



Bruxelles, 30.5.2016  
COM(2016) 363 final

2013/0027 (COD)

**COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN**

**în conformitate cu articolul 294 alineatul (6) din Tratatul privind funcționarea  
Uniunii Europene**

**privind**

**poziția Consiliului privind adoptarea unei Directive a Parlamentului European și a  
Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a  
rețelelor și a informației în Uniune**

(Text cu relevanță pentru SEE)

## COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN

**în conformitate cu articolul 294 alineatul (6) din Tratatul privind funcționarea  
Uniunii Europene**

**privind**

**poziția Consiliului privind adoptarea unei Directive a Parlamentului European și a  
Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a  
rețelelor și a informației în Uniune**

(Text cu relevanță pentru SEE)

### 1. CONTEXT

|   |           |
|---|-----------|
| Data transmiterii propunerii către Parlamentul European și Consiliu<br>[COM(2013) 48 – 2013/0027(COD)]: | 7.2.2013  |
| Data avizului Comitetului Economic și Social European:  | 22.5.2013 |
| Data avizului Parlamentului European în primă lectură:  | 13.3.2014 |
| Data adoptării poziției Consiliului:  | 17.5.2016 |

### 2. OBIECTUL PROPUNERII COMISIEI

În primul rând, propunerea solicită tuturor statelor membre să se asigure că au instituit un nivel minim de capacități naționale prin

- instituirea de autorități competente în domeniul securității rețelelor și a informațiilor (NIS);
- înființarea de echipe de intervenție în cazul producerii unor incidente care afectează securitatea informatică (CSIRT);
- adoptarea de strategii naționale NIS și de planuri de cooperare naționale în domeniul NIS.

În al doilea rând, autoritățile naționale competente ar trebui să coopereze în cadrul unei rețele care să permită coordonarea sigură și eficace, inclusiv schimbul coordonat de informații, precum și detectarea și intervenția la nivelul UE. Prin această rețea, statele membre ar urma să facă schimb de informații și să coopereze pentru a contracara amenințările și incidentele în materie de NIS, pe baza planului de cooperare european în domeniul NIS. Pentru a se asigura că toate autoritățile relevante sunt implicate în mod corespunzător și în timp util, propunerea prevede, de asemenea, ca agențiile de asigurare a punerii în aplicare a legii să fie informate cu privire la incidentele cu caracter penal, iar Europol să fie implicat în mecanismele de coordonare existente la nivelul UE.

În al treilea rând, pe baza modelului Directivei-cadru privind comunicațiile electronice, propunerea urmărește să asigure dezvoltarea unei culturi a gestionării riscurilor și partajarea informațiilor între sectoarele public și privat. Se va solicita întreprinderilor din anumite sectoare critice și administrațiilor publice să evalueze riscurile cu care se confruntă și să adopte măsuri adecvate și proporționate de asigurare a NIS. Aceste entități vor trebui să raporteze autorităților competente orice incident care le afectează grav rețelele și sistemele informatice și care afectează semnificativ continuitatea serviciilor critice și aprovizionarea cu bunuri.

### **3. OBSERVAȚII PRIVIND POZIȚIA CONSILIULUI**

În ansamblu, poziția Consiliului susține obiectivele esențiale ale propunerii Comisiei, și anume asigurarea unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice. Cu toate acestea, Consiliul introduce unele schimbări cu privire la modul de îndeplinire a acestui obiectiv.

#### *Capacitățile naționale în domeniul securității cibernetice*

În conformitate cu poziția Consiliului, se va solicita statelor membre să adopte o strategie națională privind NIS în care să se prevadă obiectivele strategice și liniile de politică și măsurile de reglementare adecvate pentru asigurarea securității cibernetice. De asemenea, se va solicita statelor membre să desemneze o autoritate națională competentă pentru punerea în aplicare și asigurarea punerii în practică a directivei, precum și echipe de intervenție în cazul producerii unor incidente care afectează securitatea informatică (*Computer Security Incident Response Teams - CSIRT*), responsabil pentru administrarea incidentelor și a riscurilor.

Cu toate că poziția Consiliului nu impune statelor membre obligația de a adopta un plan național de cooperare în domeniul NIS, astfel cum se prevede în propunerea inițială, această poziție poate fi susținută, deoarece unele aspecte ale planului de cooperare sunt reținute în dispozițiile privind strategia NIS.

#### *Cooperarea dintre statele membre*

În conformitate cu poziția Consiliului, directiva va institui un „grup de cooperare” alcătuit din reprezentanți ai statelor membre, ai Comisiei și ai Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), care va sprijini și va facilita cooperarea strategică și schimbul de informații între statele membre. De asemenea, directiva va institui o rețea de echipe de intervenție în cazul producerii unor incidente care afectează securitatea informatică (denumită și Rețeaua CSIRT), în vederea promovării unei cooperări operaționale rapide și eficiente cu privire la incidentele specifice securității cibernetice, precum și a schimbului de informații privind riscurile.

Cu toate că diferă în mod substanțial față de abordarea adoptată în propunerea inițială a Comisiei, poziția Consiliului poate fi susținută întrucât corespunde, în ansamblu, obiectivului de îmbunătățire a cooperării dintre statele membre.

#### *Cerințe de securitate și notificare pentru operatorii de servicii esențiale*

În conformitate cu poziția Consiliului, „operatorilor de servicii esențiale” (echivalentul „operatorilor de infrastructuri critice” din propunerea inițială) li se va cere să adopte măsurile de securitate corespunzătoare și să notifice incidentele grave către autoritățile naționale competente. Cu toate acestea, Consiliul nu a susținut obligația ca autoritățile naționale competente să notifice incidentele cu caracter penal către autoritățile de asigurare a respectării legii.

În conformitate cu propunerea inițială a Comisiei, poziția Consiliului include astfel de operatori din sectoarele energiei, transporturilor, serviciilor bancare, infrastructurilor piețelor financiare și sănătății. Cu toate acestea, poziția Consiliului include, de asemenea, sectorul gestionării apei și sectorul infrastructurii digitale.

Statele membre vor trebui să identifice acești operatori pe baza anumitor criterii, de exemplu dacă serviciul este esențial pentru menținerea activităților economice și societale vitale. În pofida faptului că acest proces de identificare nu a fost cuprins în propunerea inițială, acesta poate fi acceptat, având în vedere obligația statelor membre de a transmite Comisiei informațiile de care are nevoie pentru a evalua dacă statele membre recurg la abordări coerente de identificare a operatorilor de servicii esențiale.

Administrațiile publice ca atare nu sunt incluse în poziția Consiliului. Totuși, în cazul în care acestea îndeplinesc criteriile prevăzute la articolul 5, acestea vor trebui să fie identificate de statele membre ca operatori de servicii esențiale, întrucât operatorii de servicii esențiale pot fi entități publice sau private.

#### *Cerințe de securitate și notificare pentru furnizorii de servicii digitale*

În conformitate cu poziția Consiliului, statele membre vor trebui să se asigure că furnizorii de servicii digitale (DSP) iau măsurile de securitate corespunzătoare și notifică incidentele către autoritatea competentă. Poziția Consiliului include piețele online (echivalente cu platformele de comerț electronic din propunerea inițială), serviciile de tip *cloud computing* și motoarele de căutare. În comparație cu propunerea inițială, poziția Consiliului nu include:

- procesatorii de plăți online – sunt în prezent reglementate de Directiva revizuită privind serviciile de plată;
- magazinele de aplicații online – acestea trebuie să fie înțelese ca fiind un tip de piețe online;
- rețelele sociale – în conformitate cu acordul politic al Consiliului cu Parlamentul European.

Conform poziției Consiliului, Comisia a fost investită cu competențe de executare pentru a stabili dispozițiile procedurale necesare pentru funcționarea grupului de cooperare, precum și pentru a clarifica anumite elemente privind furnizorii de servicii digitale, inclusiv formatele și procedurile aplicabile cerințelor de notificare de către furnizorii de servicii digitale.

Comisia sprijină aceste modificări.

În urma discuțiilor tripartite informale desfășurate la 14 octombrie 2014, 11 noiembrie 2014, 30 aprilie 2015, 29 iunie 2015, 17 noiembrie 2015 și 7 decembrie 2015, Parlamentul European și Consiliul au ajuns la un acord politic provizoriu cu privire la textul menționat.

Acest acord politic a fost confirmat de Consiliu la 18 decembrie 2015. La 17 mai 2016, Consiliul a adoptat poziția în primă lectură.

#### **4. CONCLUZII**

Comisia sprijină rezultatele negocierilor interinstituționale și, prin urmare, poate să accepte poziția Consiliului în primă lectură.