Avizul Comitetului Economic și Social European privind Comunicarea comună către Parlamentul European și Consiliu pe tema „Politica UE în domeniul apărării cibernetice”

(aviz din proprie inițiativă)

(2023/C 293/04)

Raportor: **Anastasis YIAPANIS**

Coraportor: **Alberto MAZZOLA**

Decizia Adunării plenare	20.9.2022
Temei juridic	Articolul 52 alineatul (2) din Regulamentul de procedură
	Aviz din proprie inițiativă
Secțiunea competentă	Comisia consultativă pentru mutații industriale (CCMI)
Data adoptării în secțiune	27.3.2023
Data adoptării în sesiunea plenară	14.6.2023
Sesiunea plenară nr.	579
Rezultatul votului	
(voturi pentru/voturi împotrivă/abțineri)	208/1/2

1. **Concluzii și recomandări**

1.1. Comitetul Economic și Social European sprijină propunerea de politică a UE în domeniul apărării cibernetice, dar s-ar fi așteptat ca societății civile organizate să i se acorde un rol mai important în elaborarea acestor propuneri. Comitetul consideră că, în acest moment, este dificil de evaluat dacă viitoarele inițiative prezentate în comunicarea comună vor fi puse în aplicare și vor obține rezultatele preconizate. Acesta îndeamnă instituțiile UE și statele membre să acorde prioritate inițiativelor anunțate și să avanseze rapid în acest sens.

1.2. CESE subliniază necesitatea unor măsuri suplimentare pentru a spori capacitatea UE de a detecta amenințările cibernetice și solicită ca finanțarea C&D să fie direcționată către dezvoltarea capacităților de vârf ale UE. Cooperarea dintre sectorul privat și cel public este esențială și nu trebuie să fie unidirecțională. CESE consideră că este necesară coordonarea la nivelul UE pentru a aborda fragmentarea și a asigura cooperarea și investițiile comune între statele membre.

1.3. CESE sprijină crearea Centrului UE de coordonare a apărării cibernetice (EUCDCC) și recomandă statelor membre să se angajeze să asigure un răspuns rapid 24 de ore pe zi, șapte zile pe săptămână și să evalueze gradul de pregătire în materie de securitate cibernetică și performanța mecanismelor UE de răspuns la crizele cibernetice, cu accent atât pe capacitățile militare, cât și pe sectoarele critice, astfel cum sunt identificate în Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([1]) (Directiva NIS 2). Comitetul sprijină extinderea mandatului Centrului european de competențe în materie de securitate cibernetică (ECCC) pentru a sprijini activitatea Centrului UE de coordonare a apărării cibernetice.

1.4. Pentru a consolida autonomia strategică și suveranitatea Uniunii în materie de securitate cibernetică, CESE consideră că ar trebui dezvoltată sau adoptată din sectorul privat o platformă dinamică de testare și schimb de informații în timp real, pentru a identifica lacunele actuale în ceea ce privește capacitățile existente. Aceasta poate fi utilizată și pentru schimbul de bune practici, pentru raportarea incidentelor cibernetice și pentru crearea unei liste a UE a tuturor infractorilor cibernetici.

([1]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 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 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

1.5. CESE subliniază necesitatea unei mai bune pregătiri împotriva atacurilor cibernetice, cum ar fi cele comise de Rusia în Ucraina, care vizează în special infrastructura critică. Cooperarea dintre ecosistemele civile și militare este esențială pentru gestionarea eficace a crizelor, pentru interoperabilitate și pentru evitarea duplicării eforturilor și a investițiilor, inclusiv prin simularea unor atacuri cibernetice de testare.

1.6. CESE consideră că investițiile în apărarea cibernetică ar trebui să acorde prioritate protecției cetățenilor UE și infrastructurii critice, printre altele prin alegerea unor furnizori fiabili de hardware și software. Comitetul insistă asupra actualizării la timp a priorităților și a investițiilor, care urmează să fie convenite de UE și de statele membre, cu participarea părților interesate private relevante.

1.7. UE trebuie să păstreze și să dezvolte capacitățile necesare pentru a-și securiza economia digitală, societatea, democrația și tehnologiile critice și pentru a furniza servicii esențiale de securitate cibernetică. Pentru a asigura autonomia strategică a UE, reducerea dependenței de țările terțe este vitală. CESE consideră că este esențial ca UE să adopte o abordare pe termen mediu în ceea ce privește autonomia în domeniul tehnologiilor-cheie și pledează ferm pentru crearea unor centre de cercetare și de producție de către întreprinderi cu sediul în UE, care urmează o politică industrială europeană adecvată, axată pe un ecosistem cibernetic autonom.

1.8. IMM-urile ar trebui să beneficieze de sprijin specific și să aibă acces la programe de finanțare care să le sporească reziliența la atacurile cibernetice, precum și la oportunități de asistență, de formare și de educație privind riscurile cibernetice și apărarea împotriva acestora. UE ar trebui să ofere un mecanism de stimulare care să încurajeze familiarizarea progresivă a IMM-urilor și dezvoltarea IMM-urilor inovatoare.

1.9. CESE sprijină planul de înființare a unei Academii de competențe în domeniul cibernetic și solicită Comisiei să coordoneze și să finanțeze programe de învățământ și formare profesională la scară largă care să implice toate statele membre și să vizeze crearea unei forțe de muncă calificate pentru toate agențiile și organizațiile implicate în apărarea cibernetică, precum și pentru rețelele civile private.

1.10. Comitetul consideră că sensibilizarea cetățenilor cu privire la securitatea cibernetică este esențială pentru reducerea expunerii la atacurile cibernetice și solicită programe de învățământ în domeniul securității cibernetice și programe de formare pe tot parcursul vieții care să se concentreze pe îmbunătățirea competențelor și cunoștințelor în domeniul cibernetic. CESE sprijină integrarea securității cibernetice în toate politicile publice viitoare ale UE și informarea publicului larg cu privire la amenințările cibernetice.

1.11. CESE consideră că o cooperare strânsă cu aliații NATO în domeniile militare trebuie să se concentreze pe coordonarea și reciprocitatea deplină, pe proiecte comune de C&D&I, pe schimbul de bune practici, pe programe ample de formare și pe simulări de atacuri cibernetice, obiectivul principal fiind extinderea capacității comune de răspuns.

1.12. Comitetul invită Înaltul Reprezentant să examineze dialogurile bilaterale actuale în domeniul cibernetic și să se angajeze în discuții suplimentare cu alte țări și cu organizațiile internaționale relevante pentru a stabili un cadru mondial pentru aderarea la dreptul internațional în spațiul cibernetic, cu o atenție specială acordată reciprocității. Comitetul consideră că UE este în măsură să preia inițiativa în cadrul discuțiilor internaționale privind viitorul securității cibernetice, în special în cadrul Organizației Națiunilor Unite, întrucât are o bază solidă în ceea ce privește libertățile democratice fundamentale.

1.13. UE ar trebui să adopte o poziție fermă împotriva oricărui tip de sistem de atribuire a unui punctaj social împotriva cetățenilor. CESE clarifică faptul că adevărata democrație nu poate exista fără o protecție eficace a datelor cu caracter personal și consideră că gestionarea responsabilă și eficace a datelor este esențială pentru a transforma hiperconectivitatea într-un avantaj concurențial.

2. **Introducere și observații generale**

2.1. Expansiunea digitală a societăților este însoțită de un număr mare de amenințări la adresa securității cibernetice generate de modernizările tehnologice. În ultimii ani, atacurile cibernetice au crescut semnificativ ca număr și complexitate, subminând atât securitatea entităților publice, cât și a celor private. Indiferent dacă vorbim despre ransomware, programe malware, atacuri prin e-mail, încălcarea securității datelor, dezinformare, atacuri DDoS (*Distributed Denial of Service* – atacuri distribuite de refuzare a serviciilor) sau despre alte forme de atacuri, toate acestea reprezintă o amenințare constantă și continuă la adresa securității UE în ansamblu.

2.2. CESE salută comunicarea comună privind *Politica UE în domeniul apărării cibernetice* ([2]) și consideră că acum este momentul să se acționeze cu celeritate și în mod coordonat la nivelul UE, implicând atât ecosistemele civile, cât și cele militare ale spațiului cibernetic și asigurând cadrul adecvat de investiții pentru capacitățile de apărare cibernetică. Cu toate acestea, Comitetul observă că comunicarea nu este decât o declarație de intenție și o listă a viitoarelor inițiative ale UE care ar trebui să dea rezultate și consideră că este imposibil să se evalueze dacă aceste angajamente viitoare vor fi efectiv puse în aplicare, întrucât viitoarele negocieri dintre colegiuitori vor influența în mod natural rezultatul final al planului de acțiune al UE în materie de securitate cibernetică.

2.3. Atacul Rusiei asupra rețelei de sateliți KA-SAT, care a perturbat comunicarea dintre forțele militare ucrainene și recentul scandal în care Éric Léandri a fost contractat de unele companii de apărare pentru spionaj cibernetic în folosul lor, plasează securitatea cibernetică în fruntea listei amenințărilor de securitate din UE. Deși RGPD este o parte solidă a legislației UE și este în vigoare de mai mulți ani, este clar că volumul tot mai mare de date disponibile este vulnerabil, iar riscul ca terții să treacă granița legalității crește în fiecare zi.

2.4. Având în vedere caracterul transnațional al atacurilor cibernetice, coordonarea UE este necesară pentru a reduce fragmentarea actuală și a se asigura că statele membre sunt pregătite să coopereze și să investească în comun. Acest lucru este deosebit de important pentru cazurile viitoare în care un stat membru ar putea fi vizat și toate celelalte ar trebui să aibă posibilitatea de a oferi sprijin imediat.

3. **Acțiuni comune pentru o apărare cibernetică mai puternică**

3.1. Comitetul ia act de inițiativele ambițioase anunțate de a înființa un Centru de coordonare a apărării cibernetice al UE, de a dezvolta proiectul CyDEf-X, de a crea echipe de răspuns cibernetic rapid, de a elabora o inițiativă a UE privind solidaritatea cibernetică și de a explora dezvoltarea unor sisteme de certificare a securității cibernetice pentru produsele, serviciile și procesele TIC. CESE recomandă ca toate statele membre să se angajeze să fie pregătite să ofere un răspuns rapid 24 de ore pe zi, șapte zile pe săptămână, Centrul de coordonare al UE fiind implicat în evaluarea și elaborarea de rapoarte periodice privind gradul de pregătire în materie de securitate cibernetică al statelor membre și eficacitatea mecanismului european de răspuns la crizele cibernetice, concentrându-se atât asupra capacităților militare, cât și asupra sectoarelor critice identificate de Directiva NIS 2. Fiecare stat membru ar trebui să dispună de specialiști special instruiți pentru a interveni în cazul unor incidente cibernetice și ar trebui să-și testeze în mod regulat capacitatea de intervenție în alte state membre.

3.2. Deși comunicarea oferă o listă lungă de îmbunătățiri pas cu pas, CESE ar fi sperat să vadă o foaie de parcurs explicită privind punerea în aplicare a acestor inițiative, cu o guvernanță clară și termene de depunere și de adoptare clare. În plus, Comitetul s-ar fi așteptat ca societății civile organizate să i se acorde un rol mai important în elaborarea acestor propuneri.

3.3. CESE consideră că statele membre trebuie să-și consolideze capacitatea internă de a contracara amenințările cibernetice, implicându-se totodată în proiecte de cooperare și făcând schimb de informații și de bune practici cu omologii lor din alte state membre. Este nevoie de investiții rapide în capacitățile de apărare cibernetică și de implementarea accelerată de tehnologii ([3]) în toate statele membre și de o pregătire comună pentru detectarea și redresarea în urma atacurilor cibernetice, precum și pentru apărarea împotriva acestora. Pentru a sprijini autonomia în materie de securitate cibernetică a Uniunii, Comitetul consideră că trebuie dezvoltată sau adoptată din sectorul privat o platformă dinamică de testare și schimb de informații în timp real, axată pe identificarea capacităților care lipsesc în prezent.

3.4. CESE este de acord că, în acest stadiu, operațiunile militare din spațiul cibernetic ar trebui să rămână strict de competența statelor membre; Comitetul sprijină cooperarea anunțată între echipele militare de intervenție în caz de urgență informatică ale UE (milCERT), echipele de răspuns la incidente de securitate informatică (CSIRT) și Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE).

3.5. Directiva NIS 2 și Directiva privind reziliența entităților critice (CER) ([4]) recent adoptate au instituit deja obligații naționale și sectoriale specifice pentru cadrul UE de apărare cibernetică. Sunt necesare acțiuni suplimentare pentru a îmbunătăți capacitatea de detectare colectivă a UE, iar CESE solicită investiții în C&D pentru dezvoltarea capacităților de vârf ale UE.

([2]) Comunicarea comună privind politica UE în domeniul apărării cibernetice.
([3]) De exemplu, inițiativa Acceleratorul de inovare în domeniul apărării pentru Atlanticul de Nord (DIANA) al NATO.
([4]) Directiva privind reziliența entităților critice.

4. **Securizarea ecosistemului de apărare al UE**

4.1. CESE consideră că complexitatea inerentă și provocările tehnologice care evoluează rapid au transformat ecosistemul de apărare și că securitatea cibernetică a devenit un subiect comun atât pentru sectorul militar, cât și pentru cel civil, precum și pentru cetățenii UE. Cooperarea dintre ecosistemele civile și militare este acum mai importantă ca niciodată și ar trebui să aducă beneficii în ceea ce privește gestionarea mai eficientă a crizei, precum și progresul continuu și interoperabilitatea, evitând dublarea sau multiplicarea acelorași eforturi și investiții. Statele membre ar trebui să fie pregătite să efectueze teste de rezistență la nivelul infrastructurilor critice naționale pentru a evalua și a spori reziliența la viitoare atacuri cibernetice.

4.2. CESE consideră că investițiile în apărarea cibernetică ar trebui orientate cu prioritate către protecția cetățenilor UE și a infrastructurii critice a UE. Având în vedere evoluția rapidă a transformării digitale și a peisajului amenințărilor, Comitetul solicită insistent ca UE și statele membre să ajungă la un acord în timp util cu privire la actualizarea priorităților și a investițiilor, pe baza unei consultări temeinice a părților interesate private relevante. Adesea, dispozitivele oferite de internetul obiectelor (IoT) nu sunt la fel de bine protejate ca dispozitivele tradiționale, iar CESE solicită asigurarea unui nivel minim de securitate prin intermediul platformelor de IDAM (*identity & access management* – management al identității și al accesului). De asemenea, întrucât certificarea este o metodă esențială de asigurare a unui nivel mai ridicat de securitate, Comitetul solicită ca noua abordare a certificării UE să pună un accent mai mare pe securitatea IoT.

4.3. UE trebuie să consolideze reziliența la atacurile cibernetice și să creeze o disuasiune eficientă în spațiul cibernetic. Infrastructura critică trebuie să fie protejată împotriva atacurilor cibernetice de orice fel, inclusiv din partea sistemelor de apărare ale UE. Comitetul consideră că este în interesul strategic al UE să se asigure că Uniunea își păstrează și dezvoltă capacitățile esențiale pentru a-și securiza economia digitală, societatea și democrația, pentru a obține suveranitatea digitală deplină, ca singura modalitate de a proteja tehnologiile critice, și de a furniza servicii eficiente de securitate cibernetică. Reducerea dependenței de țările terțe este, de asemenea, vitală pentru autonomia strategică a UE. CESE consideră că agențiile sectoriale ale UE (ENISA, AESA, ERA, EMA, ABE, AES, HADEA etc.) ar trebui să fie implicate în proces și să ofere orientări în ceea ce privește dezvoltarea sistemelor de securitate cibernetică.

4.4. Pandemia de COVID-19 a accelerat tranziția digitală și a transformat munca tradițională în muncă hibridă și/sau la distanță, creând noi relații de muncă și așteptări, precum și o nouă clasă de nomazi digitali, al căror număr este în creștere. CESE ia notă de schimbările rapide de pe piața forței de muncă, care au dus la adoptarea arhitecturii de tip „încredere zero" de către întreprinderi, prin intermediul soluțiilor IAM (managementul identității și accesului) și PAM (managementul accesului privilegiat). Comitetul consideră că acest tip de gestionare a resurselor întreprinderilor aduce noi soluții legate de amenințările cibernetice și consideră că sectorul privat trebuie sprijinit în consolidarea nivelului de securitate al soluțiilor lor digitale inovatoare.

4.5. CESE este întrucâtva dezamăgit de afirmația Comisiei potrivit căreia „[î]n cooperare cu statele membre, ar putea fi stabilit un plan de punere în aplicare" și consideră că un astfel de plan de punere în aplicare este obligatoriu. Comitetul consideră că acesta ar trebui elaborat în comun cu statele membre și pus în aplicare cât mai curând cu putință. Comitetul își exprimă îngrijorarea cu privire la poziția relaxată adoptată de Comisie și îndeamnă instituțiile UE și statele membre să faciliteze realizarea de progrese rapide în ceea ce privește inițiativele anunțate.

5. **Investiții în capabilitățile de apărare cibernetică**

5.1. Pe măsură ce dezvoltarea tehnologică avansează rapid, spațiul cibernetic a devenit cel mai nou teren de război, după uscat, mare, aer și spațiu. Aceasta a creat, de asemenea, posibilități ample de activități infracționale pentru actorii cibernetici răuvoitori, de la hackeri independenți la infractori profesioniști și chiar actori statali.

5.2. Investițiile în C&D sunt vitale, iar CESE salută fondurile specifice existente în cadrul programului „Europa digitală", al Fondului european de apărare, al programului Orizont Europa și al programelor naționale de redresare. Cu toate acestea, Comitetul ar aprecia mai multe proiecte transnaționale care să se axeze pe cooperarea și interoperabilitatea dintre sistemele de apărare cibernetică din toate statele membre, precum și mai multe sinergii între instrumentele de finanțare, în special cele care însoțesc IMM-urile inovatoare.

5.3. După cum se anunța în Strategia de securitate cibernetică a UE în 2020, Comitetul ia act de faptul că termenul pentru crearea unității cibernetice comune este anul acesta și așteaptă informații cu privire la finalizarea procesului și la pregătirea UE pentru a răspunde la incidentele cibernetice de mare amploare. CESE se așteaptă ca aceasta să îmbunătățească nivelul de cunoaștere a situației la nivelul UE și capacitatea globală de răspuns și de redresare.

5.4. CESE sprijină prelungirea mandatului ECCC pentru a sprijini activitatea Centrului UE de coordonare a apărării cibernetice. În plus, această rețea ar putea sprijini suveranitatea digitală europeană prin dezvoltarea unei baze industriale europene competitive pentru capacități tehnologice cheie, bazată în parte pe activitatea desfășurată prin parteneriate contractuale public-privat (PPP). PPP s-au dovedit a fi cea mai eficientă abordare pentru îmbunătățirea securității cibernetice a întregului ecosistem digital, dar nu poate fi unidirecțională: instituțiile publice trebuie, de asemenea, să partajeze informațiile cu sectorul privat.

5.5. CESE observă că, pentru a aborda viitoarele încercări de piraterie informatică vizând computerele cuantice, UE trebuie să investească imediat în tehnologii de vârf, cum ar fi criptografia postcuantică. Comitetul consideră că este indispensabil ca Europa să adopte o abordare pe termen mediu în ceea ce privește autonomia și pledează ferm pentru dezvoltarea de către întreprinderi cu sediul în UE a unor centre de cercetare și de producție. CESE consideră că este important să se majoreze resursele UE pentru C&I în domeniul digital și să se sprijine investițiile operatorilor și ale furnizorilor în noi funcționalități tehnice de securitate, inclusiv în ceea ce privește noile tendințe, cum ar fi realitatea augmentată și metaversul. În special, este esențial să se construiască o infrastructură europeană distribuită de cloud computing, bazată pe norme europene privind stocarea și prelucrarea datelor ([5]).

5.6. IMM-urilor ar trebui să li se acorde o atenție deosebită și să aibă acces la programe de finanțare care să le sporească gradul de pregătire în fața atacurilor cibernetice, precum și la programe de asistență, de formare și de educație care să le ajute să înțeleagă riscurile cibernetice și modul în care să se protejeze. UE ar trebui să ofere un mecanism de stimulare care să încurajeze familiarizarea progresivă în cazul IMM-urilor.

5.7. Comisia estimează că în prezent lipsa de personal calificat în domeniul securității cibernetice este de jumătate de milion de persoane, iar CESE apreciază propunerea de creare a unei Academii de competențe cibernetice. Este clar că eforturile depuse la nivelul statelor membre nu sunt suficiente pentru a reduce lipsa de personal calificat, astfel încât Comitetul propune ca, odată cu lansarea Academiei, Comisia să valorifice impulsul oferit de Anul european al competențelor să coordoneze și să finanțeze programe de formare și programe EFP la scară largă la nivelul UE, care să implice toate statele membre și se axeze pe furnizarea unei forțe de muncă calificate pentru toate agențiile și organismele implicate în apărarea cibernetică, precum și pentru rețelele civile private. O atenție deosebită trebuie acordată formării forței de muncă, în special în domeniile științei, tehnologiei, ingineriei și matematicii (STIM).

5.8. În plus, CESE consideră că este esențial să se crească gradul de sensibilizare în rândul cetățenilor cu privire la securitatea cibernetică pentru a reduce expunerea la atacuri cibernetice, în special în ceea ce privește infracțiunile cibernetice de bază care vizează populația în general. Comitetul solicită programe de educație în domeniul securității cibernetice și programe de formare pe tot parcursul vieții în domeniul securității cibernetice, care să se concentreze pe îmbunătățirea competențelor cibernetice și să facă securitatea cibernetică mai accesibilă și mai atractivă pentru cetățeni, în special pentru generația tânără. CESE pledează pentru integrarea proceselor de reflecție referitoare la securitate cibernetică în toate viitoarele politici publice ale UE și pentru informarea populației cu privire la amenințările cibernetice, printre altele prin programe de formare gratuite pentru populație în general, aplicații de informare gratuite pentru telefoane mobile sau prin comunicarea în intervale de transmisie TV de maximă audiență. Progresul cultural pe scară largă la fiecare nivel al societății, către o abordare „orientată spre securitatea cibernetică”, trebuie promovat în paralel cu aceste acțiuni.

5.9. CESE consideră că este esențial să se evalueze profilul de risc al furnizorilor și să se aplice restricții relevante celor considerați a prezenta un risc ridicat, incluzând interdicțiile necesare privind activele și aplicațiile esențiale definite ca fiind critice și sensibile în cadrul evaluării coordonate a riscurilor la nivelul UE, precum și certificarea furnizorilor fiabili de hardware și software.

6. **Crearea de parteneriate pentru abordarea provocărilor comune**

6.1. Nivelul de pregătire pentru viitoarele atacuri cibernetice diferă foarte mult de la un stat membru la altul. CESE consideră că primul pas imediat este crearea unei platforme de comunicare în interiorul UE privind cele mai bune practici, în cadrul căreia statele membre cele mai avansate din punct de vedere cibernetic să-și poată partaja cunoștințele și să faciliteze adoptarea lor imediată de către celelalte țări. Acest lucru ar contribui la îmbunătățirea încrederii reciproce între entitățile naționale. În al doilea rând, Comitetul consideră că este necesară o cooperare mai strânsă între actorii statali și nestatali din întreaga UE pentru a îmbunătăți securitatea cibernetică a produselor și serviciilor în interiorul pieței interne. CESE propune, de asemenea, crearea unei platforme comune la nivelul UE pentru raportarea incidentelor cibernetice, inclusiv o listă neagră a UE cu toți activiștii din domeniul criminalității cibernetice.

([5]) De exemplu, inițiativa franco-germană Gaia-X.

6.2. CESE este de părere că o cooperare strânsă cu aliații noștri din NATO în domeniul militar trebuie să se concentreze nu numai pe consolidarea capacităților și detectarea timpurie, ci și pe proiecte comune de C&D&I, schimbul de bune practici și schimburi între experți, programe de formare de mare amploare și simulări de atacuri cibernetice. Conform cu declarațiile comune de la Varșovia din 2016 și de la Bruxelles din 2018, obiectivul principal ar trebui să fie extinderea capacității comune de răspuns și crearea de sinergii pentru combaterea viitoarelor amenințări hibride. Cooperarea dintre UE și NATO încă dispune de o serie de căi care pot fi exploatate, iar înregistrarea unor progrese imediate în acest domeniu poate determina schimbări reale în ceea ce privește asigurarea securității cetățenilor noștri și a societăților noastre.

6.3. Comitetul consideră că discuțiile la nivel mondial și cu partenerii noștri internaționali ar trebui să pună bazele promovării unui spațiu cibernetic global și deschis, care să protejeze drepturile omului, libertățile fundamentale și statul de drept și să se concentreze pe dezvoltarea unor standarde internaționale obligatorii în sectoarele cu dezvoltare digitală rapidă. CESE recomandă Înaltului Reprezentant să revizuiască dialogurile bilaterale existente în domeniul cibernetic și să se angajeze în negocieri suplimentare cu alte țări și cu organizațiile internaționale relevante pentru a promova un cadru global pentru aplicarea dreptului internațional în spațiul cibernetic, bazat pe o condiție strictă de reciprocitate.

6.4. În cele din urmă, Comitetul consideră că UE este cea mai în măsură să conducă dezbaterile internaționale privind viitorul securității cibernetice, în special în cadrul discuțiilor de la nivelul ONU, datorită fundamentului său solid, bazat pe libertățile democratice fundamentale. De asemenea, UE trebuie să se angajeze în combaterea regimurilor totalitare care practică monitorizarea datelor cetățenilor și care le încalcă drepturile și libertățile și ar trebui să se poziționeze ferm împotriva oricărui tip de sistem de atribuire a unui punctaj social îndreptat împotriva cetățenilor. CESE susține cu fermitate că adevărata democrație nu poate exista fără o protecție eficace a datelor cu caracter personal și consideră că gestionarea responsabilă și eficace a datelor este vitală pentru a transforma hiperconectivitatea într-un activ.

Bruxelles, 14 iunie 2023.

Președintele
Comitetului Economic și Social European
Oliver RÖPKE