



PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

HOTĂRÂRE

privind adoptarea opiniei referitoare la Comunicarea comună către Parlamentul European și Consiliu - Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE
JOIN(2017)450

În temeiul prevederilor art. 67 și ale art. 148 din Constituția României, republicată, ale Legii nr. 373/2013 privind cooperarea dintre Parlament și Guvern în domeniul afacerilor europene și ale art. 160 - 185 din Regulamentul Camerei Deputaților, aprobat prin Hotărârea Camerei Deputaților nr. 8/1994, republicat, cu modificările și completările ulterioare,

Camera Deputaților adoptă prezenta hotărâre.

Articol unic. – Luând în considerare opinia nr. 4c-19/461 adoptată de Comisia pentru afaceri europene, în ședința din 15 noiembrie 2017, Camera Deputaților:

1. Apreciază și consideră benefică atitudinea Comisiei și a celorlalte instituții europene cu privire la măsurile necesare în domeniul securității cibernetice, cu atât mai mult luând în considerare magnitudinea pachetului de măsuri și a comunicărilor propuse. Consideră că acest ritm trebuie menținut și dezvoltat în continuare, inclusiv prin măsuri specifice adoptate la nivel național de către statele membre.

2. Susține poziția Guvernului României, conform căreia România sprijină pachetul de propuneri în domeniul securității cibernetice, pe care îl consideră oportun și necesar, în condițiile dinamicii deosebite a amenințărilor cibernetice și, mai ales, a consecințelor pe care astfel de atacuri le pot avea asupra sistemelor informatice, economiilor statelor membre, dar și asupra stabilității sistemelor democratice și a valorilor europene.

3. Subliniază interesul României privind o implicare activă în instituirea unei rețele de consolidare a capacității cibernetice a Uniunii, care să reunească Serviciul European de Acțiune Externă, autoritățile din domeniul cibernetic ale statelor membre, serviciile Comisiei, mediul academic și societatea civilă, în acord cu strategia globală.

4. Subliniază poziția României de a sprijini o abordare constructivă în negocierile asupra propunerilor legislative, dar și în discuțiile vizând punerea în aplicare a celorlalte inițiative ale Comisiei, dată fiind importanța acordată de țara noastră securității cibernetice, problematică de interes major la nivel național, inclusiv în perspectiva Președinției române a Consiliului UE, în primul semestru al anului 2019.

5. Reliefează susținerea României față de focalizarea demersurilor comune ale statelor membre pe cele trei dimensiuni – reziliență, descurajare și apărare cibernetică, ca premisă pentru un răspuns eficient și coordonat la nivel european față de amenințările de această natură.

6. În mod particular, subliniază poziția Guvernului României, conform căreia interesul României vizează propunerile legate de pregătirea în vederea unei reacții rapide la atacurile cibernetice, creșterea conștientizării efectelor acestora, dezvoltarea competențelor, implicit a educației, în domeniul securității cibernetice, precum și susținerea eforturilor de îmbunătățire a capacităților în domeniu ale statelor terțe din politica de vecinătate a UE.

7. Evidențiază eforturile României pentru sporirea nivelului de securitate cibernetică și prin transpunerea exigențelor Uniunii Europene în materie de securitate cibernetică, sens în care România a inițiat transpunerea în plan național legislativ a prevederilor Directivei Parlamentului European și a Consiliului privind măsuri pentru un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană (Directiva NIS).

8. Sprijină poziția Guvernului României, conform căreia România susține importanța consolidării cooperării cu statele membre și cu Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), mai ales în contextul propunerilor de extindere a competențelor agenției, în privința conținutului rapoartelor situaționale, incluzând cauzele tehnice și impactul incidentelor de securitate cibernetică, în vederea unei mai bune cooperări tehnice și operaționale în situații de criză.

9. În ceea ce privește partea din regulament referitoare la cadrul de certificare a securității cibernetice, subliniază că poziția României este de susținere a obiectivului principal de a atesta faptul că produsele și serviciile în domeniul tehnologiei informațiilor și comunicației, care au fost certificate în conformitate cu o astfel de schemă, respectă cerințele specifice privind securitatea informatică. Consideră, în acest sens, că se impune o analiză aprofundată a măsurilor privind certificarea în domeniul securității cibernetice, în strânsă legătură cu actorii pieței.

10. Apreciază că o atenție particulară trebuie acordată măsurilor care trebuie adoptate la nivel național pentru crearea cadrului legal de identificare a autorității naționale de supraveghere a certificării care să participe în Grupul european pentru certificarea de securitate cibernetică.

11. În ceea ce privește pilonul apărării cibernetice din prezenta comunicare, atrage atenția asupra aspectelor referitoare la controlul exporturilor tehnologiilor critice cibernetice de supraveghere, deoarece acestea ar trebui aduse la cunoștința Grupului de lucru pentru produse cu dublă utilizare (WPDU), pentru a evita formulări inexacte în documentul final. Consideră ca posibilă măsură la nivel european incriminarea corespunzătoare a infracțiunilor de orice fel în mediul cibernetic și introducerea sancțiunilor penale pentru acestea atât în planul UE, cât și la nivelul statelor membre.

12. Consideră că este necesară abordarea modului în care instrumente cibernetice au putut sau pot influența procesele din interiorul unui stat, inclusiv procesele democratice la nivel intern, în cadrul unei comunicări specifice care să includă o evaluare a modalităților prin care un actor a putut sau poate face acest lucru.

13. Apreciază inițiativa unei reforme a Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), însă consideră necesară o consultare aprofundată a statelor membre și instituirea unor mecanisme la nivelul Agenției pentru colaborarea cu instituțiile specifice din statele membre, care să cuprindă un cadru mai larg și care să includă dar să nu se limiteze la un schimb de informații permanent.

14. Consideră pozitivă ideea unui schimb de informații prin implicarea organismelor și agențiilor UE, a statelor membre, precum și a structurilor însărcinate în acest domeniu ale statelor membre, însă consideră că o abordare cuprinzătoare ar trebui să includă un schimb de informații și expertiză cu mediul privat și sectorul neguvernamental.

15. Atrage atenția asupra necesității unei abordări prioritare, în continuarea demersurilor efectuate până acum, a verificării și controlului impactului pe care relația Uniunii Europene sau a statelor membre cu actori terți, deopotrivă în ce privește relația comercială, îl poate avea asupra infrastructurii critice, inclusiv a celei din domeniul cibernetic.

16. Apreciază că ar fi benefică analizarea aprofundată a dovezilor privind implicarea unor anumite state sau a altor actori în procese democratice interne ale unui alt stat, folosindu-se de mediul cibernetic și de mijloacele puse la dispoziție de acesta.

17. Recomandă dezvoltarea, la nivel european, a cooperării cu mediul privat activ în domeniu, atât în ceea ce privește marile companii prezente la nivel internațional, cât și întreprinderile mici și mijlocii, cu privire la schimbul de informații și expertiză, precum și privind dezvoltarea și aprofundarea unor mecanisme de control, în mediul cibernetic, a mijloacelor care pot provoca infracțiuni în mediul online, inclusiv cu privire la implicarea unor actori terți în procesele interne ale unor state membre. În același timp, atrage atenția asupra necesității respectării, în toate aceste procese, a drepturilor și libertăților fundamentale și a procedurilor democratice, cu precădere a intimității și vieții private a consumatorilor.

18. Apreciază plus-valoarea pe care Directiva NIS o aduce în planul rezilienței cibernetice la nivel european și susține punerea acesteia în aplicare, însă atrage atenția asupra necesității unor măsuri complementare cu aceasta, care să includă crearea unor legături între statele membre și între acestea și instituțiile europene, cu precădere în ceea ce privește structurile interne sau cele europene abilitate în domeniul securității cibernetice.

19. În nota de opțiunea Comisiei Europene privitoare la examinarea posibilității de a lansa un fond de răspuns la situații de urgență legate de securitatea cibernetică și recomandă declanșarea cât mai rapidă a procesului de consultare a statelor membre cu privire la această inițiativă.

20. În continuarea inițiativei Comisiei de creare a unei rețele de centre de competențe în materie de securitate cibernetică și a unui centru european de competențe și de cercetare în materie de securitate cibernetică, recomandă realizarea unei stratificări la nivelul acesteia care să cuprindă rețele aferente mediului public, privat, academic și societății civile.

21. Consideră că investițiile de orice fel în cercetare și dezvoltare de capacități în domeniul securității cibernetice necesită asigurări și protecții împotriva eventualelor scurgeri de informații sau utilizări ale acestora de către terți în scopuri proprii, inclusiv în ce privește criptarea și recomandă detalierea unor astfel de măsuri în viziunea Comisiei.

22. Susține eforturile Comisiei în ce privește promovarea conștientizării și a „igienei” cibernetice în rândul cetățenilor, sens în care consideră benefică ideea organizării unor cursuri speciale în mediul educațional și a unor campanii de informare și publicitate periodice în spațiul public, dedicate securității cibernetice.

23. Recomandă instituirea unor mijloace prin care să fie studiate în amănunt atacurile cibernetice majore de până acum, ca punct de pornire în adoptarea unei conduite preventive bazate pe lecții învățate și în identificarea și aplicarea unor eventuale soluții pentru combaterea unor astfel de atacuri.

24. Crede că, pentru a putea investiga și identifica soluții privind accesul la „Darknet” (internetul întunecat), o posibilă cale ar putea fi identificarea și cooptarea, după caz, a unor utilizatori care au avut sau au acces la mijloacele „Darknet” și utilizarea experienței acestora ca punct de pornire în investigații.

25. În vederea intensificării răspunsului politic, consideră că ar fi necesară o campanie de conștientizare și, eventual, perfecționare, desfășurată în rândul oamenilor politici din statele membre ale Uniunii Europene, cu privire la securitatea cibernetică și la toate fenomenele adiacente.

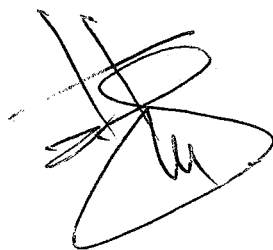
26. Apreciază propunerea Comisiei cu privire la „intensificarea sprijinului financiar pentru proiectele naționale și transnaționale care urmăresc îmbunătățirea justiției penale în spațiul cibernetic”, însă atrage atenția asupra necesității unui control al acestor proiecte și al rezultatelor lor, pentru a evita o eventuală obținere de avantaje de către terți implicați în aceste proiecte, avantaje care ar putea fi folosite în detrimentul Uniunii sau al statelor membre și al cetățenilor acestora.

27. Consideră prioritară îmbunătățirea perpetuă a relației dintre UE și NATO în domeniul securității cibernetice și încurajează Comisia să susțină cadrul regional ca mijloc de cooperare între statele membre în acest domeniu.

Această hotărâre a fost adoptată de către Camera Deputaților în ședința din 21 noiembrie 2017, cu respectarea prevederilor art. 76 alin. (2) din Constituția României, republicată.

**p. PREȘEDINTELE
CAMEREI DEPUTAȚILOR**

Petru - Gabriel VLASE



București, 21 noiembrie 2017

Nr. 87.

Departamentul legislativ,
Șef departament, Georgică Tobă

