Consiliul
Uniunii Europene

**Bruxelles, 17 mai 2016**
**(OR. en)**

**5581/1/16**
**REV 1 ADD 1**

**Dosar interinstituțional:**
**2013/0027 (COD)**

**TELECOM 7**
**DATAPROTECT 6**
**CYBER 4**
**MI 37**
**CSC 15**
**CODEC 84**
**PARLNAT 154**

**EXPUNERE DE MOTIVE A CONSILIULUI**

| | |
|---|---|
| Subiect: | Poziție în primă lectură a Consiliului în vederea adoptării unei DIRECTIVE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune<br>– Expunerea de motive a Consiliului<br>– Adoptată de Consiliu la 17 mai 2016 |

## I. INTRODUCERE

1. Comisia și-a prezentat propunerea de directivă a Parlamentului European și a Consiliului privind *măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune* (denumită în continuare „directiva”) la 12 februarie 2013, utilizând articolul 114 din TFUE ca temei juridic.

2. Comitetul Economic și Social European și-a votat avizul la 22 mai 2013, iar Comitetul Regiunilor și-a votat avizul la 3-4 iulie 2013.

3. Parlamentul European și-a votat rezoluția legislativă în primă lectură la 13 martie 2014[1], adoptând 138 de amendamente.

4. În octombrie 2014, Consiliul și Parlamentul European au inițiat negocieri în vederea obținerii unui acord timpuriu în a doua lectură. Negocierile au fost încheiate cu succes la 7 decembrie 2015, Parlamentul European și Consiliul ajungând la un acord provizoriu cu privire la un text de compromis.

5. La 18 decembrie 2015, Comitetul Reprezentanților Permanenți a confirmat textul de compromis al directivei, astfel cum fusese convenit de cele două instituții.

6. La 28 ianuarie 2016, președinta Comisiei IMCO a Parlamentului European a trimis o scrisoare președintelui Comitetului Reprezentanților Permanenți în care afirma că, în cazul în care Consiliul transmite oficial Parlamentului European poziția sa astfel cum a fost convenită, sub rezerva verificării de către experții juriști-lingviști, va recomanda plenului să accepte fără amendamente poziția Consiliului, în cadrul celei de a doua lecturi a Parlamentului.

7. La 29 februarie 2016, Consiliul și-a confirmat acordul politic cu privire la textul de compromis al directivei.

---

[1] Rezoluția legislativă a Parlamentului European din 13 martie 2014 referitoare la propunerea de directivă a Parlamentului European și a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune.

## II. OBIECTIV

8. Conform rezultatului negocierilor, directiva stabilește măsuri în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în cadrul Uniunii Europene, astfel încât să se îmbunătățească funcționarea pieței interne.

## III. ANALIZA POZIȚIEI CONSILIULUI ÎN PRIMĂ LECTURĂ

### A. Considerații generale

9. După votul în plen, Parlamentul European și Consiliul au desfășurat negocieri cu scopul de a încheia un acord în a doua lectură pe baza unei poziții în primă lectură a Consiliului pe care Parlamentul ar putea să o aprobe ca atare. Textul poziției în primă lectură a Consiliului reflectă pe deplin compromisul la care s-a ajuns între colegiuitori.

### B. Chestiuni-cheie

10. Principalele elemente ale compromisului la care s-a ajuns cu Parlamentul European sunt prezentate în cele ce urmează:

a. *Capacitățile naționale*

11. Conform compromisului, statele membre au anumite obligații în ceea ce privește capacitățile lor naționale de securitate cibernetică. În primul rând, statele membre trebuie să adopte o strategie națională care să definească obiectivele strategice și măsuri adecvate la nivelul politicilor și al reglementării, în vederea atingerii și menținerii unui nivel ridicat de securitate a rețelelor și a sistemelor informatice.

12. În al doilea rând, statele membre desemnează una sau mai multe autorități competente la nivel național privind securitatea rețelelor și a sistemelor informatice, pentru a monitoriza aplicarea directivei la nivel național.

13. În al treilea rând, statele membre au și obligația de a desemna un punct unic de contact național privind securitatea rețelelor și a sistemelor informatice, care va exercita o funcție de legătură pentru asigurarea cooperării transfrontaliere a autorităților statului membru și cu autoritățile relevante din alte state membre, precum și cu grupul de cooperare și rețeaua CSIRT. Punctul unic de contact va fi însărcinat și cu transmiterea către grupul de cooperare a unui raport anual privind notificările primite.

14. În fine, statele membre desemnează una sau mai multe echipe de intervenție în caz de incidente de securitate informatică („CSIRT”), responsabile de administrarea incidentelor și a riscurilor. Cerințele și atribuțiile pentru CSIRT sunt prevăzute în anexa I la textul de compromis.

b. *Cooperarea*

15. Pentru a sprijini și pentru a facilita cooperarea strategică între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, textul de compromis instituie un grup de cooperare. Grupul va fi format din reprezentanți ai statelor membre, ai Comisiei și ai Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și va avea atribuții specifice enumerate în text, precum schimbul de bune practici și de informații cu privire la o serie de aspecte și discutarea capacităților și a nivelului de pregătire ale statelor membre.

16. În plus, textul de compromis instituie o rețea a CSIRT naționale, pentru a contribui la dezvoltarea încrederii între statele membre și pentru a promova cooperarea operațională rapidă și eficace. Rețeaua va fi formată din reprezentanți ai CSIRT ale statelor membre și ai CERT-UE, iar Comisia va participa la rețeaua CSIRT în calitate de observator. ENISA va asigura secretariatul și va sprijini activ cooperarea între CSIRT. Textul prevede o listă de atribuții care urmează să revină rețelei, precum schimbul de informații privind serviciile, operațiunile și capacitățile de cooperare ale CSIRT, sprijinirea statelor membre în abordarea incidentelor transfrontaliere și, în anumite condiții, schimbul și discutarea unor informații legate de incidente și de riscurile asociate.

c. *Cerințele de securitate și notificare*

17. Directiva stabilește anumite obligații pentru două categorii de actori de pe piață: operatorii de servicii esențiale și furnizorii de servicii digitale.

18. În anexa II la directivă sunt enumerate mai multe sectoare importante pentru societate și pentru economie, în speță energia, transporturile, sectorul bancar, infrastructurile pieței financiare, sectorul sănătății, furnizarea și distribuirea de apă potabilă, precum și infrastructura digitală. În cadrul acestor sectoare, statele membre vor identifica operatorii de servicii esențiale, pe baza unor criterii precise prevăzute în directivă.

19. În anexa III la directivă sunt specificate trei tipuri de servicii digitale, ai căror furnizori vor trebui să se conformeze cerințelor din directivă: piețele online, motoarele de căutare online și serviciile de cloud computing. Toți furnizorii de servicii digitale care furnizează serviciile enumerate vor trebui să se conformeze cerințelor prevăzute în directivă, cu excepția microîntreprinderilor și a întreprinderilor mici.

20. Cele două categorii de actori de pe piață vor trebui să ia măsuri organizatorice și tehnice pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice și pentru a preveni și a reduce la minimum impactul incidentelor care afectează securitatea respectivelor sisteme. În plus, incidentele care au un impact de un anumit nivel asupra serviciilor în cauză vor trebui notificate autorităților competente la nivel național sau CSIRT. Directiva prevede criterii pentru determinarea nivelului impactului unor astfel de incidente.

21. Directiva adoptă o abordare diferențiată în ceea ce privește cele două categorii de actori. Cerințele de securitate și de notificare pentru furnizorii de servicii digitale sunt mai puțin exigente decât pentru operatorii de servicii esențiale, fapt care reflectă gradul de risc pe care perturbarea serviciilor acestora îl poate crea pentru societate și pentru economie. În plus, ținând seama de faptul că furnizorii de servicii digitale își desfășoară adesea activitatea în numeroase state membre și în dorința de a asigura un nivel ridicat de armonizare, directiva nu le permite statelor membre să impună furnizorilor respectivi cerințe suplimentare în materie de securitate și notificare.

22. Textul de compromis prevede, de asemenea, că entitățile care nu au fost identificate ca operatori de servicii esențiale și care nu sunt furnizori de servicii digitale pot notifica anumite incidente în mod voluntar.

d. *Transpunerea*

23. Statele membre vor trebui să transpună directiva în termen de 21 de luni de la data intrării sale în vigoare și vor avea la dispoziție șase luni suplimentare pentru a identifica operatorii de servicii esențiale de pe teritoriul lor.

## IV. CONCLUZIE

24. Poziția Consiliului reflectă pe deplin compromisul la care s-a ajuns în cadrul negocierilor dintre Parlamentul European și Consiliu, cu acordul Comisiei. Compromisul este confirmat de scrisoarea adresată de președinta Comisiei IMCO președintelui Comitetului Reprezentanților Permanenți la 28 ianuarie 2016.