

# AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

## **Rezumatul Avizului Autorității Europene pentru Protecția Datelor referitor la Comunicarea Comisiei către Parlamentul European și Consiliu privind „Restabilirea încrederii în fluxurile de date dintre UE și SUA” și la Comunicarea Comisiei către Parlamentul European și Consiliu privind „Funcționarea sferei de siguranță din perspectiva cetățenilor UE și a întreprinderilor stabilite în UE”**

(Textul integral al prezentului aviz poate fi consultat în engleză, franceză și germană pe site-ul AEPD ([www.edps.europa.eu](http://www.edps.europa.eu)))

(2014/C 116/04)

### I. Introducere

#### I.1. Consultarea AEPD

1. La 27 noiembrie 2013, Comisia a adoptat comunicarea Comisiei către Parlamentul European și Consiliu privind „Restabilirea încrederii în fluxurile de date dintre UE și SUA”<sup>(1)</sup> (denumită în continuare „Comunicarea privind restabilirea încrederii”). Această comunicare este însoțită de un raport asupra constatărilor copreședinților europeni ai Grupului de lucru *ad hoc* UE-SUA pentru protecția datelor (denumite în continuare „raportul” și, respectiv, „Grupul de lucru”).
2. La aceeași dată, Comisia a adoptat o Comunicare a Comisiei către Parlamentul European și Consiliu privind „Funcționarea sferei de siguranță din perspectiva cetățenilor UE și a întreprinderilor stabilite în UE”<sup>(2)</sup> (denumită în continuare „Comunicarea privind sfera de siguranță”).
3. AEPD salută faptul că i s-a oferit posibilitatea de a prezenta observații informale Comisiei înaintea adoptării documentelor sus-menționate. Comisia a adoptat aceste documente ca urmare a dezvăluirilor privind programele de supraveghere desfășurate de serviciile de informații ale SUA. Având în vedere impactul acestor programe de supraveghere asupra drepturilor persoanelor la viața privată și la protecția datelor lor cu caracter personal pe teritoriul UE, AEPD a decis să adopte prezentul aviz din proprie inițiativă

#### I.2. *Objective and scope of the Commission documents*

##### a) Comunicarea privind restabilirea încrederii și raportul

4. Comunicarea propune o cale de urmat, după dezvăluirile privind programele de colectare de informații la scară largă ale SUA (denumite în continuare „programele” sau „programele dezvăluite”) și având în vedere impactul acestora asupra încrederii dintre UE și SUA. Comunicarea nu se referă la dezvăluirile privind desfășurarea unor activități similare și/sau la colaborarea cu SUA a statelor membre UE sau a altor țări terțe cu SUA.
5. Raportul compilează constatările copreședinților europeni ai Grupului de lucru *ad hoc* UE-SUA pentru protecția datelor, care a fost creat în urma reuniunii Coreper din 18 iulie 2013 de stabilire a faptelor cu privire la programe și a impactului lor asupra drepturilor fundamentale în UE și asupra datelor cu caracter personal ale cetățenilor UE. Raportul analizează cadrul juridic al SUA<sup>(3)</sup>, modul în care are loc colectarea și prelucrarea ulterioară a datelor<sup>(4)</sup> și mecanismele existente de control și de remediere.

<sup>(1)</sup> COM(2013) 846 final.

<sup>(2)</sup> COM(2013) 847 final.

<sup>(3)</sup> În special Constituția, astfel cum este interpretată de Curtea Supremă; secțiunea 702 din Legea din 1978 pentru supravegherea informațiilor externe (FISA) (astfel cum a fost modificată prin Legea din 2008 de modificare a FISA, 50 U.S.C. § 1881a) și secțiunea 215 din Legea USA PATRIOT din 2001 (care a modificat, de asemenea, FISA, 50 U.S.C. 1861) și Decretul 12333.

<sup>(4)</sup> Pe baza informațiilor furnizate de SUA în cadrul grupului de lucru și pe baza documentelor declasificate, inclusiv avizele Curții de Supraveghere a Activităților Străine de Spionaj (denumită în continuare „FISC”) și a documentelor disponibile publicului, cum ar fi Orientările Procurorului General privind operațiunile interne ale FBI.

6. Raportul menționează o „a doua cale”, care a fost stabilită, de asemenea, în cursul reuniunii Coreper din 18 iulie 2013. Raportul arată că, prin intermediul acestei „a doua căi”, instituțiile UE pot adresa autorităților SUA întrebări cu privire la presupusa supraveghere a instituțiilor și misiunilor diplomatice ale UE, în timp ce statele membre pot discuta cu autoritățile SUA, într-un format bilateral, chestiuni legate de securitatea lor națională.
7. De asemenea, raportul arată că această divizare a stabilit o serie de limite ale discuțiilor și ale informațiilor furnizate în cadrul grupului de lucru. AEPD nu a primit nicio informație cu privire la cea „de a doua cale” sau la crearea unui grup de lucru paralel în această privință. Prin urmare, Comisia este invitată să informeze AEPD despre constatările celei „de a doua căi”, în special în ceea ce privește presupusa supraveghere a instituțiilor și misiunilor diplomatice ale UE.

(b) Comunicarea privind sfera de siguranță

8. Comunicarea privind sfera de siguranță analizează funcționarea sferei de siguranță, identifică nereguli și propune îmbunătățiri posibile. Comunicarea recunoaște creșterea continuă a volumului de date care fac obiectul transferurilor între UE și SUA și numărul tot mai mare de întreprinderi care aderă la principiile sferei de siguranță. După evocarea structurii și funcționării sferei de siguranță, Comisia insistă asupra necesității ca aplicarea principiilor la întreprinderile și subcontractorii lor care aderă la aceste principii să fie îmbunătățite. Potrivit comunicării, acest lucru ar impune ca principiile sferei de siguranță să fie încorporate într-un mod mai eficace în politicile de confidențialitate ale întreprinderilor care aderă și să fie făcute publice. Comisia Federală pentru Comerț din SUA ar trebui să se implice mai proactiv în asigurarea conformității cu aceste principii. În plus, autoritățile pentru protecția datelor ar trebui să participe la creșterea gradului de sensibilizare în UE în ceea ce privește sfera de siguranță și, în mod special, existența grupului UE pentru protecția datelor. De asemenea, Comisia oferă soluții de îmbunătățire a mecanismelor de soluționare alternativă a litigiilor.
9. În ceea ce privește accesul la datele transferate în cadrul sistemului sferei de siguranță și prelucrate ulterior de autoritățile SUA, Comisia insistă asupra faptului că acest acces ar trebui să fie limitat la ceea ce este strict necesar și proporțional. De asemenea, Comisia solicită ca utilizarea limitelor impuse politicilor de confidențialitate în vederea respectării cerințelor privind securitatea națională, interesul public sau aplicarea legii să fie atent monitorizată, astfel încât să nu submineze protecția acordată. Comisia încurajează întreprinderile care aderă să fie transparente în ceea ce privește aceste limite și efectul lor asupra confidențialității comunicărilor, în vederea creșterii gradului de sensibilizare a cetățenilor.

I.3. Obiectivul și domeniul de aplicare al prezentului aviz

10. Prezentul aviz se referă la Comunicarea privind restabilirea încrederii și, în același context, și la Comunicarea privind sfera de siguranță. Astfel, avizul nu ia în discuție în mod direct dezvăluirile cu privire la statele membre ale UE, fie în colaborare cu SUA, fie pe cont propriu, și nici la activitățile de supraveghere ale țărilor terțe altele decât SUA.
11. Avizul începe prin a prezenta observații asupra abordării generale a Comunicării privind restabilirea încrederii. Partea II analizează pe scurt aplicabilitatea cadrului juridic relevant și consecințele acestuia, incluzând observații asupra Comunicării privind sfera de siguranță. Întrucât Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal<sup>(1)</sup> examinează în prezent cadrul juridic european și internațional aplicabil, prezentul aviz nu intră în detalii în această parte a sa. Partea III se referă la recomandările Comisiei privind măsurile care urmează să fie luate.

I.4. Observații legate de abordarea din Comunicarea privind restabilirea încrederii

12. Comunicarea subliniază faptul că încrederea dintre UE și SUA, ca parteneri strategici, a fost afectată de dezvăluirile privind programele și că această încredere trebuie restabilită. AEPD salută această recunoaștere.

<sup>(1)</sup> Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit în temeiul Directivei 95/46/CE, are un statut consultativ și acționează independent. Grupul este alcătuit din reprezentanți ai autorităților naționale ale UE pentru protecția datelor, AEPD și Comisie.

13. Cu toate acestea, programele, a căror existență este, în unele cazuri, confirmată în mod clar în raport<sup>(1)</sup>, afectează nu numai încrederea, dar și drepturile legale stabilite în legislația primară și secundară a UE și a Consiliului European, în special drepturile la viața privată și la protecția datelor. De asemenea, programele indică scara largă la care are loc în prezent colectarea informațiilor externe în temeiul cadrului juridic al SUA<sup>(2)</sup>, astfel cum este interpretat de Curtea Supremă a SUA<sup>(3)</sup>. Raportul confirmă totodată și absența garanțiilor, protecțiilor, drepturilor, posibilităților de control și remediere disponibile cetățenilor UE potrivit cadrului juridic al SUA<sup>(4)</sup>.
14. Astfel cum Comisia a subliniat în mod repetat, încrederea cetățenilor și a întreprinderilor în comunicările pe internet depinde de disponibilitatea instrumentelor tehnice eficiente de protecție a confidențialității, mai precis de caracterul confidențial al comunicărilor. Această necesitate a fost, de asemenea, recunoscută în cadrul Grupului de analiză al SUA privind tehnologiile de informații și de comunicații<sup>(5)</sup>, care a făcut mai multe recomandări în vederea restabilirii încrederii în instrumentele de criptare și programele comerciale pentru calculatoare, precum și în funcționarea mecanismelor rapide de remediere a vulnerabilităților acestor programe. Unii dintre cei mai recunoscuți experți în domeniul securității consideră că slăbirea încrederii în aceste sisteme reprezintă unul dintre cele mai dăunătoare efecte ale recentelor discuții despre operațiunile de interceptare a informațiilor electronice<sup>(6)</sup>. Având în vedere importanța securității cibernetice eficiente pentru Europa, ar trebui formulat la nivelul UE un răspuns la această provocare de natură tehnică și politică pe baza unei inițiative a Comisiei.
15. În secțiunea 3 din comunicare, Comisia se referă la măsurile viitoare necesare a fi luate în scopul restabilirii încrederii în transferurile de date dintre UE și SUA. AEPD salută această secțiune care vizează îmbunătățirea cadrului juridic existent și propune noi instrumente. Cu toate acestea, Comisia nu menționează modul în care programele au afectat instrumentele aplicabile naționale, ale UE și ale Consiliului. AEPD consideră că impactul asupra instrumentelor juridice existente ar trebui să se bucure de o mai mare atenție în comunicare.

#### IV. Observații finale

79. AEPD salută măsurile avute în vedere de Comisie, însă subliniază faptul că activitățile dezvăluite de supraveghere realizate de serviciile de informații ale SUA nu afectează doar încrederea în fluxurile de date dintre UE și SUA. Acestea au un impact și asupra drepturilor existente și aplicabile ale cetățenilor UE la respectarea vieții private și la protecția datelor lor cu caracter personal. Aceste drepturi sunt consacrate atât în legislația primară, cât și în cea secundară a UE și a Consiliului European. În consecință, AEPD regretă faptul că în comunicare nu s-a acordat o mai mare atenție impactului asupra instrumentelor juridice existente.
80. AEPD dorește să insiste asupra mai multor puncte în legătură cu care Comisia ar trebui să manifeste mai multă ambiție atunci când definește următoarele măsuri care trebuie luate și constată că:
- aplicarea și respectarea cadrului juridic european actual privind protecția datelor nu sunt doar impuse prin lege, ci ar trebui să constituie și o contribuție esențială la restabilirea încrederii. Același lucru este valabil și pentru instrumentele de reglementare a transferurilor internaționale dintre UE și SUA, inclusiv pentru principiile existente ale sferei de siguranță;
  - Comisia ar trebui să reamintească faptul că excepțiile sau restricțiile la drepturile fundamentale, permise în scopuri de securitate națională, sunt justificate și admisibile numai dacă sunt strict necesare, proporționale și în concordanță cu jurisprudența Curții Europene a Drepturilor Omului și a Curții de Justiție;

(1) A se vedea p. 5, 10 și 26 din raport, care, pe baza avizelor declasificate ale Curții de Supraveghere a Activităților Străine de Spionaj, confirmă că „serviciile de informații ale SUA recurg la metode de colectare în temeiul secțiunii 702 care au o sferă largă, de exemplu colectarea prin programul PRISM a datelor de la furnizorii de servicii de internet sau prin «colectarea în amonte» a datelor care tranzitează SUA”.

(2) SUA au confirmat că există alte temeuri juridice pentru colectarea de informații, în care pot fi obținute date ale persoanelor care nu sunt rezidente în SUA, dar nu au oferit detalii cu privire la autoritățile judiciare și la procedurile aplicabile. Grupului de lucru nu i-au fost dezvăluite toate temeiurile juridice relevante (a se vedea p. 13 din raport).

(3) A se vedea p. 4-12 din raport.

(4) A se vedea p. 26-27 din raport.

(5) „Liberty and Security in a Changing World” (*Libertate și securitate într-o lume aflată în continuă schimbare*), raport și recomandări ale Grupului de analiză al președintelui privind tehnologiile de informații și comunicații, în special recomandările 25, 29 și 30. [http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)

(6) B. Schneier, C. Soghoian în raportul din 6 septembrie 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>; B. Preneel: ISSE 2013, discurs de încheiere: „The Cryptographic Year in Review” (*Anul criptografic în analiză*), [http://homes.esat.kuleuven.be/~preneel/preneel\\_isse13.pdf](http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf)

- AEPD este într-un acord cu faptul că îmbunătățirea și consolidarea cadrului UE de protecție a datelor impune o adoptare rapidă a propunerilor de reforme în domeniul protecției datelor, cu un conținut suficient pentru a oferi o protecție mai puternică, mai eficientă și mai coerentă a datelor cu caracter personal și a vieții private în cadrul întregului domeniu de aplicare al dreptului UE. De asemenea, acest conținut ar trebui să asigure protecția adecvată a datelor în cazul utilizării ulterioare a acestora în scopul aplicării legii, precum și în conflictele internaționale de jurisdicție;
- principiile sferei de siguranță ar trebui revizuite și consolidate în concordanță cu orientările Comisiei. AEPD recomandă stabilirea unor termene mai strânse în care trebuie luate aceste măsuri, inclusiv monitorizarea adecvată în cazul în care unele nereguli persistă;
- este necesară consolidarea garanțiilor privind protecția datelor aplicabile cooperării dintre UE și SUA în domeniul aplicării legii. Negocierile actuale privitoare la un „acord-umbrelă” nu ar trebui să legitimeze transferurile masive de date, ci să respecte cadrul existent de protecție a datelor și rezultatul procesului actual de revizuire a acestuia. În mod special, toate persoanele vizate ar trebui să aibă acces la căi de atac eficiente, indiferent de naționalitatea lor. Aceasta ar trebui să se aplice în timp și acordurilor internaționale existente, dacă este necesar, pe baza unor clauze tranzitorii adecvate;
- Comisia ar trebui să susțină eforturile Administrației SUA și ale Congresului SUA în vederea adoptării unei legi generale privind viața privată, care să ofere garanții solide și un control adecvat, în special în domenii care în prezent sunt lipsite de orice protecție adecvată a vieții private;
- negocierile care au loc în prezent în vederea adoptării unui parteneriat pentru comerț și investiții nu ar trebui să aibă un impact negativ asupra protecției datelor cu caracter personal ale cetățenilor. În același timp, Comisia ar trebui să aibă în vedere stabilirea unui obiectiv comun de dezvoltare treptată în direcția unei mai mari interoperabilități a cadrelor juridice pentru viața privată și protecția datelor, obiectiv la care SUA ar putea contribui, astfel cum s-a menționat anterior;
- promovarea la nivel internațional a standardelor în materie de protecție a vieții private ar trebui să includă:
  - (i) promovarea deplinei coerențe dintre noile instrumente internaționale și cadrul european de protecție a datelor;
  - (ii) promovarea aderării țărilor terțe, în special a SUA, la Convenția 108 a Consiliului Europei;
  - (iii) sprijinirea adoptării unui instrument internațional care să impună respectarea standardelor de protecție în cadrul activităților de spionaj. Acesta ar putea fi adoptat la nivelul Națiunilor Unite, pe baza articolului 17 din Pactul internațional cu privire la drepturile civile și politice;
- în cadrul activităților de supraveghere ar trebui introdusă obligația de a respecta, în orice moment, statul de drept și principiile necesității și proporționalității într-o societate democratică. În consecință, cadrele juridice de la toate nivelurile relevante ar trebui clarificate și, dacă este necesar, completate. Aceste cadre ar trebui să includă mecanisme de control adecvate și suficient de puternice;
- instituțiile UE și toate entitățile relevante din statele membre sunt, de asemenea, responsabile, în calitate de operatori de date, pentru asigurarea unei securități IT eficiente. Aceasta implică efectuarea unei evaluări a riscurilor pentru securitatea datelor, la nivelul corespunzător, și necesită, de asemenea, încurajarea cercetării mecanismelor de criptare și creșterea gradului de sensibilizare a operatorilor de date și a cetățenilor în ceea ce privește riscurile pentru viața privată ale produselor vândute sau utilizate, precum și obligarea dezvoltatorilor la utilizarea unor metode de proiectare concrete, în vederea evitării sau, cel puțin, a reducerii acestor riscuri. Uniunea Europeană ar trebui să ia inițiative de educație în ceea ce privește securitatea datelor pe internet.

Adoptat la Bruxelles, 20 februarie 2014.

Peter HUSTINX

*Autoritatea Europeană pentru Protecția Datelor*

---