Rezumatul Avizului Autorității Europene pentru Protecția Datelor referitor la Comunicarea comună a Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate privind „Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat" și referitor la propunerea Comisiei de directivă privind măsurile de asigurare a unui nivel comun ridicat al securității rețelelor și informației în întreaga Uniune

(Textul integral al prezentului aviz poate fi consultat în EN, FR și DE pe site-ul AEPD: http://www.edps.europa.eu)

(2014/C 32/10)

1. **Introducere**

1.1. *Consultarea AEPD*

1. La 7 februarie 2013, Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au adoptat o Comunicare comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind „Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat" ([1]) (denumită în continuare „comunicarea comună", „strategia de securitate cibernetică" sau „strategia").

2. La aceeași dată, Comisia a adoptat o propunere de directivă a Parlamentului European și a Consiliului privind măsurile de asigurare a unui nivel comun de securitate a rețelelor și informației în întreaga Uniune ([2]) (denumită în continuare „propunerea de directivă" sau „propunerea"). Această propunere a fost trimisă AEPD spre consultare la 7 februarie 2013.

3. Înainte de adoptarea comunicării comune și a propunerii, Autorității Europene pentru Protecția Datelor i s-a dat posibilitatea de a prezenta observații informale Comisiei. AEPD salută faptul că o parte dintre observațiile sale au fost luate în considerare în comunicarea comună și în propunere.

4. **Concluzii**

74. AEPD salută faptul că Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au prezentat o strategie completă de securitate cibernetică, în completarea căreia vine o propunere de măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune. Strategia completează acțiunile în materie de politici deja dezvoltate de UE în domeniul securității rețelelor și informației.

75. AEPD salută faptul că strategia depășește abordarea tradițională în cadrul căreia securitatea este contradictorie vieții private, prin prevederea recunoașterii explicite a vieții private și a protecției datelor ca valori de bază care ar trebui să reprezinte principiile directoare ale politicii de securitate cibernetică la nivelul UE și la nivel internațional. AEPD remarcă faptul că strategia de securitate cibernetică și propunerea de directivă privind securitatea rețelelor și informației pot avea un rol fundamental în contribuția la asigurarea protecției riscurilor individuale la adresa vieții private și protecției datelor în mediul online. În același timp, trebuie să se asigure că acestea nu conduc la măsuri care ar constitui interferențe ilegale cu drepturile persoanelor la viața privată și protecția datelor.

76. AEPD salută, de asemenea, faptul că protecția datelor este menționată în mai multe părți ale strategiei și este luată în considerare în propunerea de directivă privind securitatea rețelelor și a informației. Totuși, AEPD își exprimă regretul că strategia și propunerea de directivă nu subliniază mai bine contribuția legislației existente și viitoare în materie de protecție a datelor la securitate și nu asigură integral ca toate obligațiile care decurg din propunerea de directivă sau alte elemente ale strategiei să fie complementare cu obligațiile de protecție a datelor și să nu se suprapună sau să vină în contradictoriu cu acestea.

77. În plus, AEPD observă că din cauza faptului că nu se iau în considerare integral alte inițiative paralele și proceduri legislative curente ale Comisiei, precum reforma în domeniul protecției datelor și propunerea de regulament privind identificarea electronică și serviciile de asigurare a încrederii, strategia de securitate cibernetică nu oferă o imagine cuprinzătoare și generală a securității cibernetice în UE și există riscul

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

perpetuării unei abordări fragmentate și compartimentate. AEPD menționează, de asemenea, că nici propunerea de directivă privind securitatea rețelelor și informației nu permite încă o abordare cuprinzătoare a securității în UE și că obligația prevăzută în legislația privind protecția datelor este probabil cea mai cuprinzătoare obligație privind rețelele și securitatea din cadrul legislației UE.

78. AEPD își exprimă, de asemenea, regretul că rolul important al autorităților de protecție a datelor în punerea în aplicare și executarea obligațiilor de securitate și în sporirea securității cibernetice nu este, la rândul său, avut în vedere în mod corespunzător.

79. În ceea ce privește strategia de securitate cibernetică, AEPD subliniază că:

— o definiție clară a termenilor „rezistență cibernetică", „criminalitate cibernetică" și „apărare cibernetică" este deosebit de importantă, deoarece acești termeni sunt utilizați ca justificare pentru anumite măsuri speciale care pot afecta drepturile fundamentale, inclusiv drepturile la viață privată și protecția datelor. Totuși, definițiile „criminalității informatice" prevăzute în strategie și în Convenția privind criminalitatea cibernetică rămân foarte largi. Ar fi de recomandat ca definiția „criminalității cibernetice" să fie clară și *restrictivă*, și nu extinsă;

— legislația în materie de protecție a datelor ar trebui să se aplice tuturor acțiunilor prevăzute în strategie, ori de câte ori acestea vizează măsuri care implică prelucrarea de date cu caracter personal. Deși legislația privind protecția datelor nu este menționată în mod specific în secțiunile legate de criminalitatea cibernetică și apărarea cibernetică, AEPD subliniază că multe dintre acțiunile planificate în aceste domenii ar implica prelucrarea de date cu caracter personal și astfel ar intra sub incidența legislației aplicabile privind protecția datelor. Autoritatea menționează, de asemenea, că multe acțiuni constau în crearea de mecanisme de coordonare, care vor necesita punerea în aplicare a unor garanții adecvate de protecție a datelor în ceea ce privește modalitățile disponibile pentru schimbul de date cu caracter personal;

— autoritățile pentru protecția datelor (APD) au un rol important în contextul securității cibernetice. În calitate de gardieni ai drepturilor persoanelor la viața privată și protecția datelor, APD se implică activ în protejarea datelor cu caracter personal, atât offline, cât și online. Prin urmare, acestea ar trebui implicate în mod adecvat, în calitatea lor de organisme de supraveghere, în ceea ce privește punerea în aplicare a măsurilor care implică prelucrarea datelor cu caracter personal (precum lansarea proiectului-pilot al UE privind combaterea botneturilor și programelor malware). Alți actori din domeniul securității cibernetice ar trebui, la rândul lor, să coopereze cu aceste autorități în îndeplinirea sarcinilor lor, de exemplu, în cadrul acțiunilor de schimb de bune practici și creștere a gradului de conștientizare. AEPD și APD naționale ar trebui, de asemenea, implicate în mod adecvat în conferința la nivel înalt care va fi organizată în 2014 pentru evaluarea progresului punerii în aplicare a strategiei.

80. În ceea ce privește propunerea de directivă privind securitatea rețelelor și informației, AEPD recomandă legislatorului următoarele:

— să formuleze articolul 3 alineatul (8) privind definiția operatorilor de pe piață care intră sub incidența propunerii într-un mod mai clar și cu mai multă certitudine și să întocmească o listă completă care să cuprindă toate părțile interesate relevante, în vederea asigurării unei abordări integral armonizate și integrate privind securitatea în cadrul UE;

— să clarifice la articolul 1 alineatul (2) litera (c) că propunerea de directivă se aplică instituțiilor și organismelor UE și să includă o trimitere la Regulamentul (CE) nr. 45/2001 în articolul 1 alineatul (5) al propunerii;

— să recunoască un rol mai orizontal al propunerii în ceea ce privește securitatea, stipulând explicit la articolul 1 că ar trebui să se aplice fără a aduce atingere normelor existente sau viitoare mai detaliate în domenii specifice (precum cele care vor fi impuse pentru prestatorii de servicii de asigurare a încrederii în propunerea de regulament privind identificarea electronică);

— să se adauge un considerent pentru a explica necesitatea încorporării protecției datelor prin concepție și în mod implicit, încă din primele etape ale proiectării mecanismelor stabilite în propunere și pe parcursul întregului ciclu de viață al proceselor, procedurilor, organizațiilor, tehnicilor și infrastructurilor implicate, luând în considerare propunerea de regulament privind protecția datelor;

— să clarifice definiția „rețelei și sistemului informatic” de la articolul 3 alineatul (1) și a „incidentului” de la articolul 3 alineatul (4) și să înlocuiască la articolul 5 alineatul (2) obligația de a stabili un „plan de evaluare a riscurilor” prin „crearea și menținerea unui cadru de gestionare a riscurilor”;

— să specifice la articolul 1 alineatul (6) că prelucrarea datelor cu caracter personal ar fi justificată în temeiul articolului 7 litera (e) din Directiva 95/46/CE în măsura în care este necesară pentru atingerea obiectivelor de interes public urmărite de propunerea de directivă. Totuși, ar trebui să se respecte principiul necesității și proporționalității, astfel încât doar datele strict necesare pentru scopul care trebuie atins să fie prelucrate;

— să se stabilească la articolul 14 circumstanțele în care este necesară notificarea, precum și conținutul și formatul notificării, inclusiv tipurile de date cu caracter personal care ar trebui notificate și dacă este sau nu cazul și în ce măsură notificarea și documentele sale justificative vor include detalii privind datele cu caracter personal afectate de un incident specific de securitate (precum adresele IP). Trebuie să se țină seama de faptul că autorităților competente în domeniul securității rețelelor și informației ar trebui să li se permită să colecteze și să prelucreze date cu caracter personal în cadrul unui incident de securitate doar dacă este strict necesar. De asemenea, ar trebui prevăzute garanții adecvate în cadrul propunerii, pentru a se asigura protecția adecvată a datelor prelucrate de autoritățile competente privind securitatea rețelelor și informației;

— să clarifice la articolul 14 că notificările privind incidentele în temeiul articolului 14 alineatul (2) ar trebui să se aplice fără a aduce atingere obligațiilor de notificare a cazurilor de încălcare a protecției datelor cu caracter personal în temeiul legislației aplicabile în materie de protecție a datelor. Principalele aspecte ale procedurii de cooperare a autorităților în domeniul securității rețelelor și informației cu APD în cazurile în care incidentul de securitate implică o încălcare a protecției datelor cu caracter personal ar trebui să fie prevăzute în propunere;

— să se modifice articolul 14 alineatul (8) în așa fel încât excluderea microîntreprinderilor din domeniul de aplicare al notificării să nu se aplice acelor operatori care au un rol esențial în furnizarea serviciilor societății informaționale, de exemplu, având în vedere natura informațiilor pe care le prelucrează (de exemplu, date biometrice sau date sensibile);

— să se adauge dispoziții în cadrul propunerii privind reglementarea viitorului schimb de informații cu caracter personal de către autoritățile competente în domeniul securității rețelelor și informației cu alți destinatari, pentru a se asigura că: (i) datele cu caracter personal sunt divulgate doar destinatarilor pentru care prelucrarea datelor este necesară pentru efectuarea sarcinilor lor în conformitate cu un temei juridic adecvat; și (ii) aceste informații se limitează la ceea ce este necesar pentru efectuarea sarcinilor lor. Trebuie să se aibă în vedere, de asemenea, modul în care entitățile care furnizează date în rețeaua de partajare a informațiilor asigură conformitate cu principiul limitării scopului;

— să se specifice termenul de reținere a datelor cu caracter personal pentru scopul stabilit în propunerea de directivă, în special în ceea ce privește reținerea de către autoritățile competente în materie de securitate a rețelelor și informației și în cadrul infrastructurii sigure a rețelei de cooperare;

— să se reamintească autorităților competente în materie de securitate a rețelelor și informațiilor obligația acestora de a furniza informații adecvate persoanelor vizate cu privire la prelucrarea datelor lor cu caracter personal, de exemplu, prin publicarea unei politici privind viața privată pe site-ul lor;

— să se adauge o dispoziție privind nivelul de securitate care trebuie respectat de către autoritățile competente în domeniul securității rețelelor și informației în ceea ce privește informațiile colectate, prelucrate și comunicate reciproc. O trimitere la cerințele în materie de securitate de la articolul 17 din Directiva 95/46/CE ar trebui în mod specific inclusă în ceea ce privește protecția datelor cu caracter personal de către autoritățile competente în domeniul securității rețelelor și informației;

— să se clarifice la articolul 9 alineatul (2) că criteriile de participare a statelor membre la sistemul de partajare a informațiilor ar trebui să asigure garantarea unui nivel înalt de securitate și rezistență de către toți participanții la sistemele de partajare a informațiilor, în toate etapele prelucrării. Aceste criterii ar trebui să includă măsuri adecvate de confidențialitate și securitate, în conformitate cu articolele 16 și 17 din Directiva 95/46/CE și articolele 21 și 22 din Regulamentul (CE) nr. 45/2001. Aceste criterii ar trebui să fie în special obligatorii pentru Comisie, în ceea ce privește participarea acesteia, în calitate de operator, la sistemul securizat de partajare a informațiilor;

— să se adauge la articolul 9 o descriere a rolurilor și responsabilităților Comisiei și statelor membre în configurarea, operarea și mentenanța sistemului securizat de partajare a informațiilor și să se prevadă că proiectarea sistemului trebuie realizată în conformitate cu principiile protecției datelor prin concepție și în mod implicit și securității prin concepție; și

— să se adauge la articolul 13 precizarea că orice transfer de date cu caracter personal către destinatari localizați în afara UE ar trebui să aibă loc în conformitate cu articolele 25 și 26 din Directiva 95/46/CE și articolul 9 din Regulamentul (CE) nr. 45/2001.

Adoptat la Bruxelles, 14 iunie 2013.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor