I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind neutralitatea rețelei, gestionarea traficului și protecția confidențialității și a datelor cu caracter personal

(2012/C 34/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ([1]),

având în vedere Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile și organismele comunitare și privind libera circulație a acestor date ([2]), în special articolul 41 alineatul (2),

având în vedere Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice ([3]),

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

I.1. Context

1. La 19 aprilie 2011, Comisia a adoptat o comunicare pe tema internetului deschis și a neutralității rețelei în Europa ([4]).

2. Prezentul aviz poate fi considerat a fi reacția AEPD la comunicarea menționată și vizează să contribuie la continuarea dezbaterii politice din cadrul UE privind neutralitatea rețelei, în special aspecte legate de confidențialitate și protecția datelor.

([1]) JO L 281, 23.11.1995, p. 31, denumită în continuare „Directiva privind protecția datelor".
([2]) JO L 8, 12.1.2001, p. 1, denumit în continuare „Regulamentul privind protecția datelor".
([3]) JO L 201, 31.7.2002, p. 37, astfel cum a fost modificat prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (a se vedea nota de subsol 15), denumită în continuare „Directiva privind confidențialitatea în mediul electronic".
([4]) COM(2011) 222 final.

3. Avizul are la bază răspunsul ([5]) AEPD la consultarea publică a Comisiei pe tema internetului deschis și a neutralității rețelei în Europa, care a precedat comunicarea Comisiei. AEPD a luat, de asemenea, notă de recentul proiect de concluzii ale Comisiei privind neutralitatea rețelei ([6]).

I.2. **Conceptul de neutralitate a rețelei**

4. Neutralitatea rețelei se referă la o dezbatere permanentă privind necesitatea autorizării furnizorilor de servicii de internet (*Internet Service Providers*, ISP ([7])) în ceea ce privește limitarea, filtrarea sau blocarea accesului la internet sau afectarea în alt mod a performanței acestuia. Conceptul de neutralitate a rețelei pornește de la perspectiva transmiterii imparțiale a informațiilor pe internet, indiferent de conținut, destinație sau sursă, precum și de la perspectiva că utilizatorii ar trebui să poată hotărî ce aplicații, servicii și echipamente hardware doresc să utilizeze. Aceasta înseamnă că furnizorii de servicii de internet nu pot, din proprie inițiativă, să stabilească priorități sau să diminueze viteza de acces la anumite aplicații sau servicii precum cele „Peer to Peer" („P2P") etc. ([8]).

5. Filtrarea, blocarea și inspectarea traficului în rețea ridică probleme importante, adesea neglijate și trecute în plan secundar, privind confidențialitatea comunicațiilor și respectul pentru viața privată a persoanelor și confidențialitatea datelor cu caracter personal ale acestora atunci când utilizează internetul. De exemplu, anumite inspecții tehnice implică monitorizarea conținutului comunicațiilor, a site-urilor vizitate, a e-mailurilor trimise și primite, a orei când au loc operațiunile etc., ceea ce permite filtrarea comunicațiilor.

6. Prin inspectarea datelor privind comunicațiile, furnizorii de servicii de internet pot încălca confidențialitatea comunicațiilor, care este un drept fundamental, garantat prin articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (CEDO) și prin articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta"). Confidențialitatea este protejată, de asemenea, în legislația secundară a UE, respectiv articolul 5 din Directiva privind confidențialitatea în mediul electronic.

I.3. **Punctele centrale și structura avizului**

7. AEPD consideră că o dezbatere strategică serioasă privind neutralitatea rețelei trebuie să abordeze confidențialitatea comunicațiilor, precum și alte implicații asupra vieții private și protecției datelor.

8. Prezentul aviz contribuie la dezbaterea permanentă din UE. Acesta are un triplu obiectiv:

— avizul semnalează relevanța protecției datelor și a confidențialității în cadrul discuțiilor actuale privind neutralitatea rețelei. În mod special, acesta subliniază necesitatea respectării normelor existente privind confidențialitatea comunicațiilor. Ar trebui permise doar practici care respectă aceste norme;

— neutralitatea rețelei este legată de posibilitățile tehnologice relativ noi, iar experiența cu privire la modul de aplicare a cadrului juridic este redusă. Prin urmare, prezentul aviz oferă îndrumări privind modul în care furnizorii de servicii de internet aplică și respectă cadrul juridic privind protecția datelor dacă se angajează în activități de filtrare, blocare și inspectare a traficului în rețea. Astfel, avizul ar trebui să fie util furnizorilor de servicii de internet, precum și autorităților responsabile cu aplicarea cadrului juridic;

— în sfera protecției datelor și confidențialității, prezentul aviz identifică domenii care solicită acordarea unei atenții speciale și care pot necesita măsuri la nivelul UE. Acest aspect este deosebit de important în contextul dezbaterii continue la nivel european și al măsurilor strategice care ar putea fi lansate de Comisie în acest context.

([5]) În răspunsul său, AEPD a subliniat importanța luării în considerare a aspectelor privind confidențialitatea și protecția datelor, precum și alte drepturi și valori existente. Răspunsul este disponibil la: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Disponibil la http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Este inclusă furnizarea de acces atât fix, cât și mobil la internet.

([8]) Principiul nu se aplică totuși limitării de către furnizorii de servicii de internet a vitezei sau volumului de informații pe care un abonat le poate trimite sau primi, prin intermediul abonamentelor cu limite de volum sau lărgime de bandă. Prin urmare, în contextul principiului neutralității rețelei, furnizorii de servicii de internet ar putea totuși să ofere abonamente de acces la internet cu limitarea accesului pe baza unor criterii precum viteza sau volumul, în măsura în care aceasta nu implică discriminare în favoarea sau împotriva unui anumit conținut.

9. AEPD cunoaște faptul că neutralitatea rețelei ridică alte probleme, descrise în mai mare detaliu mai jos, precum cele asociate accesului la informații. Aceste probleme sunt abordate doar în măsura în care sunt asociate sau au un impact asupra protecției datelor și confidențialității.

10. Avizul este structurat astfel: Secțiunea II începe printr-o scurtă sinteză a practicilor de filtrare adoptate de furnizorii de servicii de internet. Secțiunea III prezintă cadrul juridic european privind neutralitatea rețelei. Secțiunea IV continuă cu o descriere tehnică, urmată de o evaluare a implicațiilor asupra confidențialității, în funcție de tehnica utilizată. Secțiunea V analizează detaliile practice privind aplicarea cadrului juridic european actual privind protecția datelor și confidențialitatea. Pe baza acestei analize, Secțiunea VI cuprinde sugestii privind dezvoltări strategice viitoare și identifică domeniile în care pot fi necesare clarificarea și îmbunătățirea cadrului juridic. Secțiunea VII cuprinde concluziile.

II. **NEUTRALITATEA REȚELEI ȘI POLITICILE DE GESTIONARE A TRAFICULUI**

Utilizarea în măsură din ce în ce mai mare a politicilor de gestionare a traficului

11. În mod tradițional, furnizorii de servicii monitorizează și influențează traficul în rețea doar în circumstanțe limitate. De exemplu, furnizorii de servicii de internet au aplicat inspecții tehnice și au restricționat fluxurile de informații în vederea menținerii securității rețelei, de exemplu pentru combaterea virușilor. Prin urmare, în general, internetul s-a dezvoltat menținând în același timp un grad înalt de neutralitate.

12. Totuși, în ultimii ani, unii furnizori de servicii de internet și-au arătat interesul în inspectarea traficului în rețea pentru a diferenția diferitele tipuri de trafic și pentru a aplica politici diferite acestora, de exemplu, pentru a bloca anumite servicii sau pentru a oferi acces preferențial altora. Acestea sunt denumite uneori „politici de gestionare a traficului” ([9]).

13. Motivele pentru care furnizorii de servicii de internet inspectează și diferențiază traficul sunt multiple. De exemplu, politicile de gestionare a traficului pot ajuta furnizorii de servicii de internet să gestioneze traficul în perioade de congestie ridicată, de exemplu prin acordarea unei priorități mai mari anumitor tipuri de trafic sensibil la factorul timp, precum streamingul video, și a unei priorități mai mici altor tipuri de trafic, care pot fi mai puțin sensibile la factorul timp, precum P2P ([10]). De asemenea, gestionarea traficului poate fi o modalitate prin care furnizorii de servicii internet să obțină un potențial flux de venituri, care ar putea avea diverse surse. Pe de o parte, furnizorii de servicii de internet pot percepe taxe furnizorilor de servicii de conținut, de exemplu celor ale căror servicii necesită utilizarea unei lățimi de bandă mai mare, dându-le, în schimb, prioritate (și, astfel, viteză). Aceasta înseamnă că accesarea unui anumit serviciu, de exemplu, un serviciu care furnizează materiale video la cerere, ar fi mai rapidă decât accesarea unui alt serviciu similar, care nu a aderat la transmisia de mare viteză. Venituri pot fi obținute, de asemenea, de la abonați interesați să plătească taxe mai mari (sau mai mici) pentru anumite tipuri de abonamente diferențiate. De exemplu, un abonament fără acces la P2P ar putea fi mai ieftin decât unul care oferă acces nelimitat.

14. Pe lângă motivele proprii ale furnizorilor de servicii de internet pentru utilizarea politicilor de gestionare a traficului, alte părți pot avea, de asemenea, un interes în utilizarea de către aceștia a politicilor de gestionare a traficului. Prin gestionarea rețelelor și inspectarea conținutului transmis prin instalațiile lor, furnizorii de servicii de internet își vor spori probabil capacitatea de detectare a presupuselor utilizări ilegale, de exemplu încălcarea dreptului de autor sau utilizarea materialelor pornografice.

([9]) A se vedea, de exemplu, Raportul OFCOM cu titlul „Site blocking to reduce online copyright infringement” (*Blocarea site-urilor pentru reducerea încălcării drepturilor de autor pe internet*), adoptat la 27 mai 2011, disponibil la: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Unii furnizori de servicii de internet utilizează deja un pachet de sisteme de inspecție în rețeaua lor pentru gestionarea traficului și în alte scopuri, așadar considerăm că acesta poate fi utilizat, deși aceasta ar implica un nivel crescut de complexitate și costuri pentru cei care nu operează deja astfel de servicii. Este posibil ca, pe termen scurt și mediu, sistemul DPI (*deep packet inspection*) să poată fi utilizat de furnizorii de servicii de internet de dimensiuni mai mari, dată fiind investiția de capital necesară”.

([10]) Calitatea aplicațiilor în timp real, precum streamingul video, depinde, printre altele, de latență, și anume de întârzierile datorate congestiilor în rețea.

Alte interese, inclusiv protecția datelor și confidențialitatea

15. Această tendință a declanșat o dezbatere privind legitimitatea acestui tip de practici și, în special, privind necesitatea dezvoltării în mai mare măsură în legislație a unor obligații specifice privind neutralitatea rețelei.

16. Utilizarea în măsură din ce în ce mai mare a politicilor de gestionare a traficului de către furnizorii de servicii de internet ar putea limita accesul la informații. Dacă acest comportament ar deveni o practică comună, iar utilizatorii nu ar avea posibilitatea de acces la internet fără restricții, așa cum este cazul în prezent (sau dacă acest acces ar avea un preț deosebit de ridicat), s-ar putea compromite accesul la informații și libertatea utilizatorului de a trimite și primi conținutul dorit prin aplicațiile sau serviciile alese. Un principiu obligatoriu din punct de vedere juridic privind neutralitatea rețelei ar putea evita această problemă.

17. În acest punct, AEPD ajunge la implicațiile pe care le are pentru protecția datelor și confidențialitate gestionarea traficului de către furnizorii de servicii de internet. În special:

— Atunci când furnizorii de servicii de internet prelucrează date privind traficul având ca unic scop transmiterea fluxului de informații de la expeditor către destinatar, aceștia execută, în general, o prelucrare limitată de date cu caracter personal ([11]). În același mod în care serviciul poștal prelucrează informațiile înscrise pe plicul unei scrisori, furnizorul de servicii de internet prelucrează informațiile necesare pentru a ruta comunicarea către destinatar. Aceasta nu aduce atingere cerințelor juridice privind protecția datelor și confidențialitatea comunicațiilor;

— totuși, atunci când furnizorii de servicii de internet inspectează datele de comunicații în vederea diferențierii fiecărui flux de comunicații și aplicării unor strategii specifice, care ar putea să nu fie favorabile persoanelor, implicațiile sunt mai importante. În funcție de circumstanțele fiecărui caz și de tipul de analiză efectuată, prelucrarea poate fi extrem de agresivă pentru viața privată și datele cu caracter personal ale unei persoane. Acest aspect este mai evident în cazul în care politicile de gestionare divulgă conținutul comunicațiilor prin internet ale persoanelor, inclusiv e-mailurile trimise și primite, site-urile vizitate, fișierele descărcate sau încărcate etc.

III. **PREZENTARE GENERALĂ A CADRULUI JURIDIC AL UE PRIVIND NEUTRALITATEA REȚELEI ȘI ALTE EVOLUȚII ALE POLITICILOR**

III.1. **Cadrul juridic pe scurt**

18. Până în 2009, instrumentele legislative ale UE nu conțineau dispoziții care să le interzică în mod explicit furnizorilor de servicii de internet să efectueze activități de filtrare sau blocare sau să perceapă tarife suplimentare de la abonați pentru accesul la servicii. În același timp, nu existau dispoziții care să recunoască în mod explicit această practică. Situația era, într-o anumită măsură, caracterizată de incertitudine.

19. Pachetul Telecom din 2009 a schimbat această situație, incluzând dispoziții care favorizează caracterul deschis al internetului. De exemplu, articolul 8 alineatul (4) din directiva privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice („directiva-cadru”) stabilește o obligație a autorităților de reglementare de a promova capacitatea utilizatorilor finali de a avea acces liber la conținut, aplicații sau servicii ([12]). Această dispoziție se aplică rețelei în ansamblul ei, nu la nivelul furnizorilor individuali. Recentul proiect de concluzii ale Consiliului a evidențiat, de asemenea, necesitatea menținerii caracterului deschis al internetului ([13]).

([11]) Sunt excluse operațiunile care vizează consolidarea securității rețelei și detectarea traficului care aduce prejudicii, precum și operațiunile necesare pentru facturare și interconectare. De asemenea, sunt excluse obligațiile care derivă din Directiva privind păstrarea datelor, directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea de servicii de comunicații electronice puse la dispoziția publicului sau de rețele de comunicații publice, și de modificare a Directivei 2002/58/CE (JO L 105, 13.4.2006, p. 54) (denumită în continuare „Directiva privind păstrarea datelor”).

([12]) Directiva 2002/21/CE din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, modificată prin Directiva 2009/140/CE și prin Regulamentul (CE) nr. 544/2009 (JO L 337, 18.12.2009, p. 37).

([13]) A se vedea punctul 3 litera (e), unde Consiliul recunoaște: „Necesitatea de a păstra caracterul deschis al internetului, garantând în același timp că poate continua să furnizeze servicii de înaltă calitate într-un cadru care promovează și respectă drepturile fundamentale, precum libertatea de expresie și libertatea de a desfășura o activitate comercială” și punctul 8 litera (d), care invită statele membre „să promoveze caracterul neutru și deschis al internetului ca obiectiv al politicilor proprii”.

20. Directiva privind serviciul universal ([14]) cuprinde obligații mai concrete. Articolele 20 și 21 prevăd cerințe de transparență în ceea ce privește limitările accesului și/sau ale utilizării serviciilor și aplicațiilor. Directiva prevede, de asemenea, niveluri minime ale calității serviciilor.

21. Pentru practicile furnizorilor de servicii de internet care implică inspecția comunicațiilor persoanelor, considerentul 28 al directivei de modificare a Directivei privind confidențialitatea în mediul economic și a Directivei privind serviciul universal ([15]) subliniază că „în funcție de tehnologia utilizată și de tipul de limitări, astfel de limitări ar putea necesita acordul utilizatorului, în conformitate cu Directiva privind confidențialitatea în mediul electronic". Prin urmare, considerentul 28 reamintește necesitatea acordului, în temeiul articolului 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic pentru toate limitările bazate pe monitorizarea comunicațiilor. Secțiunea IV de mai jos analizează în mai mare detaliu aplicarea articolului 5 alineatul (1) și cadrul juridic global privind confidențialitatea și protecția datelor.

22. În sfârșit, articolul 22 alineatul (3) din Directiva privind serviciul universal autorizează în prezent autoritățile naționale de reglementare să impună furnizorilor de servicii de internet, dacă este necesar, cerințe minime de calitate a serviciilor pentru a împiedica degradarea serviciilor și perturbarea sau diminuarea vitezei traficului în rețelele publice.

23. Din cele de mai sus reiese că la nivelul UE se dorește foarte mult un internet deschis [a se vedea articolul 8 alineatul (4) din directiva-cadru]. Totuși, acest obiectiv al politicilor, care se aplică rețelei în ansamblu, nu este asociat în mod direct interdicțiilor sau obligațiilor impuse furnizorilor de servicii de internet individuali. Cu alte cuvinte, un furnizor de servicii de internet ar putea aplica politici de gestionare a traficului care pot exclude accesul la anumite aplicații, cu condiția ca utilizatorii finali să fie pe deplin informați, și să își fi exprimat consimțământul în mod liber, specific și neechivoc.

24. Situația poate fi diferită, în funcție de statele membre. În unele state membre, furnizorii de servicii de internet pot aplica, în anumite condiții, politici de gestionare a traficului, de exemplu blocarea unor aplicații precum VoIP (ca parte a unui abonament de internet mai ieftin), sub rezerva ca utilizatorii să își exprime consimțământul în cunoștință de cauză, în mod liber, specific și neechivoc. Alte state membre au ales să consolideze principiul neutralității rețelei. De exemplu, în iulie 2011, parlamentul olandez a adoptat o lege care interzice, în general, furnizorilor să împiedice sau să diminueze viteza aplicațiilor sau serviciilor pe internet (precum VoIP), cu excepția cazului în care o astfel de măsură este necesară pentru a minimiza efectele congestiei, din motive de integritate sau securitate, pentru a combate spam-ul sau în conformitate cu un ordin judecătoresc ([16]).

III.2. **Comunicarea privind neutralitatea rețelei**

25. În comunicarea privind neutralitatea rețelei ([17]), Comisia Europeană a concluzionat că situația privind neutralitatea rețelei necesită monitorizare și analiză suplimentară. Această politică a fost numită „de expectativă", înainte de a fi luate în considerare măsuri suplimentare de reglementare.

([14]) Directiva 2002/22/CE, astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (JO L 337, 18.12.2009, p. 11). A se vedea, de asemenea, articolul 1 alineatul (3), care prevede că directiva nici nu autorizează, nici nu interzice furnizorilor de servicii de internet să limiteze accesul utilizatorilor finali la servicii și aplicații și/sau utilizarea acestora, în cazul în care sunt permise de legislația națională și respectă legislația comunitară, dar stabilește o obligație de a furniza informații cu privire la limitările respective.

([15]) Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului.

([16]) Modificarea inițială a legii olandeze este disponibilă la: https://zoek.officielebekendmakingen.nl/kst-32549-A.html Motivele relatate de presă cu privire la această opțiune de politică nu au făcut referire la considerente legate de protecția datelor și confidențialitate, ci la motive în legătură cu asigurarea că utilizatorii nu sunt privați de acces și nu li se oferă acces limitat la informații. Astfel, se pare că aspecte asociate accesului la informații au motivat această modificare.

([17]) A se vedea nota de subsol nr. 4.

26. Comunicarea Comisiei recunoștea că toate măsurile și acțiunile de reglementare suplimentare ar urma să facă obiectul unei evaluări aprofundate a aspectelor legate de confidențialitate și protecția datelor. În proiectul de concluzii ale Consiliului sunt menționate, de asemenea, aspectele de interes privind protecția datelor și confidențialitatea ([18]).

27. Întrebarea care trebuie evaluată dintr-o perspectivă a confidențialității și a protecției datelor, este dacă o politică de expectativă este suficientă. Deși cadrul juridic privind confidențialitatea și protecția datelor prevede, în prezent, anumite garanții, în special prin principiul confidențialității comunicațiilor, pare necesar să se monitorizeze îndeaproape nivelul de conformitate și să se emită orientări privind anumite aspecte care nu sunt suficient de clare. De asemenea, ar trebui prezentate anumite idei, cu privire la modul în care cadrul poate fi clarificat și îmbunătățit în continuare, având în vedere evoluțiile tehnologice. În cazul în care în urma monitorizării se observă că piața evoluează către inspecția masivă, în timp real, a comunicațiilor și a aspectelor legate de respectarea cadrului, vor fi necesare măsuri legislative. Propuneri concrete vor fi formulate în această privință în Secțiunea VI.

IV. **CADRUL TEHNIC ȘI IMPLICAȚIILE PRIVIND PROTECȚIA DATELOR ȘI CONFIDENȚIALITATEA**

28. Înainte de a aprofunda subiectul, este important să existe o imagine cât mai clară a tehnicilor de inspecție care pot fi utilizate de furnizorii de servicii de internet pentru a efectua activități de gestionare a traficului, precum și a modului în care aceste tehnici pot afecta principiul neutralității rețelei. Implicațiile în ceea ce privește protecția datelor și confidențialitatea care derivă din astfel de tehnici variază considerabil în funcție de tehnica sau tehnicile utilizate. Prezentarea cadrului tehnic este necesară pentru a înțelege și aplica în mod corect cadrul juridic privind protecția datelor descris la Secțiunea V. Totuși, trebuie menționat că acesta este un domeniu complex și în permanentă schimbare. Prin urmare, descrierea de mai jos nu dorește să fie exhaustivă și complet actualizată, ci doar să furnizeze informațiile tehnice indispensabile pentru înțelegerea raționamentului juridic.

IV.1. **Transmiterea de informații prin internet: elemente de bază**

29. Atunci când un utilizator transmite o comunicație prin internet, informațiile transmise sunt împărțite în pachete. Aceste pachete sunt transmise prin intermediul internetului de la expeditor la destinatar. Fiecare pachet va cuprinde, printre altele, informații referitoare la sursă și la destinație. De asemenea, furnizorii de servicii de internet ar putea include aceste pachete în straturi și protocoale suplimentare ([19]), care vor fi utilizate pentru a gestiona diversele fluxuri de trafic în cadrul propriei rețele.

30. Pentru a reveni la analogia cu scrisoarea transmisă prin serviciile poștale tradiționale, utilizarea unui protocol de transmitere în rețea echivalează cu includerea conținutului unei scrisori într-un plic, cu o adresă de destinație care urmează să fie citită, și ulterior trimisă de serviciul poștal. Serviciul poștal poate utiliza protocoale suplimentare în tranziturile sale interne, pentru a gestiona toate plicurile care trebuie trimise, urmărindu-se ca fiecare plic să ajungă la destinația înscrisă inițial de expeditor. Utilizând această analogie, fiecare pachet are două părți, prima fiind reprezentată de „încărcătura utilă IP" (*IP payload*) care cuprinde conținutul comunicației și reprezintă echivalentul scrisorii. Acesta cuprinde informații adresate exclusiv destinatarului. Cea de a doua parte a pachetului este „antetul IP" (*IP header*) care cuprinde, printre altele, adresa destinatarului și a expeditorului, și reprezintă echivalentul plicului. Antetul IP permite furnizorilor de servicii de internet și altor intermediari să transmită încărcătura utilă de la adresa sursă la adresa de destinație.

31. Furnizorii de servicii de internet și alți intermediari se asigură că pachetele IP sunt transmise de-a lungul rețelei prin noduri care citesc informațiile din antetul IP, le compară cu tabele de rutare, iar apoi le trimit către următorul nod până la destinație. Acest proces este efectuat în rețea prin utilizarea unei

([18]) A se vedea punctul 4 litera (e), unde Consiliul menționează: „Existența anumitor preocupări, majoritatea din partea consumatorilor și autorităților responsabile cu protecția datelor, în ceea ce privește protecția datelor cu caracter personal".

([19]) Astfel cum se descrie în continuare în secțiunea IV.2, aceste protocoale codează informațiile transmise complet, într-un mod asupra căruia s-a convenit, pentru ca părțile implicate în comunicare să se poată înțelege reciproc, precum HTTP, FTP etc.

abordări „a celor mai bune eforturi fără consum de memorie”, întrucât toate pachetele care ajung la un nod sunt tratate în mod neutru. După transmiterea pachetelor către următorul nod, nu mai este necesar să se păstreze informații suplimentare în router ([20]).

IV.2. **Tehnici de inspecție**

32. Astfel cum s-a explicat mai sus, furnizorii de servicii de internet citesc antetele IP în scopul transmiterii acestora către destinație. Totuși, conform celor expuse anterior, analiza traficului (care implică antetele IP și încărcăturile utile IP) poate fi efectuată în alte scopuri și cu alte tipuri de tehnologii. Noile tendințe pot include, de exemplu, diminuarea vitezei anumitor aplicații folosite de utilizatori, precum P2P, sau, ca alternativă, îmbunătățirea vitezei traficului pentru anumite servicii, precum serviciile de furnizare de materiale video la cerere pentru abonații premium. Deși toate tehnicile de inspecție efectuează *în mod tehnic* inspecția pachetelor, acestea implică diverse niveluri cu caracter invaziv diferit. Există două categorii principale de tehnici de inspecție. Una este bazată doar pe antetul IP, cea de a doua și pe încărcătura utilă IP.

Pe baza informațiilor privind antetul IP. Inspecția unui antet de pachet IP indică anumite câmpuri care pot permite furnizorilor de servicii de internet să aplice un număr de politici specifice pentru a gestiona traficul. Aceste tehnici bazate doar pe inspecția antetelor IP prelucrează date care, în principiu, sunt destinate transmiterii informațiilor, într-un alt scop (și anume, diferențierea traficului). Citind adresa IP sursă, furnizorul de servicii de internet o poate asocia cu un abonat concret și poate aplica anumite politici specifice, de exemplu transmiterea pachetului printr-un link mai rapid sau mai lent. Citind adresa IP de destinație, furnizorul de servicii de internet poate aplica, de asemenea, politici specifice, de exemplu blocarea sau filtrarea accesului la anumite site-uri web.

Pe baza unei inspecții mai detaliate. O inspecție detaliată a pachetelor permite furnizorului de servicii de internet să acceseze informații adresate exclusiv destinatarului comunicației. Revenind la exemplul serviciului poștal, această abordare este echivalentă deschiderii plicului și citirii interiorului scrisorii, pentru a efectua o analiză a conținutului comunicației (care se află în interiorul pachetelor IP) în vederea aplicării unei politici specifice a rețelei. Există metode diferite de desfășurare a inspecției, fiecare prezentând diverse amenințări la adresa persoanei vizate.

— *Inspecție detaliată a pachetelor pe baza analizei protocoalelor și a registrelor statistice*. Pe lângă protocolul IP, care are ca scop facilitarea transmiterii datelor prin internet, există protocoale suplimentare care codează informațiile transmise în mod consimțit (transport, sesiune, prezentare și aplicare etc.). Obiectivul acestor protocoale este de a asigura că părțile implicate în comunicare se pot înțelege reciproc. De exemplu, există anumite protocoale asociate navigării pe internet ([21]), altele sunt pentru transferul de fișiere ([22]) etc. Prin urmare, tehnicile de inspecție bazate pe inspectarea protocoalelor și în combinație cu analiza statistică urmăresc să găsească tipare sau amprente specifice, care stabilesc ce protocoale sunt prezente ([23]). Aceste tehnici de inspecție permit furnizorilor de servicii de internet să înțeleagă tipul de comunicație (e-mail, navigare pe internet, încărcare de fișiere) și, în anumite cazuri, să identifice serviciul specific sau aplicația utilizată, precum în cazul anumitor comunicații VoIP, în care protocoalele utilizate sunt extrem de specifice unui vânzător sau unui furnizor de servicii concret. Cunoașterea tipului de comunicație în sine poate permite furnizorilor de servicii de internet să aplice politici concrete de gestionare a traficului, de exemplu pentru a bloca traficul pe internet. Acesta poate fi, de asemenea, primul pas în autorizarea furnizorului de servicii de internet să efectueze analize suplimentare care pot necesita acces deplin la metadatele și conținutul comunicației.

([20]) Totuși, echipamentul rețelei de internet utilizează protocoale de transmitere care înregistrează activitatea, prelucrează statistici referitoare la traficul și efectuează schimburi de informații cu alte echipamente de rețea pentru a ruta pachetele IP utilizând cea mai eficientă cale. De exemplu, atunci când un link este congestionat sau avariat, iar un router primește aceste informații, acesta va actualiza tabelul său de rutare cu o alternativă care nu utilizează respectivul link. Trebuie menționate, de asemenea, colectarea și prelucrarea care pot fi efectuate, în anumite cazuri, în scopul facturării sau chiar în conformitate cu cerințele prevăzute în directiva privind păstrarea datelor.

([21]) HTTP – Hypertext transfer protocol (protocol de transfer hipertext) sau HTML – Hypertext Markup Language (limbaj de marcare a hipertextului).

([22]) FTP – File transfer protocol (protocol de transfer fișiere).

([23]) Există diverse metode de identificare a protocoalelor utilizate. De exemplu, este posibilă efectuarea unei căutări în câmpuri specifice din protocoalele interne, de exemplu pentru a identifica porturile utilizate pentru efectuarea comunicării. O caracterizare statistică a fluxului comunicației poate fi dedusă, de asemenea, din analiza anumitor câmpuri specifice, corelarea protocoalelor utilizate simultan între două adrese IP.

— *Inspecția detaliată a pachetelor pe baza analizei conținutului comunicației.* În sfârșit, există posibilitatea inspectării metadatelor ([24]) și a conținutului comunicației. Această tehnică constă în interceptarea tuturor pachetelor IP care fac parte din fluxul inițial al comunicației, astfel încât conținutul inițial al comunicației să poată fi integral reconstruit și analizat. De exemplu, pentru a detecta un conținut ilegal sau care cauzează prejudicii, precum virușii, pornografia infantilă etc., este necesară reconstruirea conținutului, astfel încât acesta să poată fi analizat. Trebuie remarcat că, uneori, comunicația poate fi criptată integral în mod intenționat de către părțile interesate, iar această practică va împiedica furnizorii de servicii de internet să efectueze analiza conținutului comunicației.

IV.3. **Implicațiile privind protecția datelor și confidențialitatea**

33. Tehnicile de inspecție bazate pe antetele IP și, în special, cele bazate pe inspecția pachetelor implică monitorizarea și filtrarea acestor date și au implicații grave asupra vieții private și protecției datelor. Acestea pot, de asemenea, intra în conflict cu dreptul la confidențialitatea informațiilor.

34. Citirea comunicațiilor persoanelor are, în sine, implicații grave asupra confidențialității și protecției datelor. Totuși, problema este mai amplă, întrucât, în funcție de efectele urmărite prin monitorizare și interceptare, implicațiile privind confidențialitatea pot spori. Într-adevăr, simpla inspectare a informațiilor, de exemplu pentru a garanta că sistemul funcționează corect, și inspectarea comunicațiilor pentru a aplica politici care pot avea un impact asupra persoanelor, nu reprezintă același lucru. Atunci când este posibil ca politicile privind traficul și selecția să urmărească doar evitarea congestiei în rețea, nu vor exista în general implicații majore pentru viața privată a persoanei. Totuși, politicile de gestionare a traficului pot urmări blocarea anumitor informații de conținut sau pot influența comunicația, de exemplu prin publicitate comportamentală. În aceste situații, efectele sunt mai intruzive. Preocuparea devine mai critică atunci când se realizează că acest tip de informații nu este colectat pentru un grup restrâns de persoane, ci în mod general, pentru toți clienții furnizorului de servicii de internet ([25]). Adoptarea de către toți furnizorii de servicii de internet a tehnicilor de filtrare ar putea conduce la o monitorizare generalizată a utilizării internetului. În plus, dacă accentul s-ar pune pe tipul de informații prelucrate, riscurile la adresa confidențialității sunt evident, ridicate, întrucât numeroase informații colectate sunt, cel mai probabil, foarte sensibile și, în urma colectării, sunt disponibile furnizorilor de servicii de internet și celor care doresc să obțină informații de la aceștia. În plus, informațiile pot fi extrem de valoroase și din punct de vedere comercial. În sine, aceasta reprezintă un risc ridicat de denaturare a funcțiilor, în care scopurile inițiale ar putea evolua cu ușurință în scopuri comerciale sau alt tip de exploatare a informațiilor colectate.

35. Aplicarea corectă a tehnicilor de monitorizare, inspecție și filtrare trebuie efectuată în conformitate cu garanțiile aplicabile privind protecția datelor și confidențialitatea, care prevăd limite în legătură cu ce se poate face și în ce circumstanțe. Urmează în continuare o prezentare generală a garanțiilor aplicabile în cadrul juridic european actual privind confidențialitatea și protecția datelor.

V. **APLICAREA CADRULUI JURIDIC AL UE PRIVIND CONFIDENȚIALITATEA ȘI PROTECȚIA DATELOR**

36. Cadrul juridic al UE privind protecția datelor este neutru din punct de vedere tehnologic; ca atare, acesta nu reglementează tehnici de inspecție specifice, precum cele descrise mai sus. Directiva privind confidențialitatea în mediul electronic reglementează confidențialitatea în furnizarea serviciilor de

([24]) Fiecare protocol are anumite câmpuri specifice în antet care furnizează informații suplimentare informale cu privire la comunicația transmisă. Prin urmare, conținutul acestor câmpuri poate fi denumit în continuare „metadatele comunicației". Un exemplu de astfel de câmpuri poate fi numărul portului utilizat. De exemplu, dacă numărul este 80, este foarte probabil ca tipul comunicației să fie navigarea internet.

([25]) Bineînțeles, nu doar furnizorii de servicii internet au capacități de urmărire. Dimpotrivă, și furnizorii de rețele de publicitate pot urmări utilizatorii pe site-urile internet, prin utilizarea modulelor cookie de la părți terțe. A se vedea, de exemplu, un articol publicat recent în mediul academic, în care se arată că Google este prezent pe 97 din primele 100 de site-uri, ceea ce înseamnă că Google poate urmări utilizatorii care nu au dezactivat modulele cookie de la părți terțe atunci când navighează pe aceste site-uri populare. A se vedea: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, *Flash Cookies and Privacy II*: Now with HTML5 and ETag Respawning (*Modulele flash cookie și confidențialitatea: Acum cu HTML5 și ETag Respawning*) (29 iulie 2011). Disponibil pe site-ul SSRN: http://ssrn.com/abstract=1898390. Urmărirea utilizatorilor prin module cookie de la părți terțe a fost abordată de Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. A se vedea Avizul nr. 2/2010 privind publicitatea comportamentală online, adoptat la 22 iunie 2010 (WP 171).

comunicații electronice în rețelele publice (în general, acces internet și telefonie) ([26]), iar directiva privind protecția datelor reglementează prelucrarea datelor în general. În ansamblu, acest cadru juridic stabilește diverse obligații aplicabile furnizorilor de servicii de internet care prelucrează și monitorizează traficul și datele de comunicații.

V.1. **Temeiuri juridice pentru prelucrarea datelor de trafic și conținut**

37. Conform legislației în materie de protecția datelor, prelucrarea datelor cu caracter personal, precum, în acest caz, prelucrarea datelor privind traficul și comunicațiile, necesită un temei juridic adecvat. Pe lângă această cerință generală, se pot aplica cerințe specifice în anumite cazuri.

38. În acest caz, tipul de date cu caracter personal prelucrate de furnizorii de servicii de internet se referă la datele de trafic și conținutul comunicațiilor. Atât conținutul informațiilor, cât și datele de trafic sunt protejate de dreptul la confidențialitatea corespondenței, garantat prin articolul 8 din CEDO și articolele 7 și 8 din Cartă. În special, articolul 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic, cu titlul „Confidențialitatea comunicațiilor", solicită statelor membre să asigure confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau unor servicii publice de comunicații electronice. În același timp, articolul 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic prevede că prelucrarea datelor de trafic și de conținut de către furnizorii de servicii de internet poate fi autorizată, în anumite circumstanțe, cu acordul utilizatorilor. Aceasta se realizează prin introducerea unei interdicții privind „ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către persoane altele decât utilizatorul, fără acordul utilizatorului în cauză, cu excepția cazurilor în care acest lucru este permis în temeiul articolului 15 alineatul (1)". Această idee este dezvoltată în continuare în cele ce urmează.

39. Pe lângă acordul utilizatorilor în cauză, directiva privind confidențialitatea în mediul electronic prevede alte motive care pot legitima prelucrarea de către furnizorii de servicii de internet a datelor de comunicații și trafic. Temeiurile juridice relevante pentru prelucrarea în acest caz sunt: (i) furnizarea serviciului; (ii) garantarea securității serviciului; și (iii) minimizarea congestiei. Alte motive posibile de legitimare a politicilor de gestionare pe baza datelor privind traficul și comunicațiile sunt discutate în continuare la punctul (iv).

(i) Temeiuri juridice pentru furnizarea serviciului

40. Astfel cum se ilustrează în Secțiunea IV, furnizorii de servicii de internet prelucrează informațiile privind antetele IP în scopul transmiterii fiecărui pachet IP către destinație. Alineatele (1) și (2) de la articolul 6 din Directiva privind confidențialitatea în mediul electronic prevăd prelucrarea datelor de trafic în scopul transmiterii unei comunicații. Prin urmare, furnizorii de servicii de internet pot prelucra informațiile necesare pentru furnizarea serviciului.

(ii) Temeiuri juridice pentru garantarea securității serviciului

41. În temeiul articolului 4 din Directiva privind confidențialitatea în mediul electronic, unui furnizor de servicii de internet i se impune obligația generală de a lua măsurile adecvate pentru a garanta securitatea serviciilor sale. Practica filtrării virușilor poate implica prelucrarea antetelor IP și a încărcăturii utile IP. Având în vedere faptul că articolul 4 din directiva privind confidențialitatea în mediul electronic solicită furnizorilor de servicii de internet să asigure securitatea rețelei, prezenta dispoziție legitimează tehnicile de inspecție pe baza antetelor IP și a conținutului, care urmăresc strict acest scop. În practică, aceasta înseamnă că, în limitele prevăzute de principiul proporționalității (a se vedea Secțiunea V.3), furnizorii de servicii de internet se pot angaja în monitorizarea și filtrarea datelor comunicațiilor pentru a elimina virușii și pentru a asigura în general securitatea rețelei ([27]).

([26]) Considerentul 10 din directiva privind confidențialitatea în mediul electronic are următorul conținut: „În sectorul comunicațiilor electronice, Directiva 95/46/CE se aplică în special acelor chestiuni care privesc protejarea drepturilor și libertăților fundamentale care nu sunt acoperite în mod anume de dispozițiile prezentei directive, inclusiv obligațiile de control și drepturile persoanelor individuale". De asemenea, considerentul 17 este relevant pentru consimțământul persoanei vizate: „În sensul prezentei directive, consimțământul acordat de un utilizator sau un abonat, indiferent dacă acesta din urmă este o persoană fizică sau juridică, trebuie să aibă aceeași însemnătate ca și consimțământul acordat de subiectul datelor, așa cum este definit și specificat de Directiva 95/46/CE".

([27]) Avizul nr. 2/2006 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal privind probleme de protecție a confidențialității asociate furnizării de servicii de filtrare a e-mail-urilor, adoptat la 21 februarie 2006 (WP 118). În prezentul aviz, Grupul de lucru consideră că utilizarea de filtre în sensul articolului 4 poate fi compatibilă cu articolul 5 din Directiva privind confidențialitatea în mediul electronic.

(iii) Temeiuri juridice pentru minimizarea efectelor congestiei

42. *Motivația* acestui temei juridic se găsește la considerentul 22 al Directivei privind confidențialitatea în mediul electronic, care explică interdicția privind stocarea comunicațiilor de la articolul 5 alineatul (1). Nu sunt interzise stocările automate, intermediare și temporare, în măsura în care au are loc în unicul scop de efectuare a transmisiei și nu durează mai mult decât este necesar pentru transmitere și gestionarea traficului și în măsura în care confidențialitatea informațiilor rămâne garantată.

43. În cazul în care există o congestie, apare întrebarea dacă furnizorii de servicii de internet pot lua în considerare scăderea sau întârzierea aleatorie a traficului sau mai degrabă diminuarea vitezei comunicațiilor care nu sunt sensibile la factorul timp, de exemplu P2P sau traficul de e-mail, permițând, de exemplu, o calitate acceptabilă a traficului de voce.

44. Având în vedere interesul global al societății în garantarea unei rețele utilizabile de comunicații, furnizorii de servicii de internet pot susține că stabilirea unor priorități sau strangularea traficului pentru a aborda congestia constituie o măsură legitimă, necesară pentru furnizarea unui serviciu adecvat. Aceasta înseamnă că, în aceste cazuri și în acest scop, ar exista un temei juridic general pentru prelucrarea datelor cu caracter personal și că acordul utilizatorilor nu mai este necesar.

45. În același timp, capacitatea de a interveni în acest mod nu este nerestricționată. În cazul în care furnizorii de servicii de internet trebuie să inspecteze comunicațiile, din perspectiva confidențialității și aplicând cu strictețe principiul proporționalității, aceștia trebuie să utilizeze metoda cea mai puțin intruzivă disponibilă în acest scop (evitarea inspecției aprofundate a pachetelor) și trebuie să o aplice doar atât timp cât este necesar pentru a soluționa problema de congestie.

(iv) Temeiuri juridice pentru prelucrarea datelor în alte scopuri

46. Furnizorii de servicii de internet ar putea, de asemenea, să inspecteze datele de trafic și de conținut în alte scopuri, de exemplu prin oferirea de abonamente specifice (de exemplu, un abonament care limitează accesul la P2P sau un abonament cu o viteză mai mare pentru anumite aplicații). Inspecția și utilizarea suplimentară a datelor privind comunicațiile și traficul în alte scopuri decât furnizarea serviciului sau asigurarea securității acestuia și a absenței congestiei sunt permise doar în condiții stricte, în conformitate cu cadrul juridic.

47. Cadrul juridic este reprezentat în special de articolul 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic, care solicită acordul utilizatorilor în cauză pentru a asculta, înregistra, stoca sau alte tipuri de interceptare sau supraveghere a datelor asociate privind comunicațiile și traficul. Practic, acest lucru înseamnă că acordul utilizatorilor implicați într-o comunicație este necesar pentru a legitima prelucrarea datelor privind traficul și comunicațiile, în temeiul articolului 5 alineatul (1).

48. Astfel cum s-a explicat mai sus, aplicarea tehnicilor de inspecție și de filtrare se bazează pe antete IP, care constituie datele de trafic, sau pe inspecția aprofundată a pachetelor, care implică și încărcăturile utile IP și constituie date de comunicație. Prin urmare, în principiu, aplicarea unor astfel de tehnici în alte scopuri decât furnizarea serviciului sau securitatea este interzisă cu excepția cazului în care un temei legitim permite procesarea, precum consimțământul [articolul 5 alineatul (1)]. Un exemplu în care articolul 5 alineatul (1) se aplică este cazul în care un furnizor de servicii de internet decide să ofere clienților un tarif redus pentru accesul la internet, în schimbul acceptării publicității comportamentale, al utilizării inspecției aprofundate a pachetelor și, astfel, a datelor privind comunicațiile. Acordul real, specific și informat este, prin urmare, necesar în temeiul articolului 5 alineatul (1).

49. De asemenea, articolul 6 din Directiva privind confidențialitatea în mediul electronic, cu titlul „Datele de transfer", prevede anumite norme aplicabile în mod specific datelor de trafic. În special, acesta prevede

posibilitatea ca furnizorii de servicii de internet să prelucreze datele de trafic pe baza acordului utilizatorilor de a primi servicii cu valoare adăugată ([28]). Această dispoziție prevede cerința referitoare la consimțământ prevăzută în articolul 5 alineatul (1) în cazul în care traficul prezintă interes.

50. Practic, nu poate fi oricând ușor să se determine, de exemplu, în ce cazuri este necesar consimțământul sau în ce cazuri securitatea rețelei poate legitima prelucrarea, în special dacă scopul tehnicilor de inspecție este dublu (de exemplu, evitarea congestiei și furnizarea de servicii cu valoare adăugată). Trebuie subliniat că acordul nu poate fi considerat drept o modalitate facilă și sistemică de conformitate cu principiile privind protecția datelor.

51. Experiența cu privire la aplicarea cadrului și, în special, cu privire la diversele aspecte subliniate mai sus este redusă. Acesta este un domeniu în care sunt esențiale orientări suplimentare, astfel cum s-a detaliat în Secțiunea VI. De asemenea, există alte aspecte relevante legate de obținerea acordului care necesită o atenție specială. Acestea sunt descrise mai jos.

V.2. **Aspecte legate de oferirea consimțământului informat ca temei juridic**

52. Acordul necesar în temeiul articolelor 5 și 6 din Directiva privind confidențialitatea în mediul electronic are același înțeles ca cel al consimțământului persoanei vizate, astfel cum este definit și specificat de Directiva 95/46/CE ([29]). Conform articolului 2 litera (h) din Directiva privind protecția datelor, „consimțământul persoanei vizate" înseamnă „orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc". Recent, rolul consimțământului și cerințele ca acesta să fie valid au fost abordate de Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal în Avizul nr. 15/2011 privind consimțământul ([30]).

53. Furnizorii de servicii de internet care solicită consimțământul pentru a efectua activități de inspectare și filtrare a traficului și a datelor de conținut trebuie să se asigure, prin urmare, că acesta este liber și specificat și că este o indicație pe deplin informată a dorințelor persoanei în cauză, ceea ce înseamnă acordul acesteia privind prelucrarea de date cu caracter personal care o privesc. Considerentul 17 din Directiva privind confidențialitatea în mediul electronic reafirmă acest lucru „Consimțământul poate fi acordat prin orice metodă potrivită acestui scop, care oferă indicații specifice și clare, acordate prin proprie voință, despre dorința utilizatorului, inclusiv prin bifarea unei căsuțe la vizitarea unui site Internet". În cele ce urmează, sunt prezentate mai multe exemple practice privind semnificația în acest context a acordului liber, specific și informat.

Consimțământul: Manifestare de voință liberă, specifică și informată

54. *Consimțământul liber*. Utilizatorii nu trebuie să fie afectați de constrângeri care asociază consimțământul cu abonamentul de internet pe care îl doresc.

55. Consimțământul persoanelor vizate nu ar fi liber dacă acestea ar fi nevoite să fie de acord cu monitorizarea datelor privind propriile comunicații pentru a obține accesul la un serviciu de comunicații. Afirmația ar fi cu atât mai mult valabilă cu cât *toți* furnizorii de pe o anumită piață ar efectua activități de gestionare a traficului în scopuri care depășesc securitatea rețelei. Singura opțiune rămasă ar fi aceea de a nu avea niciun abonament pentru servicii de internet. Având în vedere că internetul a devenit un

([28]) Considerentul 18 din directivă cuprinde o dispoziție care exemplifică serviciile cu valoare adăugată. Nu este clar dacă serviciile cărora li se aplică cerințele de gestionare a traficului pot fi interpretate ca făcând parte din listă. Se poate interpreta că politicile de gestionare a traficului care urmăresc acordarea unei priorități mai mari unui anumit conținut conferă o calitate serviciului. De exemplu, gestionarea traficului care implică doar prelucrarea antetelor IP și are ca scop furnizarea de servicii de jocuri la prețuri ridicate, în cadrul cărora traficul personal al utilizatorilor în rețea în legătură cu jocurile este prioritar, poate fi considerată drept un serviciu cu valoare adăugată. Pe de altă parte, nu este deloc clar dacă se poate considera la fel pentru gestionarea traficului pentru a strangula anumite tipuri de trafic, de exemplu pentru a diminua viteza traficului P2P.

([29]) A se vedea considerentul 17 și articolul 2 litera (f) din Directiva privind confidențialitatea în mediul electronic.

([30]) Adoptat la 13 iulie 2011 (WP 187).

instrument esențial, atât în scopuri profesionale, cât și de petrecere a timpului liber, absența oricărui tip de abonament la un serviciu de internet nu constituie o alternativă valabilă. Rezultatul ar fi acela că persoanele vizate nu ar avea nicio opțiune reală, și anume nu și-ar putea exprima consimțământul în mod liber ([31]).

56. AEPD consideră că există o necesitate clară ca autoritățile naționale și Comisia să monitorizeze piața, în special pentru a stabili dacă acest scenariu – și anume, asocierea de către furnizori a serviciilor de telecomunicații cu monitorizarea comunicațiilor – devine dominant. Furnizorii ar trebui să ofere servicii alternative, inclusiv un abonament de internet care să nu fie supus gestionării traficului, fără a impune costuri mai mari persoanelor.

57. *Consimțământul specific*. Nevoia ca un consimțământ să fie specific impune în acest caz ca furnizorii de servicii de internet să solicite consimțământul pentru monitorizarea datelor privind comunicațiile și traficul într-un mod clar și distinctiv. Potrivit Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, „pentru a fi specific, consimțământul trebuie să fie inteligibil: acesta trebuie să se refere în mod clar și precis la domeniul de aplicare și consecințele prelucrării datelor. Consimțământul nu poate viza un set deschis de activități de prelucrare. Aceasta înseamnă, cu alte cuvinte, că contextul în care este aplicat consimțământul este limitat". Există probabilitatea să nu se obțină un consimțământ specific în cazul în care consimțământul pentru inspecția datelor privind traficul comunicațiile este inclus în consimțământul general de abonare la serviciu. Dimpotrivă, specificitatea impune utilizarea unor metode directe de obținere a consimțământului, precum un formular de consimțământ specific sau o casetă separată destinată în mod clar scopului monitorizării (mai degrabă decât introducerea acestor informații în condițiile generale ale contractului și solicitarea semnării contractului în forma sa actuală).

58. *Consimțământul informat*. Pentru a fi valabil, consimțământul trebuie să fie informat. Necesitatea de a furniza informații prealabile adecvate derivă nu doar din Directiva privind confidențialitatea în mediul electronic și din Directiva privind protecția datelor, ci și din articolele 20 și 21 din Directiva privind serviciul universal, astfel cum a fost modificată prin Directiva 2009/136/CE ([32]). Necesitatea informării și a consimțământului a fost exprimată în mod expres în considerentul 28 din Directiva 2009/136/CE: „Utilizatorii ar trebui să fie în orice caz pe deplin informați cu privire la toate limitările impuse de către furnizorul de servicii și/sau de rețea cu privire la utilizarea serviciilor de comunicații electronice. Astfel de informații ar trebui, la alegerea furnizorului, să precizeze fie tipul de conținut, aplicații sau servicii vizate, fie aplicațiile sau serviciile individuale, fie ambele". Acesta prevede, în continuare, că: „În funcție de tehnologia utilizată și de tipul de limitări, astfel de limitări ar putea necesita acordul utilizatorului, în conformitate cu Directiva 2002/58/CE."

59. Având în vedere complexitatea acestor tehnici de monitorizare, oferirea de informații prealabile semnificative este una dintre principalele provocări în obținerea unui consimțământ valid. Consumatorii ar trebui să fie informați într-un mod în care să înțeleagă ce informații sunt prelucrate, modul în care acestea sunt utilizate și impactul asupra experienței în calitate de utilizator și a nivelului de intruziune în viața privată în legătură cu tehnicile.

60. Aceasta înseamnă nu doar că informațiile în sine trebuie să fie clare și inteligibile pentru utilizatorii medii, ci și că informațiile sunt oferite în mod direct persoanelor, într-un mod vizibil, astfel încât acestea să nu le treacă cu vederea.

61. *Manifestarea voinței*. Consimțământul conform cadrului juridic aplicabil necesită, de asemenea, o acțiune afirmativă din partea utilizatorului de a-și exprima acordul. Consimțământul implicit nu îndeplinește acest standard. Acesta confirmă, de asemenea, necesitatea de a se utiliza mijloace speciale de obținere a consimțământului care să permită furnizorului de servicii de internet să inspecteze datele privind comunicațiile și traficul în contextul aplicării politicilor de gestionare a traficului. În avizul său recent privind consimțământul, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal a subliniat nevoia abordării specifice în legătură cu obținerea consimțământului în legătură cu diversele elemente care constituie prelucrarea datelor.

([31]) Un acord similar îl constituie registrul cu numele pasagerilor (PNR), în contextul căruia s-a discutat dacă este valid consimțământul pasagerilor de a transfera detalii privind rezervarea autorităților americane. Grupul de lucru a considerat că consimțământul pasagerilor nu poate fi acordat liber, întrucât companiile aeriene sunt obligate să trimită datele înainte de plecarea zborului, iar pasagerii nu au, prin urmare, o opțiune reală dacă doresc să zboare; Avizul nr. 6/2002 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal privind transmiterea informațiilor din listele de pasageri și a altor date de la companiile aeriene către SUA.

([32]) Directiva 2009/136/CE din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice (a se vedea nota de subsol 15).

62. Se poate susține că, în cazul în care părțile implicate într-o comunicație nu doresc interceptarea acesteia de către furnizorii de servicii de internet în vederea aplicării politicilor de gestionare a traficului, acestea pot oricând cripta comunicația. Această abordare poate fi considerată utilă în termeni practici, însă necesită un anumit efort și cunoștințe tehnice și nu poate fi considerată a fi similară unui consimțământ liber, specific și informat. De asemenea, utilizarea tehnicilor de criptare nu păstrează confidențialitatea deplină a comunicației, întrucât furnizorul de servicii de internet va putea, cel puțin, să acceseze informațiile referitoare la antetul IP pentru a ruta comunicația și va fi, de asemenea, în măsură să aplice o analiză statistică.

63. În conformitate cu articolul 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic, trebuie obținut consimțământul de la utilizatorii în cauză. În multe cazuri, utilizatorul va fi aceeași persoană cu abonatul, care își exprimă consimțământul în momentul abonării la serviciul de telecomunicație. În alte cazuri, inclusiv cele în care sunt implicate mai mult de o persoană, consimțământul utilizatorilor vizați trebuie să fie obținut separat. Aceasta poate ridica probleme practice, astfel cum se explică în cele ce urmează.

Consimțământul tuturor persoanelor vizate

64. Articolul 5 alineatul (1) prevede consimțământul utilizatorului pentru a legitima prelucrarea. Consimțământul trebuie obținut de la *toți utilizatorii* implicați într-o comunicație. Raționamentul care stă la baza acestei condiții este acela că o comunicație implică, în general, cel puțin două persoane (expeditorul și destinatarul). De exemplu, dacă un furnizor de servicii de internet scanează încărcături utile IP care se referă la un e-mail, acestea inspectează informații asociate atât expeditorului, cât și destinatarului e-mailului.

65. În timpul monitorizării și al interceptării traficului și comunicațiilor (de exemplu, trafic web), poate fi suficient pentru furnizorii de servicii de internet să obțină consimțământul utilizatorului, și anume, al abonatului. Aceasta se datorează faptului că cealaltă parte din cadrul comunicației, în acest caz, un site vizitat, nu poate fi considerată drept „utilizator vizat" ([33]). Totuși, situația poate fi mai complexă, atunci când monitorizarea implică inspectarea conținutului e-mailurilor și, prin urmare, a informațiilor cu caracter personal ale expeditorului și destinatarului e-mailului, care pot să nu aibă o relație contractuală cu același furnizor de servicii de internet. Într-adevăr, în aceste cazuri, furnizorul de servicii de internet ar prelucra date cu caracter personal (numele, adresa de e-mail și date posibil confidențiale) ale unor persoane care nu sunt clienții furnizorului respectiv. Dintr-o perspectivă practică, obținerea consimțământului de la aceste persoane poate fi mai dificilă, întrucât ar trebui să fie realizată în fiecare caz, nu doar odată cu finalizarea serviciului de telecomunicație. De asemenea, nu ar fi realist să se presupună că consimțământul abonatului a fost exprimat și în numele altor utilizatori, cum poate fi de multe ori cazul în gospodăriile particulare.

66. În acest context, AEPD consideră că furnizorii de servicii de internet sunt obligați să respecte cerințele juridice existente și să pună în aplicare politici care nu implică monitorizarea și inspectarea informațiilor. Aceasta se impune cu atât mai mult în ceea ce privește serviciile de comunicații, care implică părți terțe care nu își pot exprima consimțământul pentru monitorizare, în special cu privire la e-mailurile trimise și primite (cerința nu se aplică în cazul în care scopul se bazează pe considerente de securitate).

67. În același timp, ar trebui remarcat că legislația națională care pune în aplicare articolul 5 alineatul (1) din Directiva privind confidențialitatea în mediul electronic poate să nu fie întotdeauna satisfăcătoare din acest punct de vedere, și că, în general, pare să fie necesară îmbunătățirea orientărilor în ceea ce privește cerințele prevăzute în Directiva privind confidențialitatea în mediul electronic, în acest context. Prin urmare, AEPD invită Comisia să fie mai activă în această privință și să ia o inițiativă care ar putea beneficia de contribuții din partea autorităților de supraveghere reunite în cadrul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și de la alte părți interesate. Dacă este necesar, ar trebui să se înainteze o cauză Curții de Justiție în vederea clarificării pe deplin a semnificației și consecințelor articolului 5 alineatul (1).

([33]) Cu excepția cazurilor în care traficul implică transferul de informații cu caracter personal cum ar fi, de exemplu, imagini cu persoane fizice identificabile afișate pe un site. Prelucrarea acestor informații necesită un temei juridic, însă nu este reglementată de articolul 5 alineatul (1), întrucât aceste persoane nu sunt „utilizatori vizați".

V.3. **Proporționalitatea – principiul minimizării datelor**

68. Articolul 6 litera (c) din Directiva privind protecția datelor prevede principiul proporționalității ([34]), care se aplică furnizorilor de servicii de internet, întrucât aceștia sunt responsabili pentru prelucrarea datelor în sensul prezentei directive, atunci când efectuează monitorizarea și filtrarea.

69. În temeiul acestui principiu, datele cu caracter personal pot fi prelucrate doar în măsura în care sunt „adecvate, pertinente și neexcesive în ceea ce privește scopurile pentru care sunt colectate și prelucrate ulterior". Aplicarea acestui principiu atrage necesitatea efectuării unei evaluări pentru a aprecia dacă metoda utilizată pentru prelucrarea datelor și dacă tipurile de date cu caracter personal utilizate sunt adecvate și este destul de probabil ca acestea să își atingă obiectivele. Dacă se concluzionează că sunt colectate mai multe date decât este necesar, principiul nu este respectat.

70. Respectarea principiul proporționalității de către anumite tipuri de tehnici de inspecție trebuie evaluată de la caz la caz. Nu este posibil să se ajungă la concluzii *in abstracto*. Totuși, este posibil să se atragă atenția asupra unor diverse aspecte concrete care trebuie evaluate în cazul evaluării respectării principiului proporționalității.

71. *Volumul de informații prelucrate.* Supravegherea comunicațiilor clienților furnizorilor de internet la cele mai profunde niveluri posibile va fi, în majoritatea cazurilor, excesivă și ilegală. Faptul că supravegherea se poate efectua prin mijloace care nu sunt vizibile persoanelor și că acestea pot înțelege cu dificultate ce se întâmplă sporește impactul asupra vieții private. Furnizorii de servicii de internet trebuie să evalueze ce mijloace mai puțin intruzive pot fi disponibile pentru a obține rezultatul dorit. De exemplu, se pot obține rezultatele dorite prin monitorizarea antetelor IP, în locul efectuării unei inspecții aprofundate a pachetelor? Chiar și atunci când este utilizată inspecția aprofundată a pachetelor, identificarea doar a anumitor protocoale poate furniza informațiile necesare. Aplicarea unor garanții de protecție a datelor, inclusiv pseudoanonimizarea, poate fi, de asemenea, relevantă. Rezultatul evaluării trebuie să confirme că prelucrarea datelor este proporțională.

72. *Efectele prelucrării (asociate în mod direct scopurilor).* Proporționalitatea poate fi absentă în cazurile în care furnizorii de servicii de internet utilizează politici de gestionare a traficului care exclud accesul la anumite servicii fără a oferi utilizatorilor un beneficiu echitabil, în schimb.

73. Este important să se reamintească faptul că principiul proporționalității continuă să se aplice chiar dacă au fost satisfăcute alte cerințe juridice obligatorii, inclusiv dacă un furnizor de servicii de internet a obținut, de exemplu, consimțământul din partea persoanelor pentru a efectua monitorizarea conținutului. Aceasta înseamnă că prelucrarea datelor efectuată prin monitorizarea conținutului poate fi totuși considerată ilegală dacă încalcă principiul fundamental subiacent al proporționalității.

V.4. **Măsuri de securitate și organizare**

74. Articolul 4 din Directiva privind confidențialitatea în mediul electronic prevede în mod explicit ca furnizorii de servicii de internet să adopte măsuri tehnice și de organizare, pentru a asigura: (i) accesarea datelor cu caracter personal doar de personal autorizat și în scopuri legale; (ii) protecția datelor cu caracter personal împotriva prelucrării accidentale sau ilegale; și (iii) punerea în aplicare a unei politici de securitate în ceea ce privește prelucrarea datelor cu caracter personal. De asemenea, conform acestui articol, autoritățile naționale competente sunt autorizate să efectueze audituri cu privire la aceste măsuri.

75. De asemenea, în temeiul articolului 4 alineatele (3) și (2) din Directiva privind confidențialitatea în mediul electronic, furnizorii de servicii de internet sunt, de asemenea, obligați să notifice autoritățile naționale competente în cazul unei încălcări a securității datelor, precum și persoanele afectate, în cazul în care divulgarea ar putea avea efecte negative asupra acestora.

76. Prelucrarea informațiilor cu caracter personal incluse în comunicații în scopul aplicării politicilor de gestionare a traficului pot oferi furnizorilor de servicii de internet accesul la date care sunt mai confidențiale decât datele de trafic.

([34]) Așa cum s-a specificat anterior, Directiva privind protecția datelor se aplică tuturor chestiunilor care vizează protecția libertăților și a drepturilor fundamentale, care nu sunt reglementate în mod specific de Directiva privind confidențialitatea în mediul electronic.

77. Prin urmare, politicile de securitate elaborate de furnizorii de servicii de internet incorporează garanții specifice, pentru a asigura că măsurile adoptate sunt adecvate acestor riscuri. În același timp, autoritățile naționale competente care auditează aceste măsuri trebuie să fie deosebit de exigente. În sfârșit, trebuie să se garanteze că sunt instituite măsuri eficiente de notificare a persoanelor vizate ale căror informații au fost compromise și care ar putea astfel să fie afectate.

VI. **SUGESTII DE MĂSURI POLITICE ȘI LEGISLATIVE**

78. Inspecțiile tehnice bazate pe datele de trafic și inspecția încărcăturilor utile IP, și anume conținutul informațiilor, pot indica activitatea utilizatorilor pe internet: site-urile vizitate și activitățile de pe aceste site-uri, utilizarea aplicațiilor P2P, fișierele descărcate, e-mailurile trimise și primite, de la cine, pe ce temă și în ce termeni etc. Furnizorii de servicii de internet ar putea utiliza aceste informații pentru a acorda prioritate anumitor comunicații, precum materialele video la cerere. Aceștia ar putea utiliza informațiile pentru a identifica viruși sau pentru a crea profiluri în beneficiul publicității comportamentale. Aceste acțiuni intră în conflict cu dreptul la confidențialitatea comunicațiilor.

79. În funcție de tehnicile utilizate și de particularitățile cazului, implicațiile privind confidențialitatea vor spori. Cu cât interceptarea și analiza informațiilor colectate ating un nivel mai aprofundat, cu atât mai mare este conflictul cu principiul confidențialității comunicațiilor. Scopul în care are loc monitorizarea și garanțiile aplicate pentru protecția datelor sunt, de asemenea, elemente esențiale pentru stabilirea gradului de intruziune în viața privată și datele cu caracter personale ale utilizatorilor. Blocarea și monitorizarea în scopul combaterii programelor informatice rău-intenționate (malware), cu limitări stricte asupra păstrării și utilizării datelor inspectate, nu pot fi comparate cu situații în care informațiile sunt înregistrate într-un jurnal pentru a construi profiluri individuale care să servească publicității comportamentale.

80. În principiu, AEPD consideră că actualul cadru juridic european privind confidențialitatea și protecția datelor, dacă este interpretat, aplicat și executat corect, ar fi potrivit pentru a garanta că dreptul la confidențialitate este confirmat și, în general, că protejarea confidențialității și a datelor persoanelor nu este compromisă ([35]). Furnizorii de servicii de internet nu trebuie să utilizeze astfel de mecanisme, decât dacă au aplicat în mod corect cadrul juridic. În special, printre elementele relevante ale cadrului pe care furnizorii de servicii de internet ar trebui să le ia în considerare și să le respecte, se numără:

— furnizorii de internet pot aplica politici de gestionare a traficului, urmărind securitatea serviciului în timpul furnizării acestuia, inclusiv limitarea congestiei, în temeiul articolelor 4 și 6 din Directiva privind confidențialitatea în mediul electronic;

— furnizorii de servicii de internet au nevoie de un alt temei juridic specific, și, eventual, de consimțământul utilizatorilor, pentru a aplica politici de gestionare a traficului care implică prelucrarea datelor privind traficul și/sau comunicațiile în alte scopuri decât cele expuse mai sus. De exemplu, este necesar consimțământul informat al utilizatorilor pentru a monitoriza și filtra comunicațiile persoanelor în scopul limitării (sau acordării) accesului la anume aplicații și servicii, precum P2P sau VoIP;

— consimțământul trebuie să fie liber, explicit și informat. Acesta trebuie să se manifeste printr-o acțiune afirmativă. Aceste cerințe pun un accent deosebit pe nevoia de intensificare a eforturilor, pentru a se asigura că persoanele sunt informate corect, în mod direct, inteligibil și specific, astfel încât să poată evalua efectele practicilor și, în ultimă instanță, să ia o decizie informată. Având în vedere complexitatea acestor tehnici, oferirea de informații prealabile semnificative utilizatorilor este una dintre principalele provocări în obținerea unui consimțământ valid. În plus, utilizatori care nu își exprimă consimțământul cu privire la monitorizare nu ar trebui să suporte consecințe nefavorabile (inclusiv costuri financiare);

([35]) Aceasta nu aduce atingere necesității modificărilor legislative pe baza altor considerații, în special în contextul revizuirii generale a cadrului juridic al UE privind protecția datelor, în vederea eficientizării acesteia în contextul noilor tehnologii și globalizării.

— principiul proporționalității are un rol crucial atunci când furnizorii de servicii de internet se angajează în politici de gestionare a traficului, indiferent de fundamentul juridic al prelucrării și de scop: furnizarea serviciului, evitarea congestiei sau furnizarea de abonamente specifice cu sau fără acces la anumite servicii și aplicații. Acest principiu limitează capacitatea furnizorilor de servicii de internet de a monitoriza conținutul comunicațiilor unei persoane, într-un mod care implică prelucrarea excesivă a informațiilor sau creșterea beneficiilor doar pentru furnizorii de servicii de internet. Ceea ce furnizorii de servicii de internet pot realiza din punct de vedere logistic depinde de nivelul de intruziune al tehnicilor, de rezultatele necesare (pentru care aceștia își pot crește beneficiile) și de garanțiile specifice de confidențialitate și protecția datelor aplicate. Înainte de utilizarea tehnicilor de inspecție, furnizorii de servicii de internet trebuie să efectueze o evaluare a conformității acestora cu principiul proporționalității.

81. Deși cadrul juridic actual include condiții și garanții relevante, este necesar să se acorde o atenție deosebită întrebării dacă furnizorii de servicii de internet îndeplinesc efectiv cerințele juridice, dacă furnizează consumatorilor informațiile necesare pentru ca aceștia să își exprime opțiunea în cunoștință de cauză și dacă respectă principiul proporționalității. La nivel național, autoritățile competente pentru cele de mai sus includ autoritățile naționale responsabile cu telecomunicațiile, pe de o parte, și autoritățile naționale responsabile cu protecția datelor, pe de altă parte. La nivelul UE, printre organismele relevante se numără OAREC (Organismul autorităților europene de reglementare în domeniul comunicațiilor electronice). AEPD ar putea, de asemenea, avea un rol în acest context.

82. Pe lângă monitorizarea nivelului actual de conformitate, având în vedere relativa noutate a posibilității de a realiza o inspecție masivă, în timp real, a comunicațiilor, unele aspecte legate de aplicarea cadrului care au fost discutate în prezentul aviz necesită o analiză suplimentară mai detaliată și clarificare ulterioară. Printre orientările relevante în special în anumite domenii se numără:

— stabilirea acelor practici de inspecție care sunt legitime pentru a asigura fluxul normal de trafic, care ar putea să nu necesite consimțământul utilizatorilor, cum ar fi, de exemplu, combaterea spam-ului. Pe lângă caracterul intruziv al monitorizării aplicate, sunt relevante aspecte precum, de exemplu, nivelul de perturbare a fluxului normal al traficului care ar putea apărea în caz contrar;

— stabilirea acelor tehnici de inspecție care pot fi utilizate în scopul securității, care ar putea să nu necesite consimțământul utilizatorilor;.

— stabilirea cazurilor în care monitorizarea necesită consimțământul persoanei, în special consimțământul tuturor utilizatorilor vizați, și a parametrilor tehnici admisibili pentru a se asigura că tehnica de inspecție nu determină o prelucrare a datelor care nu este proporțională față de obiectivele sale propuse;

— pe lângă cele trei cazuri de mai sus, pot fi necesare orientările privind aplicarea garanțiilor necesare de protecție a datelor (limitarea scopului, securitatea etc.).

83. Având în vedere că în acest domeniu competențele sunt atât naționale, cât și la nivelul UE, AEPD consideră că este esențială partajarea punctelor de vedere și experiențelor în vederea unor abordări armonizate la cele de mai sus. În acest sens, AEPD propune crearea unei platforme sau a unui grup de experți care să reunească reprezentanți ai autorităților naționale de reglementare, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, AEPD și OAREC. Primul obiectiv al acestei platforme ar consta în elaborarea de orientări, cel puțin cu privire la elementele identificate anterior, în vederea asigurării unor abordări solide și armonizate și a unor condiții de egalitate. AEPD solicită Comisiei să organizeze această inițiativă.

84. Nu în ultimul rând, atât autoritățile naționale, cât și autoritățile omoloage la nivelul UE, inclusiv OAREC și Comisia Europeană trebuie să acorde o atenție deosebită evoluțiilor pieței din acest domeniu. Din perspectiva confidențialității și a protecției datelor, scenariul în care furnizorii de servicii de internet instituie ca procedură de rutină politici de gestionare a traficului, oferind abonamente pe baza filtrării accesului la conținut și aplicații, este extrem de problematic. În cazul în care această situație ar deveni realitate, ar trebui să se elaboreze acte legislative în acest sens.

VII. **CONCLUZII**

85. Faptul că furnizorii de servicii de internet recurg din ce în ce mai des la tehnici de inspecție și monitorizare afectează neutralitatea internetului și confidențialitatea comunicațiilor. Acest fapt ridică probleme grave legate de protecția vieții private și a datelor cu caracter personal ale utilizatorilor.

86. Deși comunicarea Comisiei privind internetul deschis și neutralitatea rețelei în Europa abordează pe scurt aceste probleme, AEPD consideră că ar trebui depuse mai multe eforturi, pentru a se ajunge la o politică satisfăcătoare privind calea de urmat. Prin prezentul aviz, AEPD a contribuit la continuarea dezbaterii politicilor privind neutralitatea rețelei, în special cu privire la aspecte legate de confidențialitate și protecția datelor.

87. AEPD consideră că este necesar ca autoritățile naționale și OAREC să monitorizeze situația pieței. Această monitorizare ar trebui să conducă la o imagine clară care să descrie dacă piața evoluează spre inspecția masivă, în timp real, a comunicațiilor și aspectele legate de respectarea cadrului juridic.

88. Monitorizarea pieței ar trebui să fie însoțită de o analiză suplimentară a efectelor noilor practici în raport cu protecția datelor și confidențialitatea pe internet. Prezentul aviz subliniază o serie de domenii în care clarificarea ar fi benefică. Deși agențiile și organismele UE precum OAREC, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și AEPD ar putea fi în măsură să clarifice condițiile de aplicare a cadrului, AEPD consideră că Comisia are obligația de a coordona și direcționa dezbaterea. Prin urmare, aceasta solicită Comisiei să ia o inițiativă care să implice toate părțile interesate în cadrul unei platforme sau unui grup de lucru, în acest scop. Printre aspectele care necesită analiză suplimentară, ar trebui abordate următoarele puncte:

— stabilirea acelor practici de inspecție care sunt legitime pentru a asigura fluxul normal de trafic și care pot fi efectuate în scopuri de securitate;

— stabilirea cazurilor în care monitorizarea necesită consimțământul persoanei, în special consimțământul tuturor utilizatorilor vizați, și a parametrilor tehnici admisibili pentru a asigura că tehnica de inspecție nu determină o prelucrare a datelor care nu este proporțională cu obiectivele sale propuse;

— în cazurile de mai sus, pot fi necesare orientări privind aplicarea garanțiilor necesare de protecție a datelor (limitarea la un scop specific, securitate etc.).

89. În funcție de aceste concluzii, pot fi necesare măsuri legislative suplimentare. Într-un astfel de caz, Comisia trebuie să prezinte măsuri strategice menite să consolideze cadrul juridic și să asigure certitudinea juridică. Noi măsuri ar trebui să clarifice efectele practice ale principiului neutralității rețelei, întrucât acest lucru a fost deja realizat în unele state membre, și să asigure că utilizatorii pot exercita o alegere reală, în special prin obligarea furnizorilor de servicii de internet să ofere conexiuni nemonitorizate.

Adoptat la Bruxelles, 7 octombrie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor