniul său de aplicare cuprinde întreprinderi mijlocii și mari din sectoarele identificate pe baza importanței lor critice pentru economie și societate. Aceste entități, publice sau private, sunt împărțite în critice și importante, făcând obiectul unor regimuri de supraveghere diferite. Cu toate acestea, rămâne la latitudinea statelor membre să ia în considerare și entitățile mai mici care prezintă profiluri de risc ridicat.

3.5. Se preconizează înființarea unei noi rețele de centre operaționale de securitate bazate pe inteligența artificială (IA) la nivelul UE, care să reprezinte un veritabil „scut de securitate cibernetică”, capabil să detecteze semnalele unui atac cibernetic cu în timp util, astfel încât să se poată interveni înainte de producerea daunelor. Relevanța IA pentru securitatea cibernetică este evidențiată și în raportul privind inteligența artificială (IA) al Comisiei pentru securitate națională a SUA (NSCAI), prezentat la 1 martie 2021. Prin urmare, statele membre și operatorii de infrastructură critică vor avea acces direct la informații privind amenințările în cadrul unei rețele europene de securitate cu informații despre amenințări (Threat Intelligence).

3.6. De asemenea, Comisia abordează problema securității lanțurilor de aprovizionare și a relațiilor cu furnizorii: statele membre, în cooperare cu Comisia și cu ENISA, pot efectua evaluări coordonate ale riscurilor legate de lanțurile de aprovizionare critice, pe baza abordării de succes pentru rețelele 5G, prevăzută în Recomandarea din 26 martie 2019 ([4]).

3.7. Propunerea consolidează și raționalizează obligațiile de securitate și de raportare ale întreprinderilor, prin impunerea unei abordări comune a gestionării riscurilor, cu o listă minimă de elemente de securitate de bază care trebuie aplicate. Există dispoziții mai precise privind procesul de raportare a incidentelor, conținutul rapoartelor și termenele-limită. În acest sens, propunerea prezintă o abordare în două etape: întreprinderile au la dispoziție 24 de ore pentru a prezenta un prim raport de sinteză, urmat de un raport final detaliat în termen de o lună.

([3]) JO L 345, 23.12 2008, p. 75.
([4]) JO L 88, 29.3 2019, p. 42.

3.8. Se prevede ca statele membre să identifice autoritățile naționale responsabile de gestionarea crizelor, sprijinite prin planuri specifice și o nouă rețea de cooperare operațională, „Rețeaua UE a organizațiilor de legătură în materie de crize cibernetice” („EU-CyCLONe”). Este consolidat rolul grupului de cooperare în definirea deciziilor strategice și este creat un registru al vulnerabilităților constatate în UE, gestionat de ENISA. De asemenea, se intensifică schimbul de informații și cooperarea dintre autoritățile statelor membre, inclusiv cea operațională privind gestionarea crizelor cibernetice.

3.9. Sunt introduse măsuri de supraveghere mai stricte pentru autoritățile naționale și cerințe mai stricte de asigurare a respectării legislației și se preconizează armonizarea regimurilor de sancțiuni în toate statele membre.

3.10. În aceste sens, directiva propusă stabilește o listă de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscurilor de securitate informatică și de raportare. Există dispoziții privind răspunderea persoanelor fizice cu funcții de reprezentare sau de conducere în întreprinderile care intră în domeniul de aplicare al directivei. În acest context, propunerea îmbunătățește modul în care UE previne și gestionează incidentele și crizele de securitate cibernetică de mare amploare, reacționând la ele, cu responsabilități clare, o planificare adecvată și o cooperare consolidată la nivelul UE.

3.11. Propunerea permite statelor membre să monitorizeze în comun punerea în aplicare a normelor UE, să se sprijine reciproc în cazul unor probleme transfrontaliere, să stabilească un dialog mai structurat cu sectorul privat, să coordoneze cartografierea vulnerabilităților programelor informatice și de hardware comercializate pe piața internă și să evalueze riscurile de securitate și amenințările legate de noile tehnologii, așa cum s-a întâmplat în cazul tehnologiei 5G.

4. **Propunerea de directivă privind reziliența entităților critice**

4.1. UE a instituit în 2006 Programul european pentru protecția infrastructurii critice (PEPIC), adoptând în 2008 Directiva privind infrastructurile critice europene (ICE), care se aplică în sectoarele energiei și transporturilor. Atât Strategia UE privind o uniune a securității 2020-2025 ([5]), adoptată de Comisia Europeană, cât și Agenda privind combaterea terorismului, adoptată recent, subliniază importanța garantării rezilienței infrastructurii critice la riscurile fizice și digitale. Cu toate acestea, atât evaluarea efectuată în 2019 a punerii în aplicare a Directivei privind ICE, cât și constatările evaluării impactului prezentei propuneri au arătat că măsurile existente la nivel european și național nu garantează în mod suficient că operatorii pot contracara riscurile actuale. Ca atare, Consiliul și Parlamentul solicită Comisiei să revizuiască abordarea actuală în materie de protecție a infrastructurii critice.

4.2. Strategia UE privind o uniune a securității, adoptată de Comisie la 24 iulie 2020, a recunoscut creșterea interconectării și interdependenței infrastructurilor fizică și digitală, subliniind necesitatea unei abordări mai coerente și mai consecvente între Directiva privind ICE și Directiva NIS. În acest sens, directiva propusă (REC), a cărei referință obiectivă este identică cu NIS 2 privind entitățile esențiale, extinde domeniul de aplicare al Directivei 2008/114/CE, limitat inițial la energie și transporturi, la următoarele sectoare: bănci, infrastructurile pieței financiare, sănătate, apă potabilă, ape reziduale, infrastructură digitală, administrație publică și spațiu, stabilind inclusiv responsabilități clare, o planificare adecvată și cooperare consolidată. În acest sens, ar trebui stabilit un cadru de referință pentru toate riscurile, iar statele membre ar trebui sprijinite în eforturile lor de a garanta că actorii critici sunt capabili să prevină incidentele, să le reziste și să le gestioneze impactul, indiferent dacă riscurile sunt generate de pericole naturale, accidente, terorism, de amenințări interne sau de urgențe în materie de sănătate publică, cum se întâmplă în prezent.

4.3. Fiecare stat membru trebuie să adopte o strategie națională pentru a asigura reziliența entităților critice, să efectueze evaluări periodice ale riscurilor și, pe această bază, să identifice entitățile critice. Entitățile critice sunt obligate și să evalueze riscuri, să ia măsuri tehnice și organizatorice adecvate pentru a spori reziliența și să semnaleze incidentele autorităților naționale. Entitățile care furnizează servicii pentru cel puțin o treime din statele membre sau fac obiectul unei supravegheri specifice în cel puțin o treime din ele, inclusiv pentru misiuni de asistență specifice ale Comisiei, care le vizează.

4.4. Directiva propusă (REC) prevede diverse forme de sprijin pentru statele membre și entitățile critice, o prezentare generală a riscurilor la nivelul UE, bune practici și metodologii, acțiuni de formare și exerciții care să testeze reziliența entităților critice. Sistemul de cooperare transfrontalieră prevede și un grup ad-hoc de experți, Grupul pentru reziliența entităților critice, un forum de cooperare strategică și pentru schimb de informații între statele membre.

([5]) COM(2020) 605 final.

5. **Propuneri de modificare a propunerii legislative supuse examinării**

5.1. CESE salută efortul depus de Comisie pentru a spori reziliența entităților publice și private la amenințările ce decurg din atacuri cibernetice și fizice. Acest aspect este deosebit de însemnat și de relevant, mai ales având în vedere transformarea digitală rapidă provocată de epidemia de COVID-19. De asemenea, Comitetul este de acord, că – așa cum se menționează în comunicarea „Conturarea viitorului digital al Europei" – Europa ar trebui să fructifice avantajele erei digitale și să-și consolideze industria (îndeosebi IMM-urile) și capacitatea de inovare într-un mod favorabil incluziunii, în conformitate cu o strategie bazată pe patru piloni: protecția datelor, drepturi fundamentale, siguranță și securitate cibernetică, ca premise esențiale pentru o societate bazată pe date.

5.2. Cu toate acestea, în lumina rezultatelor evaluării impactului și ale consultării care a precedat propunerea NIS 2, dat fiind obiectivul subliniat în repetate rânduri de a evita fragmentarea normelor adoptate la nivel național, astfel cum s-a solicitat și în Comunicarea din 4 octombrie 2017 privind punerea în aplicare a Directivei NIS ([6]), CESE constată că nu se deduc motivele pentru care Comisia nu a considerat oportun să propună adoptarea unui regulament în locul unei directive, chiar și numai printre opțiunile luate în considerare.

5.3. CESE observă că unele prevederi ale celor două propuneri de directivă se suprapun, dat fiind că sunt strâns legate și complementare, prima abordând mai ales profilurile de securitate cibernetică, iar cealaltă – securitatea fizică. De asemenea, ar trebui remarcat că entitățile critice menționate în SEC acoperă aceleași sectoare și coincid cu entitățile esențiale menționate în NIS 2 ([7]). În plus, toate entitățile critice acoperite de SEC sunt supuse obligațiilor NIS 2 în materie de securitate cibernetică. Cele două propuneri prevăd o serie de clauze-pasarelă pentru a asigura legătura: dispoziții pentru o cooperare consolidată între autorități, schimb de informații cu privire la activitățile de supraveghere, notificări adresate autorităților competente pentru NIS 2 privind identificarea entităților critice în conformitate cu REC, precum și reuniuni regulate ale grupurilor de cooperare (cel puțin o dată pe an). Cele două propuneri împart și același temei juridic, și anume articolul 114 din TFUE, care vizează funcționarea pieței interne prin apropierea standardelor naționale, așa cum au fost interpretate *ex multis* de Curtea de Justiție a UE în hotărârea sa în cauza C-58/08, Vodafone și alții. Prin urmare, este nevoie să se analizeze dacă cele două propuneri ar trebui să fie reunite într-un singur text, în interesul simplificării și al concentrării funcționale.

5.4. CESE salută eliminarea distincției dintre operatorii de servicii esențiale și furnizorii de servicii digitale, prevăzută de Directiva NIS inițială. Cu toate acestea, în ceea ce privește domeniul său de aplicare, Comitetul subliniază că sunt necesare orientări specifice și mai clare pentru identificarea celor care au obligații în temeiul directivei. Alături de trimiterile din anexele I și II, NIS 2 se referă la o serie de criterii diferite între ele, care implică evaluări calitative și cantitative sensibile aplicabile în mod diferit la nivel național, ceea ce ar implica riscul de a da naștere din nou unei situații fragmentate, pe care măsura legislativă supusă atenției urmărea tocmai să o evite. Este important să se evite abordările divergente la nivel național care să conducă la obstacole în calea concurenței și a liberei circulații a bunurilor și serviciilor, cu riscul de a prejudicia întreprinderile și de a afecta schimburile comerciale.

5.5. Directiva NIS 2 prevede că operatorii critici din sectoarele considerate „esențiale" de prezenta propunere fac și obiectul unor obligații generale de consolidare a rezilienței, cu un accent deosebit pe riscurile non-cibernetice în termenii Directivei REC. Cu toate acestea, acesta din urmă precizează în mod expres că nu se aplică aspectelor acoperite de NIS 2. Într-adevăr, REC prevede că, întrucât securitatea cibernetică este abordată în mod suficient în Directiva NIS 2, aspectele reglementate de aceasta ar trebui excluse din domeniul de aplicare al Directivei REC, fără a prejudicia regimul special aplicabil entităților din sectorul infrastructurii digitale. În continuare, REC observă că entitățile din domeniul infrastructurii digitale se bazează în principal pe rețele și sisteme informatice și intră în domeniul de aplicare al Directivei NIS 2, care abordează și securitatea fizică a unor astfel de sisteme, ca parte a obligațiilor lor de a gestiona riscurile și de a raporta în materie de securitate cibernetică. În același timp, textul arată că nu este exclus ca unele dispoziții specifice ale REC să li se poată aplica.

5.6. Ca atare, în acest cadru complex, CESE consideră că este esențial pentru Comisie să clarifice domeniul de aplicare al celor două seturi de norme, în special în cazul în care dispozițiile reglementează aceleași situații sau aceleași entități.

5.7. Claritatea oricărei dispoziții legislative, cu atât mai mult când face parte din texte ample și articulate – cum este cel de față – trebuie să fie un obiectiv esențial la toate nivelurile, alături de reducerea birocrației și a fragmentării, prin simplificarea procedurilor, a cerințelor de siguranță și a cerințelor de raportare a incidentelor. De asemenea, ar trebui să se

([6]) COM(2017) 476 final.
([7]) Anexa 1 (JO L 194, 19.7.2016, p. 1).

evite ca multiplicarea organismelor înființate pentru misiuni specifice să compromită identificarea clară a propriilor competențe și să submineze obiectivele urmărite. Și din acest motiv, în beneficiul cetățenilor și al întreprinderilor, ar putea fi oportună fuzionarea celor două propuneri de directivă într-un singur text, evitând astfel un exercițiu de interpretare și de aplicare care se poate dovedi uneori complicat.

5.8. În mai multe locuri, Directiva NIS 2 se referă la dispoziții din alte instrumente juridice, cum ar fi Directiva (UE) 2018/1972 ([8]) de instituire a Codului european al comunicațiilor electronice, a cărei aplicare este reglementată de criteriul specialității. Anumite dispoziții ale acestei directive sunt abrogate explicit (articolele 40 și 41), în timp ce altele trebuie să se aplice conform aceluiași principiu, fără nicio precizare în acest sens. În această privință, CESE speră că orice îndoială va fi înlăturată, pentru a evita problemele de interpretare. În ceea ce privește sistemul de sancțiuni, CESE sprijină și obiectivul Comisiei de a armoniza regimul acestora în caz de nerespectare a gestionării riscurilor, în contextul unui schimb de informații și al unei cooperări îmbunătățite la nivelul UE.

5.9. CESE recunoaște rolul esențial (subliniat în propunerea de directivă) în strategia de securitate cibernetică și în gestionarea riscurilor al organelor de conducere ale entităților esențiale și importante, întrucât acestea trebuie să aprobe măsurile de gestionare a riscurilor, să supravegheze punerea lor în aplicare și să reacționeze la orice eventuală neconformitate. În acest sens, se prevede ca membrii acestor organisme să urmeze regulat cursuri de formare specifice, astfel încât să dobândească cunoștințe și competențe suficiente, pentru a cunoaște diversele riscuri cibernetice, a le gestiona și a evalua impactul lor. Cu toate acestea, se consideră că propunerea ar trebui să indice conținutul acestor cunoștințe și competențe, astfel încât să fie oferite orientări la nivel european cu privire la competențele de formare considerate adecvate, pentru a răspunde cerințelor indicate în propunere și a evita ca diversele cursuri de formare să fie diferite în conținut de la o țară la alta.

5.10. CESE recunoaște importanța esențială a Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) în cadrul instituțional și operațional general al securității cibernetice la nivel european. În acest sens, consideră că, pe lângă raportul privind starea securității cibernetice în Uniune, acest organism ar trebui să publice online informații actualizate despre incidentele de securitate cibernetică, pe lângă fișe informative sectoriale, pentru a oferi un instrument suplimentar de informare util care să le permită părților interesate afectate de NIS 2 să își protejeze mai bine întreprinderile.

5.11. CESE împărtășește opinia că accesul în timp util la informații corecte cu privire la vulnerabilitățile produselor și serviciilor TIC contribuie la o mai bună gestionare a riscului în materie de securitate informatică. În această privință, sursele de informații accesibile publicului cu privire la vulnerabilități reprezintă un instrument important atât pentru autoritățile naționale competente, CSIRT, cât și pentru întreprinderi și utilizatori. Din acest motiv, CESE sprijină propunerea de a încredința ENISA sarcina de a institui un registru european al vulnerabilităților, unde entitățile esențiale și importante și furnizorii lor să poată transmite informații, astfel încât utilizatorii să poată lua măsuri adecvate de atenuare. Consideră, însă, că transmiterea acestor informații, cu privire la vulnerabilități și incidente majore, ar trebui să fie obligatorie, mai curând decât voluntară, pentru a deveni un instrument util și pentru entitățile contractante în contextul diverselor proceduri de achiziții la nivel european, inclusiv al produselor și tehnologiilor 5G. Un astfel de registru ar cuprinde elemente utilizabile pentru evaluarea ofertelor, în scopul verificării calității lor și a fiabilității contractanților europeni și neeuropeni, din perspectiva securității produselor și serviciilor care fac obiectul procedurii de ofertare, în conformitate cu recomandarea privind securitatea cibernetică a rețelelor 5G din 26 martie 2019. Registrul ar trebui să garanteze și că informațiile conținute sunt puse la dispoziție într-un mod care să evite orice fel de discriminare.

Bruxelles, 27 aprilie 2021.

Președinta
Comitetului Economic și Social European
Christa SCHWENG

([8]) JO L 321, 17.12.2018, p. 36.