I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind negocierile curente purtate de Uniunea Europeană pentru un Acord comercial de combatere a contrafacerii (ACTA)

(2010/C 147/01)

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 articolul 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 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 [2],

având în vedere Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [3], în special articolul 41,

ADOPTĂ URMĂTORUL AVIZ:

I. **INTRODUCERE**

1. Uniunea Europeană ia parte la negocieri privind elaborarea unui Acord comercial de combatere a contrafacerii (ACTA). Aceste negocieri au fost lansate în anul 2007 în rândul unui grup inițial de părți interesate și au continuat cu un grup mai amplu de participanți; în prezent acești participanți includ Australia, Canada, Uniunea Europeană, Japonia, Coreea, Mexic, Maroc, Noua Zeelandă, Singapore, Elveția și Statele Unite. Comisia Europeană a primit un mandat de la Consiliu pentru a începe aceste negocieri în 2008.

2. AEPD recunoaște că schimburile comerciale cu bunuri contrafăcute sau piratate reprezintă un motiv de îngrijorare din ce în ce mai mare care deseori implică rețele criminale organizate, ceea ce impune adoptarea unor mecanisme adecvate de cooperare la nivel internațional pentru combaterea acestei forme de criminalitate.

3. AEPD subliniază că negocierile purtate de Uniunea Europeană pentru un acord multilateral care are drept obiect principal protejarea drepturilor de proprietate intelectuală ridică probleme importante în ceea ce privește impactul măsurilor luate pentru combaterea contrafacerii și a pirateriei asupra drepturilor fundamentale ale persoanelor fizice, în special asupra dreptului acestora la protecția vieții private și a datelor cu caracter personal.

4. În acest sens, AEPD regretă îndeosebi că nu a fost consultată de către Comisia Europeană cu privire la conținutul acestui acord. Acționând din proprie inițiativă, AEPD a adoptat, în consecință, prezentul aviz în temeiul articolului 41 alineatul (2) din Regulamentul (CE) nr. 45/2001 în vederea oferirii de orientări Comisiei privind aspectele referitoare la protecția vieții private și a datelor cu caracter personal care trebuie luate în considerare în negocierile pentru ACTA.

II. **SITUAȚIA ACTUALĂ ȘI CONȚINUTUL PREVĂZUT AL ACTA**

5. Cea de a șaptea rundă de negocieri a avut loc în Mexic între 26 și 29 ianuarie 2010 în vederea încheierii unui acord în decursul anului 2010. Cu toate acestea, până în prezent nu a fost publicat niciun proiect de acord.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 201, 31.7.2002, p. 37.
[3] JO L 8, 12.1.2001, p. 1.

6. Negocierile vizează adoptarea unui acord multilateral menit să consolideze respectarea drepturilor de proprietate intelectuală (DPI) și să combată contrafacerea și pirateria. Dacă se adoptă, acest nou acord va crea standarde internaționale îmbunătățite privind modul de acțiune împotriva încălcărilor DPI pe scară largă. Direcția Generală Comerț a Comisiei Europene a subliniat în special faptul că „obiectivul concret îl reprezintă activitățile de contrafacere și piraterie care afectează în mod semnificativ interesele comerciale, mai degrabă decât activitățile cetățenilor obișnuiți" ([4]).

7. În ceea ce privește conținutul acordului, *Rezumatul elementelor cheie în discuție* publicat de Direcția Generală Comerț a Comisiei Europene în noiembrie 2009 arată că obiectivul ACTA de combatere a pirateriei și contrafacerii va fi urmărit prin intermediul a trei componente principale: (i) cooperarea internațională; (ii) practicile de punere în aplicare și (iii) definirea unui cadru legal pentru punerea în aplicare a DPI în mai multe domenii identificate, în special în mediul digital ([5]). Măsurile preconizate vor viza în special proceduri legale (precum interdicțiile, măsurile temporare), rolul și responsabilitățile furnizorilor de servicii internet (FSI) în ceea ce privește împiedicarea încălcării drepturilor de autor pe internet și măsuri de cooperare transfrontalieră pentru împiedicarea circulației transfrontaliere a bunurilor obținute. Cu toate acestea, informațiile făcute publice prezintă numai liniile generale ale acordului și nu intră în detalii cu privire la nicio măsură specifică și concretă.

8. AEPD observă că în cazul în care obiectivul intenționat al ACTA este de a urmări doar încălcările pe scară largă ale DPI, nu se poate exclude posibilitatea de a include în ACTA activitățile cetățenilor obișnuiți, în special având în vedere că măsurile de protecție se aplică în mediul digital. AEPD subliniază că aceasta va necesita stabilirea de garanții adecvate pentru protejarea drepturilor fundamentale ale persoanelor fizice. De asemenea, legile privind protecția datelor vizează persoanele fizice, inclusiv cele potențial implicate în activități de contrafacere și piraterie; combaterea încălcărilor pe scară largă vor include în mod cert și prelucrarea datelor cu caracter personal.

9. În acest sens, AEPD încurajează ferm Comisia Europeană să stabilească un dialog public și transparent privind ACTA, eventual prin intermediul unei consultări publice care, de asemenea, ar contribui la asigurarea faptului că măsurile ce urmează să fie adoptate sunt conforme cu cerințele dreptului UE privind protecția vieții private și a datelor cu caracter personal.

III. SFERA OBSERVAȚIILOR AEPD

10. AEPD adresează un apel Uniunii Europene, în special Comisiei Europene care a primit mandatul pentru încheierea acordului, să realizeze un echilibru corect între cererile de protecție a drepturilor de proprietate intelectuală și drepturile de protecție a vieții private și a datelor cu caracter personal ale persoanelor fizice.

11. AEPD subliniază că protecția vieții private și a datelor sunt valori principale ale Uniunii Europene, recunoscute în articolul 8 al CEDO și articolele 7 și 8 ale Cartei drepturilor fundamentale a UE ([6]), care trebuie să fie respectate în cadrul tuturor politicilor și normelor adoptate de UE în conformitate cu articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE).

12. De asemenea, AEPD subliniază că orice acord la care ajunge Uniunea Europeană cu privire la ACTA trebuie să respecte obligațiile legale impuse UE în legătură cu legislația privind protecția vieții private și a datelor, astfel cum s-a stabilit în special în Directiva 95/46/CE, în Directiva 2002/58/CE ([7]) și în jurisprudența Curții Europene a Drepturilor Omului ([8]) și a Curții de Justiție ([9]).

13. Protecția vieții private și a datelor trebuie să fie luată în considerare încă de la începutul negocierilor, nu atunci când măsurile și procedurile sunt deja definite și convenite și, în consecință, este prea târziu pentru a găsi soluții alternative care să respecte viața privată.

14. Având în vedere că puține informații sunt făcute publice, AEPD observă că nu se află în poziția în care să furnizeze o analiză a prevederilor specifice ale ACTA. Prin urmare, în prezentul aviz, AEPD se va concentra pe prezentarea potențialelor amenințări împotriva protecției vieții private și a datelor reprezentate de posibilele măsuri concrete pe care acordul, astfel cum s-a raportat, le-ar putea genera în următoarele două domenii: protejarea drepturilor de proprietate intelectuală în mediul digital (capitolul IV) și mecanismele de cooperare internațională (capitolul V).

([4]) A se vedea http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, p. 2.

([5]) A se vedea nota de subsol nr. 2 de mai sus.

([6]) Carta drepturilor fundamentale a Uniunii Europene, JO C 303, 14.12.2007, p. 1.

([7]) 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 (Directiva privind confidențialitatea și comunicațiile electronice) JO L 201, 31.7.2002, p. 37.

([8]) Interpretarea principalelor elemente și condiții stabilite în articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (CEDO) adoptată la Roma la 4 noiembrie 1950, astfel cum se aplică diferitelor domenii. A se vedea, în special, jurisprudența la care se face referire în alte părți ale prezentului aviz.

([9]) A se vedea, în special: Cauza C-275/06, *Productores de Música de España* (Promusicae), Clg. 2008, p. I-271 și Cauza C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nepublicată încă.

IV. PROTEJAREA DREPTURILOR DE PROPRIETATE INTELECTUALĂ ÎN MEDIUL DIGITAL

IV.1. Necesitatea de a analiza implicațiile „politicilor de deconectare de la internet după trei abateri consecutive" asupra protecției vieții private/datelor

15. Potrivit Comisiei Europene, ACTA va crea un cadru legal pentru a lupta împotriva pirateriei în mediul digital ([10]). Acest cadru va stabili condițiile în baza cărora FSI și alți intermediari online ([11]) pot fi considerați răspunzători ca urmare a încălcării drepturilor de autor ale materialelor distribuite prin intermediul echipamentelor lor. De asemenea, cadrul poate stipula măsuri sau soluții impuse utilizatorilor de internet ca urmare a încărcării sau descărcării de materiale încălcând drepturile de autor. Deși detaliile acestui cadru nu au fost comunicate în mod oficial, având în vedere informațiile disponibile pe diferite canale, se poate prevedea că acesta ar putea include impunerea unor obligații asupra FSI de a adopta „politici de deconectare de la internet după trei abateri consecutive" denumite și măsuri de „răspuns treptat". Aceste măsuri vor permite proprietarilor drepturilor de autor să monitorizeze utilizatorii de internet și să identifice presupușii contravenienți. După ce este contactat FSI al presupusului contravenient, FSI va avertiza utilizatorul identificat drept contravenient, acesta din urmă fiind deconectat de la internet după ce primește trei avertismente.

16. Concomitent cu negocierile privind ACTA, politicile privind deconectarea de la internet după trei abateri consecutive sunt puse în aplicare în anumite state membre, precum Franța. De asemenea, acestea sunt dezbătute în mai multe forumuri ale UE precum Dialogul părților interesate privind încărcarea și descărcarea ilegală care se desfășoară în prezent fiind moderat de DG MARKT, în legătură cu adoptarea Comunicării Comisiei privind îmbunătățirea protejării drepturilor de proprietate intelectuală pe piața internă ([12]). Discuții privind acest subiect au loc și în Parlamentul European în contextul unei dezbateri prevăzute privind proiectul de Rezoluție a Parlamentului European cu privire la îmbunătățirea protejării drepturilor de proprietate intelectuală pe piața internă (denumită „Raportul Gallo").

17. Aceste practici sunt foarte invazive în ceea ce privește viața privată a persoanelor fizice. Acestea implică monitorizarea generalizată a activităților utilizatorilor de internet, inclusiv a celor care respectă pe deplin legea. Acestea afectează milioane de utilizatori de internet care respectă legea, inclusiv mulți copii și adolescenți. Acestea sunt puse în aplicare de părți private și nu de autorități de aplicare a legii. În plus, în prezent, internetul joacă un rol esențial în aproape toate aspectele vieții moderne și, astfel, efectele deconectării de la internet pot fi imense, prin blocarea accesului persoanelor fizice la muncă, cultură, aplicații de guvernare electronică (e-guvern) etc.

18. În acest context, este relevant să se evalueze măsura în care aceste politici sunt conforme cu dreptul UE privind protecția datelor și a vieții private și, în special, dacă politicile privind deconectarea de la internet după trei abateri consecutive constituie o măsură necesară pentru protejarea drepturilor de proprietate intelectuală. Din această perspectivă, ar trebui să se analizeze în continuare dacă există alte metode mai puțin invazive.

19. Încă nu este clar dacă politicile privind deconectarea de la internet după trei abateri consecutive vor face parte din ACTA. Totuși, aceste politici sunt luate în considerare chiar și în alte domenii și au un – potențial – impact enorm asupra protecției datelor cu caracter personal și a vieții private. Din aceste motive, AEPD consideră că este necesar să le dezbată în cadrul prezentului aviz. Înainte de a efectua analiza menționată, AEPD va descrie pe scurt cadrul legal aplicabil privind protecția datelor și a vieții private.

20. Trebuie observat că, în plus față de protecția datelor și a vieții private, politicile privind deconectarea de la internet după trei abateri consecutive ridică probleme cu privire la alte valori precum dreptul la justiție și libertatea de exprimare. Cu toate acestea, prezentul aviz va aborda numai acele aspecte care sunt legate de protecția datelor cu caracter personal și a vieții private a persoanelor fizice.

IV.2. Politicile privind deconectarea de la internet după trei abateri consecutive și aplicarea cadrului legal al UE privind protecția datelor și a vieții private

Cum pot fi stabilite politicile privind deconectarea de la internet după trei abateri consecutive

21. Pe scurt, conform politicilor privind deconectarea de la internet după trei abateri consecutive, titularii de drepturi de autor care folosesc mijloace tehnice automatizate, eventual furnizate de terți, ar identifica presupusa încălcare a drepturilor de autor prin monitorizarea activităților utilizatorilor de internet, de exemplu, prin supravegherea forumurilor, blogurilor sau asumându-și calitatea de

([10]) A se vedea nota de subsol nr. 2 de mai sus.

([11]) Diferiții intermediari online pot fi definiți în funcție de rolurile funcționale ale acestora. Cu toate acestea, în realitate intermediarii au de obicei mai multe dintre aceste funcții. Intermediarii online includ: (a) *furnizorii de acces*: utilizatorii se conectează la rețea prin conectarea la un server al furnizorului de acces; (b) *furnizorii de rețea*: aceștia furnizează rutere, *mai exact* instalațiile tehnice necesare pentru transmisia de date; (c) *furnizori de găzduire web*: aceștia închiriază spațiu pe serverul lor, pe care utilizatorii sau furnizorii de conținut pot încărca conținut. Utilizatorii pot încărca și descărca conținut de la un serviciu online, precum rețelele de buletine informative sau P2P.

([12]) Comunicarea Comisiei către Consiliu, Parlamentul European și Comitetul Economic și Social European – O mai bună protejare a drepturilor de proprietate intelectuală pe piața internă, Bruxelles, 11 septembrie 2009, COM(2009) 467 final.

persoane care partajează fișiere în rețele peer to peer pentru a-i identifica persoanele despre care se presupune că partajează fișiere protejate de drepturi de autor ([13]).

22. După identificarea utilizatorilor de internet despre care se presupune că sunt implicați în încălcarea drepturilor de autor prin colectarea adreselor de protocol internet (adrese IP) ale acestora, titularii drepturilor de autor ar trimite adresele IP ale acelor utilizatori respectivilor furnizori de servicii de internet care ar avertiza abonații cărora le aparțin adresele IP cu privire la posibila implicare a acestora în încălcarea drepturilor de autor. Primirea unui număr de avertismente din partea FSI ar rezulta automat în încetarea sau suspendarea conexiunii la internet a abonatului de către FSI ([14]).

Cadrul legal aplicabil al UE privind protecția datelor/vieții private

23. Politicile privind deconectarea de la internet după trei abateri consecutive trebuie să fie conforme cu cerințele care rezultă din dreptul la viața privată, astfel cum se stipulează în articolul 8 al CEDO și articolul 7 din Carta drepturilor fundamentale, și din dreptul la protecția datelor, astfel cum este stipulat în articolul 8 din Carta drepturilor fundamentale și articolul 16 din TFUE, și astfel cum s-a detaliat în Directiva 95/46/CE și Directiva 2002/58/CE.

24. În opinia AEPD, monitorizarea comportamentului utilizatorilor de internet și colectarea ulterioară a adreselor IP ale acestora reprezintă o ingerință cu privire la drepturile acestora de a le fi respectată viața privată și corespondența; cu alte cuvinte, este afectat dreptul la viața privată. Această opinie este în conformitate cu jurisprudența Curții Europene a Drepturilor Omului ([15]).

25. Directiva 95/46/CE este aplicabilă ([16]) deoarece politicile privind deconectarea de la internet după trei abateri consecutive implică prelucrarea adreselor IP care – în orice caz în circumstanțele relevante – trebuie să fie considerate date cu caracter personal. Adresele IP sunt elemente de identificare reprezentate printr-un un șir de numere separate prin puncte, precum 122.41.123.45. Abonarea la un furnizor de acces la internet va oferi abonatului acces la internet. De fiecare dată când abonatul dorește să intre pe internet, acestuia i se va atribui o adresă IP prin dispozitivul pe care îl folosește pentru a avea acces la internet (un calculator, de exemplu) ([17]).

26. Dacă un utilizator începe o anumită activitate, de exemplu, încărcă materiale pe internet, utilizatorul poate fi identificat de terți prin adresa IP pe care acesta o folosește. De exemplu, utilizatorul care deține adresa IP 122.41.123.45 a încărcat materiale despre care se presupune că încalcă drepturile de autor pe un serviciu P2P la 1 ianuarie 2010, ora 15:00. FSI va putea atunci să asocieze această adresă IP cu numele abonatului căruia i-a fost atribuită adresa și astfel poate să îi verifice identitatea.

27. Dacă se ia în considerare definiția datelor cu caracter personal prevăzută în articolul 2 din Directiva 95/46/CE, „orice informații referitoare la o persoană fizică identificată sau identificabilă (persoană vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare” ([18]), se poate concluziona în mod evident că adresele IP și informațiile privind activitățile asociate acestor adrese constituie date cu caracter personal în toate cazurile relevante aici. Într-adevăr, o adresă IP servește drept număr de identificare ce permite găsirea numelui abonatului căruia această adresă IP i-a fost atribuită. În plus, informațiile colectate cu privire la abonatul care deține o adresă IP („acesta a încărcat anumite materiale pe site-ul web ZS la 1 ianuarie 2010 ora 15:00”) *au legătură cu, respectiv* se referă în mod clar la activitățile unei persoane fizice identificabile (deținătorul adresei IP) și, astfel trebuie să fie considerate, de asemenea, date cu caracter personal.

([13]) Tehnologia P2P este o arhitectură software de prelucrare distribuită care permite unor calculatoare individuale să se conecteze și să comunice direct cu alte calculatoare.

([14]) Exemple de sancțiuni alternative ar include limitarea funcționalității conexiunii la internet, de exemplu, viteza conexiunii, volumul etc.

([15]) A se vedea în special CEDO 26 iunie 2006, *Weber și Saravia/Germania* (dec.), nr. 54934/00, alineatul (77) și CEDO 1 iulie 2008, *Liberty și alții/UK*, nr. 58243/00.

([16]) Curtea de Justiție are o abordare amplă a aplicabilității Directivei 95/46/CE, ale cărei prevederi trebuie să fie interpretate în lumina articolului 8 CEDO. Curtea de Justiție a afirmat în hotărârea sa din 20 mai 2003, *Rundfunk*, cauzele conexate C-465/00, C-138/01 și C-139/01, Rec. 2003, p. I-4989, alineatul (68), că „dispozițiile Directivei 95/46/CE în măsura în care acestea guvernează prelucrarea datelor cu caracter personal susceptibilă să încalce libertățile fundamentale, în special dreptul la viața privată, trebuie să fie interpretate în mod obligatoriu în lumina drepturilor fundamentale care, în conformitate cu jurisprudența stabilită, fac parte integrantă din principiile generale de drept a căror respectare este asigurată de Curte”.

([17]) Adresa IP pe care FSI o atribuie unei persoane fizice poate fi aceeași de fiecare dată când acesta navighează pe internet (denumită adresă IP statică). Alte adrese IP sunt dinamice, însemnând că furnizorul de acces la internet atribuie o adresă IP diferită clienților săi ori de câte ori aceștia se conectează la internet. În mod evident, FSI poate să asocieze adresa IP cu contul abonatului căruia acesta i-a atribuit adresa IP (dinamică sau statică).

([18]) Considerentul 26 completează această definiție: „Întrucât principiile protecției trebuie să se aplice oricărei informații privind o persoană identificată sau identificabilă; întrucât, pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată; întrucât principiile protecției nu se aplică datelor anonime astfel încât persoana vizată să nu mai fie identificabilă; …”.

28. Aceste opinii sunt împărtășite în totalitate de Grupul de lucru instituit în temeiul articolului 29 care, într-un document privind aspectele legate de drepturile de proprietate intelectuală, a afirmat că adresele IP colectate în scopul protejării drepturilor de proprietate intelectuală, *respectiv* pentru identificarea utilizatorilor de internet despre care se presupune că au încălcat drepturile de proprietate intelectuală, sunt date cu caracter personal în măsura în care acestea sunt folosite pentru protejarea acestor drepturi împotriva unei anumite persoane fizice ([19]).

29. Directiva 2002/58/CE este, de asemenea, aplicabilă deoarece politicile privind deconectarea de la internet după trei abateri consecutive atrag colectarea datelor privind traficul și comunicațiile. Directiva 2002/58/CE reglementează utilizarea acestor date și prevede principiul confidențialității comunicărilor efectuate prin intermediul rețelelor publice de comunicații și al datelor inerente acestor comunicări.

IV.3. **Dacă politicile privind deconectarea de la internet după trei abateri consecutive constituie o măsură necesară**

30. Articolul 8 din CEDO prevede principiul necesității potrivit căruia orice măsură care încalcă dreptul la viața privată al persoanelor fizice este permisă numai dacă acesta constituie o măsură necesară în cadrul unei societăți democratice pentru scopul legitim pe care îl urmărește ([20]). Principiul necesității poate fi găsit și în articolele 7 și 13 din Directiva 95/46/CE și în articolul 15 din Directiva 2002/58/CE ([21]). Principiul necesită o analiză a proporționalității măsurii, care trebuie să fie evaluată pe baza echilibrului între interesele implicate, în contextul societății democratice în ansamblu ([22]). De asemenea, acesta implică o evaluare în ceea ce privește existența unor măsuri alternative care să fie mai puțin invazive.

31. Deși AEPD recunoaște importanța protejării drepturilor de proprietate intelectuală, aceasta consideră că politica privind deconectarea de la internet după trei abateri consecutive astfel cum este cunoscută în prezent – implicând anumite elemente cu aplicare generală – constituie o măsură disproporționată și, în consecință, nu poate fi considerată drept o măsură necesară. AEPD are, de asemenea, convingerea că există soluții alternative, mai puțin invazive sau că politicile prevăzute pot fi realizate într-o manieră mai puțin invazivă sau pot avea un domeniu de aplicare mai limitat. De asemenea, la nivel legal mai detaliat, abordarea celor trei abateri consecutive ridică anumite probleme. Aceste concluzii vor fi explicate mai jos.

Politicile care utilizează abordarea celor trei abateri consecutive sunt disproporționate

32. AEPD dorește să sublinieze natura amplă a măsurilor impuse. În acest sens, trebuie menționate următoarele elemente:

(i) faptul că monitorizarea (neobservată) ar afecta milioane de persoane fizice și *toți* utilizatorii indiferent dacă aceștia sunt suspectați;

(ii) monitorizarea ar atrage înregistrarea sistematică a datelor, iar unele dintre acestea pot determina chemarea persoanelor în fața instanțelor civile sau chiar penale; mai mult, anumite informații colectate ar putea fi calificate, în consecință, drept date sensibile în temeiul articolului 8 din Directiva 95/46/CE care necesită garanții mai solide;

(iii) este probabil ca monitorizarea să atragă multe cazuri fals pozitive. Încălcarea drepturilor de autor nu reprezintă o întrebare cu răspuns clar „da" sau „nu". Deseori, instanțele trebuie să analizeze volume semnificative de amănunte tehnice și juridice din zeci de pagini pentru a stabili dacă există o încălcare ([23]);

([19]) Grupul de lucru instituit în temeiul articolului 29, Document de lucru privind aspecte de protecție a datelor aferente drepturilor de proprietate intelectuală (GL 104), adoptat la 18 ianuarie 2005. Acest Grup de lucru a fost instituit conform articolului 29 din Directiva 95/46/CE. Este un organ consultativ independent european privind protecția datelor și a vieții private. Atribuțiile acestuia sunt descrise în articolul 30 din Directiva 95/46/CE și în articolul 15 din Directiva 2002/58/CE. A se vedea și avizul Grupului de lucru nr. 4/2007 privind conceptul de date cu caracter personal (GL 136), adoptat la 20 iunie 2007, mai ales pagina 16.

([20]) Articolul 8 CEDO se referă în mod expres la cerința potrivit căreia orice implicare sau restricție trebuie să fie „necesară într-o societate democratică".

([21]) Articolul 13 din Directiva 95/64/CE permite o restricție numai atunci când aceasta constituie „o măsură necesară pentru a proteja: (a) securitatea statului; (b) apărarea; (c) siguranța publică; (d) prevenirea, investigarea, detectarea și punerea sub urmărire a infracțiunilor sau a încălcării eticii în cazul profesiunilor reglementate; (e) un interes economic sau financiar important al unui stat membru sau al Uniunii Europene, inclusiv în domeniile monetar, bugetar și fiscal; (f) o funcție de monitorizare, inspecție sau de reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la literele (c), (d) și (e); (g) protecția persoanei vizate sau a drepturilor și libertăților altora". Articolul 15 din Directiva 2002/58/CE prevede că „restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (mai exact, siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE".

([22]) A se vedea și CEDO 2 august 1984, *Malone/Regatul Unit*, seria A nr. 82, p. 32, alineatele (81) și următoarele. Și CEDO 4 decembrie 2008, *Marper/Regatul Unit* [GC], nr. 30562/04 și 30566/04, alineatul (101) și următoarele.

([23]) Este posibil ca instanțele să fie nevoite să evalueze dacă materialele sunt într-adevăr protejate de drepturi de autor, care din drepturi au fost încălcate, dacă uzul poate fi considerat drept un caz de utilizare corectă, legea aplicabilă, daunele etc.

(iv) potențialele *efecte* ale monitorizării, care ar putea avea drept rezultat întreruperea accesului la internet. Aceasta ar reprezenta o ingerință cu privire la dreptul persoanelor la libertatea de exprimare, libertatea de informare și accesul la cultură, la aplicațiile e-guvern, piețe, e-mail și, în anumite cazuri, la activitatea profesională. În acest context, este deosebit de important să se realizeze că efectele vor fi resimțite nu numai de presupusul contravenient ci de toate rudele acestuia care folosesc aceeași conexiune de internet, inclusiv elevii care folosesc internetul pentru activitățile școlare;

(v) faptul că entitatea care efectuează evaluarea și care ia decizia va fi, în mod tipic, o entitate privată (*respectiv*, titularii drepturilor de autor sau FSI). Într-un aviz anterior, AEPD și-a exprimat deja preocuparea în legătură cu monitorizarea persoanelor de către sectorul privat (*de exemplu*, FSI sau titularii de drepturi de autor) în domenii care, în principiu, sunt de competența autorităților de aplicare a legii ([24]).

33. AEPD nu are convingerea că beneficiile măsurilor depășesc impactul acestora asupra drepturilor fundamentale ale persoanelor. Protejarea drepturilor de autor reprezintă un interes al titularilor drepturilor și al societății. Cu toate acestea, limitarea drepturilor fundamentale nu pare să fie justificată, dacă se pun în balanță gravitatea ingerinței, *respectiv* scara intervenției în viața privată, astfel cum este evidențiată de elementele de mai sus, și beneficiile scontate, împiedicarea încălcării drepturilor de proprietate individuală care implică – în mare parte – încălcări la scară redusă ale drepturilor de proprietate intelectuală. După cum s-a arătat în Avizul Avocatului General Kokott în *Promusicae*: „Nu este sigur că partajarea privată de fișiere, în special atunci când are loc în lipsa oricărei intenții de obținere a unui profit, reprezintă o amenințare suficient de gravă pentru protecția drepturilor de autor pentru a justifica recurgerea la această excepție. Măsura în care partajarea privată de fișiere produce un prejudiciu real rămâne o problemă încă în dezbatere”. ([25])

34. În acest context, trebuie amintită și reacția Parlamentului European la „schemele celor trei abateri consecutive” în condițiile revizuirii pachetului telecom, în special modificarea nr. 138 la directiva-cadru ([26]). În această modificare se stipula că orice restricție a drepturilor sau libertăților fundamentale poate fi impusă doar dacă aceasta este adecvată, proporțională și necesară în cadrul unei societăți democrate iar punerea în aplicare a acesteia face obiectul unor garanții procedurale adecvate în conformitate cu dispozițiile CEDO și cu principiile generale ale dreptului comunitar, inclusiv protecția judiciară efectivă și dreptul la justiție ([27]).

35. În acest sens, AEPD subliniază, de asemenea, că orice limitare a drepturilor fundamentale va fi supusă analizei atente atât la nivel național, cât și la nivelul UE. În acest context, se poate face o paralelă cu Directiva 2006/24/CE privind păstrarea datelor ([28]), care conține o derogare de la principiul general al protecției datelor privind ștergerea datelor atunci când acestea nu mai sunt necesare pentru scopul în care au fost colectate. Această directivă prevede ca datele de trafic să fie păstrate în scopul combaterii infracțiunilor grave. Trebuie remarcat să păstrarea este permisă numai pentru „infracțiuni grave”, că păstrarea este limitată numai la „datele de trafic” care, în principiu, exclud informațiile privind conținutul comunicărilor și că sunt prezentate garanții stricte. Cu toate acestea, a fost pusă la îndoială compatibilitatea cu standardele drepturilor fundamentare; Curtea Constituțională din România a decis că reținerea totală a datelor nu este compatibilă cu drepturile fundamentale ([29]) și în prezent există o cauză în curs în fața Curții Constituționale din Germania ([30]).

Existența altor mijloace mai puțin invazive

36. Constatările susmenționate sunt întărite de faptul că există mijloace mai puțin invazive pentru realizarea aceluiași scop. AEPD insistă că aceste modele mai puțin invazive ar trebui să fie cercetate și testate.

([24]) Avizul AEPD din 23 iunie 2008 privind propunerea de decizie de stabilire a unui program comunitar multianual privind protejarea copiilor care folosesc internetul și alte tehnologii de comunicații, JO C 2, 7.1.2009, p. 2.

([25]) A se vedea cauza menționată în nota de subsol nr. 8, punctul 106.

([26]) A se vedea Directiva 2009/140/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, JO L 337, 18.12.2009, p. 37.

([27]) Formularea finală a așa-numitei modificări 138 este următoarea: „Articolul 1.3*a*. Măsurile luate de statele membre cu privire la accesul utilizatorilor finali la serviciile și aplicațiile prin rețele de comunicații electronice sau cu privire la utilizarea acestor servicii și aplicații de către utilizatorii finali respectă drepturile și libertățile fundamentale ale persoanelor fizice, astfel cum sunt garantate de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, precum și principiile generale ale dreptului comunitar. Oricare dintre aceste măsuri cu privire la accesul utilizatorilor finali la serviciile și aplicațiile prin rețele de comunicații electronice sau cu privire la utilizarea acestor servicii și aplicații de către utilizatorii finali care ar putea restrânge acele drepturi sau libertăți fundamentale pot fi impuse doar dacă sunt adecvate, proporționale și necesare într-o societate democratică, iar punerea în aplicare a acestora face obiectul unor garanții procedurale adecvate în conformitate cu dispozițiile Convenției europene pentru apărarea drepturilor omului și a libertăților fundamentale și cu principiile generale ale dreptului comunitar, inclusiv o protecție jurisdicțională efectivă și dreptul de a beneficia de garanțiile prevăzute de lege. În consecință, aceste măsuri pot fi adoptate doar cu respectarea deplină a principiului prezumției de nevinovăție și a dreptului la viață privată. Se garantează o procedură prealabilă, echitabilă și imparțială, inclusiv dreptul de a fi audiat al persoanei sau persoanelor vizate, sub rezerva necesității unor condiții și a unor mecanisme procedurale adecvate în cazuri de urgență demonstrate în mod corespunzător, în conformitate cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale. Dreptul la o reexaminare judiciară eficientă și într-un termen rezonabil este garantat”.

([28]) Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006, JO L 105, 13.4.2006, p. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. În acest context, AEPD reamintește că Directiva 2002/22/CE, modificată, privind serviciile universale și drepturile utilizatorilor în legătură cu rețelele și serviciile de comunicații electronice (denumită „directiva privind drepturile cetățenilor"), care face parte din pachetul telecom recent reformat, conține anumite norme și proceduri pentru limitarea încălcării la scară redusă a drepturilor de autor în rândul consumatorilor ([31]). Aceste proceduri includ obligația statelor membre de a elabora informații standardizate de interes public privind diferite teme, în care să se precizeze în mod specific încălcările drepturilor de autor și a celor conexe precum și consecințele legale ale acestora ([32]). Statele membre pot ulterior să solicite FSI să distribuie aceste materiale tuturor clienților și să le includă în contractele lor.

38. Scopul sistemului este de a informa și de a descuraja persoanele fizice să disemineze informații protejate de drepturi de autor și să se implice în activități de încălcare, în timp ce se evită monitorizarea folosirii internetului și motivele de îngrijorare privind protecția vieții private și a datelor. Directiva privind drepturile cetățenilor trebuie să fie pusă în aplicare în mai 2011; astfel, aceste proceduri nu au fost încă instituite. Prin urmare, încă nu au existat ocazii de testare a acestor beneficii. Astfel, este prematur să se omită potențialul rezultat benefic al acestor noi proceduri și să se accepte în schimb „politicile privind deconectarea după trei abateri consecutive", care limitează în mult mai mare măsură drepturile fundamentale.

39. În plus față de cele de mai sus, trebuie să reamintim că Directiva 2004/48/CE din 28 aprilie 2004 privind respectarea drepturilor de proprietate intelectuală prevede diferite instrumente pentru protecția drepturilor de proprietate intelectuală înaintea instanțelor judecătorești [dezbătute mai jos în alineatul (43) și următoarele] ([33]).

40. Directiva ADPI (*directiva privind respectarea drepturilor de proprietate intelectuală*) a fost recent transpusă în legislația statelor membre. Până în prezent, nu a existat suficient timp pentru evaluarea adecvării dispozițiilor acesteia în scopul protejării drepturilor de proprietate intelectuală. În consecință, orice necesitate de a înlocui sistemul curent bazat pe proceduri judiciare, care nu a fost încă testat, este cel puțin îndoielnică. Cele de mai sus ridica inevitabila întrebare privind motivul pentru care încălcările existente nu pot fi soluționate în mod adecvat prin penalitățile civile și penale existente pentru încălcarea drepturilor de autor. Astfel, înainte de a propune astfel de măsuri de politică, Comisia ar trebui să prezinte informații fiabile care să arate că prin cadrul legal existent nu s-au putut obține efectele scontate.

41. De asemenea, nu este clar dacă s-au analizat cu seriozitate modelele alternative economice comerciale care nu ar implica monitorizarea sistematică a persoanelor. De exemplu, dacă titularii drepturilor de autor își demonstrează pierderile cauzate de uzul P2P, aceștia și FSI ar putea, de exemplu, să testeze utilizarea unor abonamente diferențiate de acces la internet în care o parte din prețul unui abonament cu acces nelimitat este repartizat titularilor de drepturi de autor.

Posibilitatea de a realiza monitorizarea specifică într-un mod mai puțin invaziv

42. În afară de utilizarea unor modele complet diferite care, astfel cum s-a arătat, ar trebui să fie cercetate și testate, monitorizarea specifică ar putea în orice caz să fie realizată într-un mod mai puțin invaziv.

43. Scopul protejării drepturilor de proprietate intelectuală poate fi realizat prin monitorizarea doar a unui număr limitat de persoane suspectate a fi implicate în activități de încălcare gravă a drepturilor de autor. Directiva ADPI oferă anumite orientări în acest sens. Aceasta prevede condițiile în care autoritățile pot dispune ca datele cu caracter personal deținute de furnizorii de acces la internet să fie dezvăluite în scopul protejării drepturilor de proprietate intelectuală. Articolul 8 prevede că FSI pot fi obligați de autoritățile judiciare competente să furnizeze informații cu caracter personal pe care aceștia le dețin cu privire la presupușii contravenienți (de exemplu, informații privind proveniența și rețelele de distribuție a bunurilor sau serviciilor care încalcă drepturile de proprietate intelectuală) ca răspuns la o cerere justificată și proporțională în cazurile de încălcări la *scară comercială* ([34]).

44. Astfel, criteriul „scării comerciale" este decisiv. În conformitate cu acest criteriu, monitorizarea poate fi proporțională în contextul unor situații limitate, specifice și *ad hoc*, în care există suspiciuni bine fondate de abuz al

([31]) A se vedea Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, JO L 337, 18.12.2009, p. 11.

([32]) În special, articolul 21 alineatul (4) din Directiva 2009/136/CE stipulează că „Statele membre pot solicita ca întreprinderile menționate la alineatul (3) să distribuie gratuit informații de interes public abonaților existenți sau noi atunci când este cazul, prin aceleași mijloace care sunt utilizate în mod normal de acestea pentru comunicarea cu abonații. În acest caz, astfel de informații sunt furnizate într-o formă standardizată de autoritățile publice relevante și privesc, *inter alia*, următoarele aspecte (a) cele mai frecvente utilizări ale serviciilor de comunicații electronice pentru a se implica în activități ilegale sau pentru a disemina conținuturi dăunătoare, în special atunci când acestea ar putea aduce atingere respectării drepturilor și libertăților celorlalți, inclusiv încălcări ale drepturilor de autor și ale drepturilor conexe și consecințele juridice ale acestora (…)." Mai mult, în conformitate cu articolul 20 alineatul (2), „De asemenea, statele membre pot solicita ca în contract să fie incluse toate informațiile care ar putea fi furnizate de către autoritățile publice relevante în acest scop cu privire la utilizarea rețelelor și a serviciilor de comunicații electronice pentru a se implica în activități ilegale sau pentru a disemina conținuturi dăunătoare, precum și cu privire la mijloacele de protecție împotriva riscurilor la adresa siguranței personale, a vieții private și a datelor cu caracter personal, menționate la articolul 21 alineatul (4) și relevante pentru serviciile furnizate".

([33]) JO L 157, 30.4.2004, p. 45 (în continuare: Directiva ADPI).

([34]) Acest lucru este confirmat și în considerentul 14 al Directivei ADPI.

drepturilor de autor la scară comercială. Acest criteriu ar putea include situații de abuz clar al drepturilor de autor exercitat de persoane fizice cu scopul de a obține beneficii comerciale economice directe sau indirecte.

45. În practică, pentru ca cele de mai sus să fie eficace, titularii drepturilor de autor se implică în monitorizarea specifică a anumitor adrese IP pentru a verifica scara la care sunt încălcate drepturile de autor. Aceasta ar însemna că titularilor de drepturi de autor li s-ar permite, de asemenea, să păstreze o evidență a rapoartelor cu presupusele încălcări în același scop. Aceste informații ar trebui să fie folosite doar după ce se verifică importanța încălcării. De exemplu, cazurile clare de încălcări majore precum și cele nesemnificative dar continue, de-a lungul unei anumite perioade de timp, în scopul obținerii de avantaje comerciale sau de câștiguri financiare. Necesitatea de continuitate pe parcursul anumitor perioade de timp este accentuată și explicată suplimentar mai jos în dezbaterea legată de principiu conservării.

46. Aceasta ar însemna că în astfel de cazuri, colectarea de informații în scopul demonstrării unui presupus abuz prin intermediul internetului poate fi considerată proporțională și necesară în scopul pregătirii procedurilor legale inclusiv a acțiunilor în justiție.

47. AEPD consideră, ca garanție suplimentară, că operațiunile de prelucrare a datelor care vizează colectarea acestui tip de probe ar trebui să fie în prealabil verificate și autorizate de autoritățile naționale pentru protecția datelor. Aceste opinii se bazează pe faptul că operațiunile de prelucrare a datelor ar prezenta riscuri specifice pentru drepturile și libertățile persoanelor având în vedere scopul acestora, *respectiv* desfășurarea de acțiuni de protejare care ar putea în cele din urmă să fie de natură penală și având în vedere natura sensibilă a datelor colectate. Faptul că prelucrarea implică monitorizarea comunicațiilor electronice reprezintă un factor suplimentare care impune sporirea supravegherii.

48. AEPD consideră că „scara comercială" stipulată în Directiva ADPI reprezintă un element foarte adecvat pentru stabilirea limitelor monitorizării în vederea respectării principiului proporționalității. În plus, nu par să existe probe fiabile care să arate, conform criteriilor prevăzute în ADPI, că acțiunile legale efective împotriva încălcării drepturilor de autor se dovedesc a nu fi posibile sau eficace. De exemplu, rapoarte precum cel din Germania, în care începând din 2008, după transpunerea Directivei ADPI, au existat aproximativ 3 000 de hotărâri judecătorești conform cărora FSI au dezvăluit instanțelor informații referitoare la 300 000 de abonați, par să sugereze opusul.

49. În concluzie, dat fiind că Directiva ADPI este în vigoare numai de doi ani, este dificil să înțelegem de ce legiuitorii ar renunța la criteriile prevăzute în această directivă în favoarea unor metode mult mai invazive într-un moment în care UE abia începe să le testeze pe cele recent adoptate. Din același motiv, este la fel de dificil să se înțeleagă nevoia de a înlocui sistemul actual bazat pe acțiunile în justiție cu alt tip de măsuri (în plus față de întrebările privind asigurarea dreptului la justiție, care nu sunt abordate aici).

IV.4. **Conformitatea politicilor privind deconectarea de la internet după trei abateri consecutive cu dispozițiile mai detaliate privind protecția datelor**

50. Există alte motive legale mai specifice pentru care această abordare a celor trei abateri consecutive este problematică din punctul de vedere a protecției datelor. AEPD dorește să sublinieze temeiul juridic îndoielnic pentru prelucrare, care este impus prin Directiva 95/46/CE, și obligația inclusă în Directiva 2002/58/CE de a elimina fișierele-jurnal.

Temeiul juridic pentru prelucrare

51. Măsurile care se bazează pe abordarea celor trei abateri consecutive implică prelucrarea de date cu caracter personal, unele din acesta urmând a fi utilizate pentru proceduri juridice sau administrative în scopul întreruperii accesului la internet al contravenienților. Din această perspectivă, aceste date sunt calificate drept date sensibile în temeiul articolului al Directivei 95/46/CE. Articolul 8 alineatul (5) stabilește că „Prelucrarea datelor referitoare la infracțiuni, condamnări penale sau măsuri de securitate se poate efectua numai sub controlul autorității publice sau dacă garanțiile corespunzătoare și specifice sunt prevăzute de dreptul intern …".

52. În acest context, este pertinent să se amintească documentul menționat anterior al Grupului de lucru instituit în temeiul articolului 29 în care se discută aspectul prelucrării datelor cu caracter judiciar ([35]). Grupul de lucru afirmă că „Deși orice persoană beneficiază în mod evident de dreptul de a prelucra date judiciare în cadrul unui litigiu propriu, principiul nu se extinde la investigații amănunțite, colectarea și centralizarea datelor cu caracter personal de către terți incluzând, în special, cercetări sistematice la scară generală, precum analiza internetului (…). O astfel de investigație este de competența autorităților judiciare" ([36]). În timp ce colectarea de probe orientate, specifice, în special în cazul încălcărilor grave, poate fi necesară pentru a stabili și a exercita o acțiune în instanță, AEPD împărtășește în totalitate opiniile Grupului de lucru instituit în temeiul articolului 29 cu privire la lipsa legitimității anchetelor pe scară largă care implică prelucrarea unor volume masive de date ale utilizatorilor de internet.

53. Discuția privind principiul proporționalității de mai sus și criteriul „scării comerciale" este relevantă pentru stabilirea condițiilor în care colectarea adreselor IP și a informațiilor conexe va fi legitimă.

([35]) A se vedea alineatul 28 din prezentul aviz.
([36]) Subliniere adăugată.

54. FSI ar putea încerca să confere un caracter legitim prelucrării efectuate de titularii drepturilor de autor prin introducerea unor clauze în contractele cu clienții care să le permită monitorizarea datelor acestora și întreruperea abonamentelor respective. Prin încheierea acestor contracte, s-ar considera că clienții sunt de acord cu monitorizarea. Totuși, această practică ridică în primul rând întrebarea de bază dacă persoanele fizice își pot exprima consimțământul față de FSI pentru o prelucrare a datelor care nu va fi desfășurată de FSI ci de terți care nu sunt sub „autoritatea" FSI.

55. În al doilea rând, există întrebarea privind validitatea consimțământului. Articolul 2 litera (h) din Directiva 95/46/CE definește consimțământul ca „orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc". Un aspect important este că pentru a fi valid, consimțământul, indiferent de circumstanțele în care este exprimat, trebuie să fie o manifestare de voință, liberă, specifică și informată a dorințelor persoanei vizate, astfel cum este definit în articolul 2 litera (h) din directivă. AEPD are îndoieli serioase că persoanele fizice cărora li se cere consimțământul pentru monitorizarea activităților proprii pe internet vor avea posibilitatea unei alegeri efective – în special deoarece alternativa va fi lipsa accesului la internet, ceea ce ar periclita multe alte aspecte ale vieții acestora.

56. În al treilea rând, este deosebit de îndoielnică posibilitatea ca o astfel de monitorizare să fie considerată vreodată *necesară* pentru executarea unui contract la persoana vizată este parte, după cum se cere în articolul 7 alineatul (b) din Directiva 95/46/CE, având în vedere că monitorizarea nu face obiectul contractului semnat de persoana vizată, ci numai un mijloc pentru ca FSI să servească alte interese.

Eliminarea fișierelor-jurnal

57. Conform Directivei 2002/58/CE, în special articolul 6, datele de trafic, precum adresele IP pot fi colectate și stocate numai din motivele direct legate de comunicația propriu-zisă, incluzând facturarea, gestionarea traficului și prevenirea fraudei. Ulterior, datele trebuie să fie șterse. Aceasta nu va aduce atingere obligațiilor în temeiul directivei privind păstrarea datelor care, astfel cum s-a arătat, prevede păstrarea datelor de trafic și comunicarea acestora către poliție și procurori pentru a contribui **exclusiv la anchetarea infracțiunilor grave** ([37]).

([37]) A se vedea punctul 35 al prezentului aviz.

58. În conformitate cu cele de mai sus, furnizorii de servicii de internet ar trebui să elimine orice fișiere-jurnal care dezvăluie activitățile utilizatorilor de internet care nu mai sunt necesare pentru scopurile susmenționate. Având în vedere că fișierele-jurnal nu sunt necesare în scopul facturării, s-ar părea că trei sau patru săptămâni ar fi suficiente pentru FSI în vederea gestionării traficului ([38]).

59. Aceasta înseamnă că, atunci când sunt contactați de titularii drepturilor de autor, cu excepția cazurilor în care acest contact are loc în perioada limită specificată mai sus, FSI nu ar trebui să dețină fișierele-jurnal care să asocieze adresele IP cu abonații corespunzători. Păstrarea fișierelor-jurnal după această perioadă ar trebui să se realizeze doar din motive justificate în sfera scopurilor prevăzute de lege.

60. În termeni practici, aceasta înseamnă că, în afara cazurilor în care sunt prezentate foarte repede, cererile titularilor de drepturi de autor către FSI nu vor putea fi îndeplinite, din simplul motiv că FSI nu vor mai deține respectivele informații. Aceasta în sine stabilește limitele a ceea ce înseamnă practici acceptabile de monitorizare descrise în secțiunea de mai sus.

Riscurile de efecte colaterale

61. AEPD este, de asemenea, preocupată nu numai în privința impactului politicilor privind deconectarea de la internet după trei abateri consecutive asupra protecției vieții private și a datelor ci și în privința efectelor colaterale ale acestora. Dacă politicile privind deconectarea de la internet după trei abateri consecutive ar fi permise, acestea ar reprezenta o etapă foarte periculoasă către legitimizarea unor activități chiar mai ample de supraveghere a utilizatorilor de internet în diferite domenii și în diferite scopuri.

62. AEPD solicită Comisiei să se asigure că ACTA nu depășește și nu contravine regimului actual al UE pentru protejarea DPI, care respectă drepturile și libertățile fundamentale și libertățile civile, precum protecția datelor cu caracter personal.

V. **MOTIVE DE ÎNGRIJORARE PRIVIND PROTECȚIA DATELOR ÎN RAPORT CU MECANISMELE DE COOPERARE INTERNAȚIONALĂ**

63. Unul dintre mijloacele avansate de participanții la ACTA pentru abordarea aspectului protejării DPI este

([38]) Gestionarea traficului include analiza traficului rețelei informatice pentru a optimiza sau garanta performanța, timpul de așteptare mai redus și/sau creșterea lărgimii de bandă utilizabilă.

îmbunătățirea cooperării internaționale printr-o serie de măsuri care ar permite aplicarea efectivă a drepturilor de proprietate intelectuală în jurisdicțiile semnatarilor ACTA.

64. Având în vedere informațiile disponibile, se poate preconiza că mai multe dintre măsurile planificate pentru asigurarea protejării drepturilor de proprietate intelectuală vor implica partajarea de informații la nivel internațional cu privire la presupusele încălcări ale DPI între autorităților publice (precum autoritățile vamale, polițienești sau judiciare) dar și între factorii publici și privați (precum FSI și organizațiile titularilor de drepturi PI). Astfel de transferuri de date ridică o serie de probleme din perspectiva protecției datelor.

V.1. **Sunt schimburile de date avute în vedere în contextul ACTA legitime, necesare și proporționale?**

65. În stadiul actual al procesului de negocieri, în care o serie de elemente concrete privind prelucrarea de date sunt fie nedefinite, fie necunoscute, este imposibil să se verifice conformitatea cadrului propus de măsuri cu principiile fundamentale ale protecției datelor și cu legislația comunitară privind protecția datelor.

66. În primul rând, se poate pune întrebarea dacă sunt legitime transferurile de date către țări terțe în contextul ACTA. Relevanța adoptării măsurilor la nivel internațional în acel domeniu poate fi pusă la îndoială atâta timp cât nu există un acord între statele membre UE privind armonizarea măsurilor de protecție în mediul digital și tipurile de sancțiuni penale care trebuie aplicate ([39]).

67. Având în vedere cele de mai sus, se pare că principiul necesității și cel al proporționalității transferurilor de date conform ACTA ar putea fi îndeplinite mai ușor dacă acordul s-ar limita în mod expres la lupta împotriva celor mai grave infracțiuni de încălcare a DPI, în loc să permită transferurile de date în vrac în legătură cu orice suspiciuni de încălcare a DPI. Aceasta ar necesita definirea clară a domeniului a ceea ce constituie „cele mai grave infracțiuni de încălcare a DPI" pentru care pot avea loc transferuri de date.

68. În plus, o atenție deosebită ar trebui acordată persoanelor implicate în schimbul de date și întrebării dacă schimbul de date va avea loc numai între autoritățile publice sau dacă aceste date vor implica schimburi între factorii privați și autoritățile publice. Astfel cum s-a arătat mai sus în prezentul aviz, implicarea factorilor privați într-un domeniu care în principiu este de competența autorităților de aplicare a legii ridică o serie de probleme ([40]). Condițiile în care factorii privați vor fi implicați în colectarea și schimbul de date cu caracter personal în legătură cu de încălcarea DPI cu autoritățile publice ar trebui să fie limitate strict la circumstanțe specifice cu garanții adecvate.

V.2. **Legislația privind protecția datelor aplicabilă transferurilor de date în contextul ACTA**

Regimul general pentru transferul de date

69. Cadrul general pentru protecția datelor aplicabil în UE este prevăzut în Directiva 95/46/CE. Articolele 25 și 26 din Directiva 95/46/CE definesc regimul aplicabil transferurilor de date către țări terțe. Articolul 25 prevede ca transferurile să fie efectuate numai către țările care asigură un nivel adecvat de protecție, în caz contrar, aceste transferuri fiind, în principiu, interzise.

70. Gradul de adecvare pe care țările terțe în pot oferi este evaluat de la caz la caz de către Comisia Europeană, care a emis mai multe decizii în care este recunoscut caracterul adecvat al mai multor țări în urma unei analize riguroase realizate de Grupul de lucru instituit în temeiul articolului 29 ([41]).

71. AEPD observă că majoritatea participanților la ACTA nu sunt incluși în lista întocmită de Comisie a țărilor care oferă o protecție adecvată a datelor: cu excepția Elveției și – în circumstanțe speciale – a Canadei și SUA, toți ceilalți participanți la ACTA nu sunt recunoscuți ca țări care asigură un nivel adecvat de protecție. Aceasta înseamnă că, pentru a putea fi transferate date din UE către aceste țări, trebuie îndeplinită una dintre condițiile de la articolul 26 alineatul (1) din Directiva 95/46/CE sau părțile trebuie să prezinte garanții adecvate pentru transferul de date în conformitate cu articolului 26 alineatul (2) din directivă.

Regimul specific al transferurilor de date în domeniul aplicării dreptului penal

72. Deși Directiva 95/46/CE constituie principalul instrument pentru protecția datelor în UE, domeniul de aplicare al acesteia este în prezent limitat deoarece exclude activități privind, *inter alia*, activitățile statului în domeniul dreptului

([39]) În prezent, o propunere privind sancțiunile penale se dezbate în cadrul Consiliului, COM(2006) 168 din 26 aprilie 2006.

([40]) A se vedea punctele 32 și 52 ale prezentului aviz. A se vedea și Avizul AEPD din 11 noiembrie 2008 privind Raportul final al Grupului de contact la nivel înalt UE-SUA privind schimbul de informații și protecția vieții private și a datelor cu caracter personal, JO C 128, 6.6.2009, p. 1.

([41]) A se vedea deciziile privind caracterul adecvat acordate de Comisia Europeană Argentinei, Canadei, Elveției, US Safe Harbor și autorităților Statelor Unite în contextul PNR, Guernsey, Isle of Man, și Jersey; disponibile la http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

penal (articolul 3). Schimburile de date în scopul aplicării dreptului penal nu vor intra, în consecință, sub incidența Directivei 95/46/CE și vor face obiectul principiilor generale de protecție a datelor stipulate în Convenția nr. 108 a Consiliului Europei și în Protocolul adițional la care toate statele membre ale UE sunt parte ([42]). În plus, se vor aplica normele adoptate de UE privind cooperarea judiciară și polițienească în materie penală care sunt prevăzute în Decizia-cadru 2008/877/JAI a Consiliului ([43]).

73. De asemenea, aceste instrumente impun ca principiu faptul că trebuie să existe un nivel adecvat de protecție a datelor în țările terțe în care datele urmează să fie transferate. Sunt prevăzute o serie de derogări, în special atunci când țările terțe oferă garanții adecvate. În mod similar schimburilor de date în temeiul Directivei 95/46/CE, schimburile de date în domeniul aplicării dreptului penal vor necesita, în consecință, prezentarea unor garanții adecvate de către părțile la transferul de date pentru ca acest transfer să poată avea loc.

Către un nou regim al transferurilor de date

74. Se poate preconiza că în viitorul apropiat în UE vor fi adoptate noi norme comune privind protecția datelor aplicabile tuturor domeniilor de activitate ale UE, în temeiul articolului 16 din TFUE. Aceasta înseamnă că peste câțiva ani UE ar putea dispune de un cadrul cuprinzător privind protecția datelor, care să prevadă norme coerente pentru protecția datelor în toate domeniile de activitate ale UE, impunând același nivel de securitate și garanții pentru toate activitățile de prelucrare a datelor. Astfel cum a subliniat Viviane Reding ([44]), Comisarul pentru justiție, drepturi fundamentale și cetățenie, acest nou cadru trebuie să funcționeze ca un unic „instrument juridic modern și exhaustiv" pentru protecția datelor în UE. Un astfel de cadru este cu atât mai oportun cu cât ar aduce mai multă claritate și constanță în ceea ce privește normele aplicabile în UE în privința protecției datelor.

75. Într-un context internațional, AEPD indică Rezoluția privind standardele internaționale pentru protecția datelor cu caracter personal și a vieții private adoptată recent de autoritățile de protecție a datelor, ceea ce reprezintă un prim pas către stabilirea unor standarde globale de protecție a datelor ([45]). Standardele internaționale includ o serie de garanții pentru protecția datelor similare celor indicate în Directiva 95/46/CE și în Convenția nr. 108. Chiar dacă Standardele internaționale nu au încă forță obligatorie, acestea oferă totuși orientări utile cu privire la principiile de protecție a datelor care pot fi puse în aplicare, în mod voluntar, de către țările terțe astfel încât cadrul legal al acestora să fie compatibil cu standardele UE. AEPD consideră că semnatarii ACTA trebuie să ia în considerare și principiile stipulate în Standardele internaționale atunci când prelucrează date cu caracter personal provenind din UE.

V.3. **Necesitatea punerii în aplicare a unor garanții adecvate pentru protejarea transferurilor de date din UE către țări terțe**

Ce formă vor lua garanțiile în vederea protejării efective a transferurilor de date către țările terțe?

76. Dacă se demonstrează necesitatea transferului de date cu caracter personal către țările terțe, AEPD subliniază că Uniunea Europeană ar trebui să negocieze cu țările terțe destinatare – în plus față de acordul privind ACTA – instrumente specifice care să conțină garanții pentru protecția datelor pentru reglementarea schimbului de date cu caracter personal.

77. Garanțiile adecvate pentru protecția datelor ar trebui să fie prevăzute în mod normal într-un acord obligatoriu între UE și țările terțe destinatare, prin care destinatarul se obligă să respecte legislația UE privind protecția datelor și să ofere persoanelor fizice aceleași drepturi și căi de atac precum cele acordate în temeiul dreptului UE. Necesitatea unui acord obligatoriu derivă din articolul 26 alineatul (2) din Directiva 95/46/CE și articolul 13 alineatul (3) litera (b) din decizia-cadru și, în plus, este sprijinită de practicile existente ale UE de a încheia acorduri specifice pentru a permite transferurile de date către țări terțe ([46]).

78. În mod similar, conform proiectului de standarde internaționale, destinatarului i se poate cere să garanteze că va asigura nivelul obligatoriu de protecție pentru transferurile care urmează să aibă loc. Aceste garanții ar putea fi transpuse și într-un angajament contractual.

Conținutul garanțiilor care trebuie prezentate de semnatarii ACTA în ceea ce privește transferurile de date cu caracter personal

79. AEPD subliniază în special că schimburile internaționale de informații în scopul aplicării legii sunt deosebit de sensibile din perspectiva protecției datelor deoarece un cadru ar putea conferi legitimitate transferurilor masive de date

([42]) Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal adoptată la Strasbourg la 28 ianuarie 1981 și Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal cu privire la autoritățile de supraveghere și fluxurile transfrontaliere de date din 8 noiembrie 2001 de la Strasbourg.

([43]) Decizia-cadru 2008/877/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării judiciare și polițienești în materie penală, JO L 350, 30.12.2008, p. 60.

([44]) A se vedea Răspunsurile la chestionarul Parlamentului European pentru Comisarul desemnat Viviane Reding, p. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Rezoluție adoptată la Madrid în noiembrie 2009.

([46]) De exemplu acordurile Europol și Eurojust cu SUA, acordul PNR, Acordul Swift, acordul între UE și Australia privind prelucrarea și transferul de către transportatorii aerieni către Serviciul vamal australian de date din registrul de nume ale pasagerilor (PNR) provenind din Uniunea Europeană.

într-un domeniu în care impactul asupra persoanelor fizice este deosebit de semnificativ și în care cu atât mai mult sunt necesare garanții stricte și fiabile.

80. AEPD subliniază că garanțiile și condițiile specifice pot fi definite numai de la caz la caz în lumina tuturor parametrilor schimburilor de date. În scopul orientării, AEPD evidențiază totuși mai jos unele dintre principiile și garanțiile care trebuie să fie prezentate de către destinatarii terți pentru ca transferurile de date să aibă loc:

— trebuie să se verifice care este justificarea legală în baza căreia au loc activitățile de prelucrare a datelor (mai exact, se bazează operațiunile de prelucrare pe o obligație legală, pe consimțământul persoanelor vizate sau pe o altă justificare validă?) și dacă transferurile de date respectă scopul inițial al colectării de date. Nu trebuie să aibă loc niciun transfer care este în afara sferei scopului specificat;

— volumul și tipurile de date cu caracter personal care urmează să fie transferate ar trebui să fie specificate clar și limitate la ceea ce este strict necesar pentru atingerea scopului transferului. Datele cu caracter personal colectate și transferate pot include în special adrese IP ale utilizatorilor de internet, data și ora infracțiunii suspectate și tipul de infracțiune. AEPD recomandă ca datele să nu fie asociate niciunei persoane fizice specifice în timpul fazei de cercetare și amintește că identificarea persoanei suspectate ar trebui să aibă loc numai în conformitate cu legislația și sub controlul unui judecător. În acest sens, AEPD subliniază că datele privind încălcările DPI și suspiciunile de încălcare reprezintă o categorie specială de date iar prelucrarea acestora este rezervată, de regulă, numai autorităților de aplicare a legii și necesită aplicarea unor garanții suplimentare. Persoanele autorizate pentru prelucrarea datelor privind încălcările și suspiciunile de încălcare a DPI și condițiile de prelucrare a acestor date trebuie, prin urmare, să fie definite în mod specific în conformitate cu legislația existentă privind protecția datelor;

— persoanele între care poate exista un schimb de date trebuie să fie prevăzute cu claritate, iar transferurile ulterioare către alți destinatari ar trebui, în principiu, să fie interzise, în afara cazurilor în care acestea sunt necesare pentru o anumită anchetă. Această limitare este deosebit de importantă, deoarece destinatarii desemnați nu ar trebui să efectueze în mod necorespunzător un schimb de informații cu destinatari neautorizați;

— AEPD pornește de la premisa că ACTA nu doar va stipula cooperarea între autoritățile publice, ci va acorda și atribuții de aplicare organizațiilor private (precum FSI, organizațiile titularilor drepturilor de autor etc.). În cazul din urmă, condițiile și nivelul de implicare al organizațiilor private în respectarea DPI trebuie să fie evaluate cu atenție în sensul că măsurile din ACTA nu ar trebui să acorde un drept *de facto* FSI și organizațiilor titulare ale drepturilor IP pentru a monitoriza online comportamentul utilizatorilor. În plus, prelucrarea datelor cu caracter personal de către organizațiile private în contextul aplicării legii trebuie să aibă loc conform unui temei juridic adecvat. De asemenea, este important să se clarifice dacă organizațiile private vor fi obligate să coopereze cu poliția precum și măsura acestei cooperări. În orice caz, aceasta ar trebui să se limiteze la „infracțiuni grave" a căror definiție trebuie, de asemenea, să fie formulată în mod clar având în vedere că nu toate încălcările DPI vor fi considerate infracțiuni grave;

— metoda utilizată pentru schimbul de date cu caracter personal trebuie să fie aleasă cu atenție; în special, ar trebui să se precizeze dacă acesta va fi efectuat prin intermediul unei metode de transmitere de tip „înaintare" – de exemplu FSI și organizațiile titularilor drepturilor PI ar controla transferul unei serii de date către terți, precum poliția sau autoritățile de aplicare a legii situate în străinătate – sau prin intermediul unei metode de tip „retragere" – de exemplu, poliția și autoritățile de aplicare a legii ar avea acces direct la bazele de date ale părților private sau la bazele de date în care sunt centralizate informațiile. După cum s-a subliniat deja în contextul PNR, metoda „înaintare" ar fi singura opțiune care îndeplinește principiile de protecție a datelor din perspectiva UE privind protecția datelor, deoarece permite expeditorului din UE, care cel mai probabil este operatorul de date, să exercite un control asupra transferului de date ([47]);

— trebuie să se specifice perioada în care datele cu caracter personal vor fi păstrate de către destinatari, precum și scopul pentru care această păstrare este necesară. Această perioadă de păstrare trebuie să fie proporțională în raport cu scopul care trebuie atins, însemnând că acele date trebuie să fie eliminate sau șterse atunci când nu mai sunt necesare pentru atingerea scopului;

— obligațiile impuse operatorilor de date din țările terțe trebuie să fie stipulate în mod clar. Mecanismele de control și/sau mecanismele privind obligativitatea asumării răspunderii trebuie să fie garantate astfel încât să existe căi de atac și sancțiuni eficace împotriva operatorilor de date în cazul prelucrării ilegale sau a altor incidente relevante. În plus, trebuie instituite căi de atac, astfel încât persoanele fizice să poată depune o reclamație la o autoritate independentă

([47]) A se vedea Avizul 4/2003 al Grupului de lucru instituit în temeiul articolului 29 privind nivelul de protecție asigurat în SUA pentru transferul datelor pasagerilor, GL78, 13 iunie 2003.

de protecția datelor și astfel încât acestea să poată solicita o soluționare eficientă oricărui tribunal independent și imparțial ([48]);

— actul semnat de părți ar trebui să specifice în mod clar drepturile persoanelor vizate în privința datelor cu caracter personal ale acestora atunci când aceste date sunt prelucrate de către destinatari terți, pentru a se garanta că aceștia dispun de mijloace eficiente de pentru protejarea drepturilor lor în ceea ce privește prelucrarea efectuată în străinătate;

— transparența este cu atât mai importantă, iar părțile la instrumentul privind protecția datelor trebuie să convină asupra modului în care vor informa persoanele vizate în legătură cu prelucrarea datelor care are loc precum și cu drepturile acestora și modul de a le exercita.

VI. **CONCLUZII**

81. AEPD încurajează ferm Comisia Europeană să stabilească un dialog public și transparent privind ACTA, eventual prin intermediul unei consultări publice care, de asemenea, ar ajuta la asigurarea faptului că măsurile care urmează să fie adoptate sunt conforme cu normele legislative privind protecția vieții private și a datelor cu caracter personal.

82. Pe parcursul desfășurării negocierilor privind ACTA, AEPD îndeamnă Comisia Europeană să realizeze un echilibru corect între cererile pentru protecția drepturilor de proprietate intelectuală și drepturile de protecție a vieții private și a datelor. AEPD subliniază că este esențial ca protecția vieții private și a datelor să fie luată în considerare încă de la începutul negocierilor, înainte să se convină asupra vreunei măsuri, astfel încât să nu fie prea târziu pentru a se găsi soluții alternative de respectare a vieții private.

83. Deși proprietatea intelectuală este importantă pentru societate și trebuie să fie protejată, nu ar trebui să fie mai presus de drepturile fundamentale ale persoanelor fizice la viața privată, la protecția datelor, și de alte drepturi precum prezumția de nevinovăție, protecția judiciară efectivă și libertatea de exprimare.

84. În măsura în care actualul proiect al ACTA include sau cel puțin solicită în mod indirect politicile privind deconectarea de la internet după trei abateri consecutive, ACTA ar restricționa profund drepturile și libertățile fundamentale ale cetățenilor europeni, în special protecția datelor cu caracter personal și a vieții private.

85. AEPD consideră că politicile privind deconectarea de la internet după trei abateri consecutive nu sunt necesare pentru a atinge scopul protejării drepturilor de proprietate intelectuală. AEPD are convingerea că există soluții alternative mai puțin invazive sau, cel puțin, că politicile avute în vedere pot fi aplicate într-un mod mai puțin invaziv sau la un nivel mai limitat, în special prin intermediul monitorizării orientate *ad hoc*.

86. Politicile privind deconectarea de la internet după trei abateri consecutive sunt problematice și la un nivel juridic mai amănunțit, în special deoarece prelucrarea datelor judiciare, mai ales de către organizațiile private, trebuie să aibă la bază un temei juridic adecvat. Aplicarea măsurilor care se bazează pe abordarea celor trei abateri consecutive poate să atragă și stocarea de fișiere-jurnal pe termen mai lung, ceea ce ar fi în contradicție cu legislația existentă.

87. În plus, în măsura în care ACTA implică schimburi de date cu caracter personal între autorități și/sau organizații private care se află în țările semnatare, AEPD îndeamnă Uniunea Europeană să implementeze garanțiile adecvate. Aceste garanții ar trebui să se aplice tuturor transferurilor de date efectuate în contextul ACTA – indiferent dacă acestea sunt în domeniul aplicării legii în materie civilă, penală sau digitală – și ar trebui să fie în conformitate cu principiile de protecție a datelor stipulate în Convenția nr. 108 și Directiva 95/46/CE. AEPD recomandă ca aceste garanții să fie transpuse în acorduri obligatorii între expeditorii din UE și destinatarii din țările terțe.

88. De asemenea, AEPD dorește să fie consultată cu privire la măsurile care urmează să fie implementate cu privire la transferurile de date care vor avea loc conform ACTA pentru a verifica proporționalitatea acestora și faptul că acestea garantează un nivel adecvat de protecție a datelor.

Adoptat la Bruxelles, 22 februarie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

([48]) A se vedea Avizul Autorității Europene pentru Protecția Datelor privind Raportul final al Grupului de contact la nivel înalt UE-SUA privind schimbul de informații și protecția vieții private și a datelor cu caracter personal, 11.11.2008.