AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de decizie a Parlamentului European și a Consiliului de stabilire a unui program comunitar multianual privind protecția copiilor care utilizează internetul și alte tehnologii de comunicare

(2009/C 2/02)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

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 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 [2], în special, articolul 41,

având în vedere solicitarea unui aviz primită la 4 martie 2008 din partea Comisiei Europene în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001,

ADOPTĂ PREZENTUL AVIZ:

I. **INTRODUCERE**

Consultarea AEPD

1. Propunerea de decizie a Parlamentului European și a Consiliului de stabilire a unui program comunitar multianual privind protecția copiilor care utilizează internetul și alte tehnologii de comunicare (denumită în continuare „propunerea") a fost trimisă de către Comisie, la 4 martie 2008, Autorității Europene pentru Protecția Datelor în vederea consultării, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001. Consultarea ar trebui menționată explicit în preambulul deciziei.

Propunerea și contextul acesteia

2. Noul program multianual (denumit în continuare „programul") este prezentat în continuarea programelor „Programului pentru un internet mai sigur" („Safer Internet") (1999-2004) și a „Programului pentru un internet mai sigur Plus" („Safer Internet Plus") (2005-2008).

3. Sunt definite patru orientări:

   — reducerea nivelului de conținut ilegal și atacarea problemei comportamentului dăunător din mediul on-line,

   — promovarea unui mediu on-line mai sigur,

   — asigurarea conștientizării la nivel public,

   — stabilirea unei baze de cunoștințe.

4. Programul este prezentat ca fiind consecvent față de politicile, programele și acțiunile comunitare relevante și complementar acestora. Ținând seama de numărul măsurilor de reglementare existente în domeniul protecției copilului în contextul noilor tehnologii, prezentul program se axează pe acțiuni mai mult decât pe reglementări. Accentul este pus pe eficiența și eficacitatea inițiativelor care urmează să fie adoptate și pe adaptarea la evoluția noilor tehnologii. Din această perspectivă, acesta prevede schimburi consolidate de informații și de cele mai bune practici.

5. Fiind un instrument-cadru, programul nu specifică detaliile acțiunilor care urmează a fi întreprinse, dar permite lansarea de invitații pentru prezentarea de propuneri și anunțuri de licitații, în conformitate cu cele patru orientări definite.

Punctele centrale ale avizului

6. Orientările generale ale programului se referă la protecția copiilor care utilizează internetul și alte tehnologii de comunicare, fără a se insista asupra aspectelor legate de confidențialitate ale problemei [3]. Deși susține în totalitate obiectivele propunerii, AEPD va insista, în avizul său, asupra aspectelor legate de confidențialitate.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.

[3] Anumite trimiteri la confidențialitate se regăsesc în evaluarea impactului (3.2.2. Riscuri specifice: dezvăluirea informațiilor cu caracter personal; 3.3. Grupuri țintă; 5.2. Analiza impactului opțiunilor de politică) dar nu sunt suficient dezvoltate.

7. AEPD consideră că este esențială asigurarea consecvenței inițiativelor planificate cu cadrul juridic existent, astfel cum este citat în propunere ([1]), în special cu Directiva 2000/31/CE privind comerțul electronic, Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice și Directiva 95/46/CE privind protecția datelor ([2]).

8. Ar trebui să se țină seama de protecția datelor cu caracter personal în cazul diferitelor aspecte și a diferiților factori interesați implicați în program: protecția datelor cu caracter personal ale copiilor reprezintă fără îndoială aspectul principal, dar nu singurul: ar trebui să se țină seama, de asemenea, de datele cu caracter personal privind persoanele și conținuturile supuse verificărilor în scopul protejării copiilor.

9. În cuprinsul prezentului aviz, aceste aspecte vor fi dezvoltate după cum urmează:

   — Capitolul II va prezenta detaliat legătura dintre protecția datelor și siguranța copiilor, subliniind faptul că protecția datelor copiilor este un pas indispensabil în vederea unei siguranțe sporite și a prevenirii abuzurilor.

   — În capitolul III, avizul va insista asupra faptului că prelucrarea datelor cu caracter personal este inerentă raportării, filtrării sau blocării conținuturilor sau persoanelor care ridică suspiciuni în mediul virtual:

      — la primul punct va fi analizată, din perspectiva protecției datelor, chestiunea raportării cu privire la persoanele sau faptele suspectate,

      — cel de al doilea punct se va axa asupra rolului instrumentelor tehnice,

      — responsabilitatea sectorului în ceea ce privește controlul exercitat de acesta asupra datelor utilizatorilor și a celor referitoare la conținut, va face obiectul ultimului punct.

II. **PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI A SIGURANȚEI COPIILOR**

10. AEPD susține pe deplin obiectivul programului și orientările definite pentru a spori protecția on-line a copiilor. Diminuarea conținutului ilegal sau dăunător și conștientizarea în rândul copiilor și al altor factori interesați reprezintă principalele măsuri decisive care ar trebui dezvoltate în continuare.

11. AEPD dorește să reamintească faptul că o protecție adecvată a informațiilor cu caracter personal ale copilului reprezintă o etapă preliminară esențială pentru garantarea siguranței on-line. Această interdependență între confidențialitate și securitatea copiilor este exprimată explicit în recenta Declarație a comitetului miniștrilor privind „protejarea demnității, securității și confidențialității în cazul copiilor care utilizează internetul” ([3]). Declarația respectivă reamintește dreptul copiilor la demnitate, protecție specială și îngrijire, necesare bunăstării lor, dreptul la „protecția împotriva tuturor formelor de discriminare sau de amestec arbitrar sau ilegal care le afectează confidențialitatea, precum și împotriva atacurilor ilegale la adresa onoarei și reputației lor”.

12. Ca exemple de riscuri asociate protejării confidențialității copiilor, declarația menționează trasabilitatea activităților copiilor, care îi poate expune unor activități infracționale, precum solicitarea de favoruri sexuale, precum și altor activități ilegale. Stabilirea de profiluri și păstrarea datelor cu caracter personal legate de activitățile copiilor sunt la rândul lor prezentate ca antrenând un risc posibil de utilizare frauduloasă, de exemplu în scopuri comerciale sau pentru căutări efectuate de instituții de învățământ și potențiali angajatori. În consecință, declarația îndeamnă la eliminarea sau ștergerea, într-un termen rezonabil de limitat, a conținuturilor și a urmelor lăsate on-line de copii, precum și la dezvoltarea și promovarea informațiilor pentru copii, în special cu privire la utilizarea competentă a instrumentelor care permit accesul la informații, la dezvoltarea analizei critice a conținutului și dobândirea unor aptitudini de comunicare adecvate.

13. AEPD susține aceste concluzii. AEPD consideră esențială în special conștientizarea în rândul copiilor a riscurilor legate de comunicarea spontană a detaliilor cu caracter personal, precum numele real, vârsta sau reședința.

14. Punctul 3 al măsurilor ([4]) propuse de programul multianual este dedicat explicit „asigurării conștientizării la nivel public” prin acțiuni destinate direct copiilor, părinților, persoanelor care au grijă de copii și educatorilor, cu privire la oportunitățile și riscurile pe care le prezintă utilizarea tehnologiilor on-line și a „modalităților de garantare a siguranței on-line”. Printre modalitățile indicate în propunere, furnizarea de informații adecvate și punerea la dispoziție a unor puncte de contact unde părinții și copiii pot primi răspunsuri la întrebările referitoare la modalitatea de menținere a siguranței on-line reprezintă două instrumente utile, care ar trebui să integreze în mod explicit această dimensiune a protecției datelor cu caracter personal ale copiilor.

15. AEPD dorește să sublinieze faptul că autoritățile de protecție a datelor reprezintă interlocutori competenți în acest context. Acestea ar trebui menționate ca atare în propunere, în special acolo unde se prevede promovarea cooperării și schimburilor de informații, experiență și bune practici la nivel național și european ([5]).

([1]) Expunerea de motive a propunerii, 2.1. Contextul legislativ; Rezumat al evaluării impactului, 1.2. Situația actuală: legislația.

([2]) — Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic) (JO L 178, 17.7.2000, p. 1),
— 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 asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37),
— 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 (JO L 281, 23.11.1995, p. 31).

([3]) Declarație adoptată de către Comitetul de Miniștri la 20 februarie 2008, la cea de a 1018-a reuniune a delegaților miniștrilor, disponibilă la: „wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001”.

([4]) Acțiuni, punctul 3.

([5]) Anexa I, acțiuni, punctul 1.

16. Pot fi menționate câteva inițiative care ilustrează acțiunile recente întreprinse în acest sens în statele membre sau statele membre ale SEE. Autoritatea de protecție a datelor (APD) din Suedia realizează un studiu anual privind atitudinea tinerilor față de internet și supraveghere, la fel ca APD din Regatul Unit ([1]), care a realizat un studiu asupra a 2 000 de copii cu vârste cuprinse între 14 și 21 de ani. În ianuarie 2007, APD din Norvegia a lansat, împreună cu Ministerul Educației, o campanie de educare destinată școlilor ([2]). În Portugalia s-a semnat un protocol între APD și Ministerul Educației, în vederea promovării unei culturi de protecție a datelor pe internet, în special în cadrul rețelelor sociale ([3]). În urma acestui proiect, rețelele sociale portugheze au introdus o interfață și o mascotă destinată copiilor între 10 și 15 ani.

17. Aceste exemple ilustrează rolul activ și decisiv jucat de factorii implicați în protecția datelor pentru protecția copiilor în mediul on-line, precum și nevoia de includere explicită a acestora ca interlocutori în programul multianual.

III. PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI A DREPTURILOR CELORLALȚI FACTORI INTERESAȚI

I. *Raportare și schimb de informații*

18. Primul punct al propunerii [„Reducerea volumului de conținut ilegal și atacarea problemei comportamentului dăunător din mediul on-line” ([4])] include printre punctele principale crearea unor puncte de contact pentru semnalarea conținutului ilegal și a comportamentului dăunător on-line. Indubitabil, pentru a fi combătute eficient, conținutul ilegal sau comportamentul dăunător trebuie aduse în atenția autorităților competente. Au fost înființate deja puncte de contact pentru protecția copilului dar și, de exemplu, pentru combaterea programelor spam ([5]).

19. Cu toate acestea, AEPD constată că noțiunea de comportament dăunător rămâne neclară: nu se precizează cine este responsabil pentru definirea comportamentului dăunător și pe baza căror criterii se realizează aceasta. Acest lucru este extrem de îngrijorător având în vedere implicațiile unei posibile semnalări a acestor conținuturi.

20. De asemenea, după cum s-a precizat deja, în contextul unui program ca acesta, sunt în joc nu numai datele cu caracter personal ale copiilor, ci și ale tuturor persoanelor legate în vreun fel de circulația informațiilor pe internet. Poate fi vorba, de exemplu, de persoana suspectată de comportament inadecvat și semnalată ca suspect, dar și de persoana care semnalează un comportament sau un conținut suspicios, sau de victima abuzului. Deși informațiile sunt necesare pentru un sistem de raportare eficient, AEPD consideră că este important să se reamintească faptul că ele trebuie întotdeauna prelucrate în conformitate cu principiile de protecție a datelor.

21. Anumite date sensibile pot necesita chiar o protecție specială, dacă pot fi considerate ca atare în sensul articolului 8 din Directiva 95/46/CE. Poate fi cazul datelor privind autorii încălcărilor și victimele abuzurilor, mai ales când este vorba de pedopornografie. Trebuie menționat faptul că la nivel național, anumite sisteme de raportare au necesitat modificarea legislației de protecție a datelor, pentru a permite prelucrarea datelor judiciare ale infractorilor prezumați și ale victimelor prezumate ([6]). AEPD insistă asupra faptului că orice sistem de raportare care urmează a fi instituit trebuie să țină seama de cadrul de protecție a datelor existent. Manifestarea interesului public, precum și garanțiile legate de supravegherea sistemului, în principiu de către autoritățile de aplicare a legii sunt elemente decisive care trebuie respectate în acest cadru.

II. *Rolul instrumentelor tehnice din perspectiva confidențialității*

22. Folosirea instrumentelor tehnice este promovată ca una dintre soluțiile de combatere a conținutului ilegal și a comportamentului dăunător ([7]). Evaluarea impactului cuprinde exemple de astfel de instrumente ([8]), inclusiv tehnologiile de recunoaștere a vârstei, recunoaștere facială (pentru identificarea victimei de către autoritățile de aplicare a legii) sau filtrare. Propunerea afirmă că aceste instrumente ar trebui să fie mai bine adaptate necesităților practice și accesibile părților interesate relevante.

23. AEPD și-a exprimat deja poziția clară ([9]) în favoarea utilizării noilor tehnologii în scopul sporirii protecției drepturilor persoanelor. AEPD consideră că principiul „privacy by design” (respectarea prin concepție a confidențialității) ar trebui să fie inerentă a dezvoltării tehnologice care implică prelucrarea datelor cu caracter personal. În consecință, AEPD încurajează puternic dezvoltarea unor proiecte menite să dezvolte tehnologiile în acest sens.

24. Este importantă în special dezvoltarea unor sisteme care să reducă la minim expunerea datelor cu caracter personal ale copiilor, oferindu-le o protecție adecvată și dându-le în consecință posibilitatea de a folosi noile instrumente ale societății informaționale, precum rețelele sociale, într-un mod mai sigur.

([1]) A se vedea anexa I, www.ico.gov.uk/youngpeople
([2]) A se vedea: www.dubestemmer.no
([3]) A se vedea: dadus.cnpd.pt
([4]) Anexa 1 la propunere.
([5]) A se vedea, de exemplu, site-ul creat de autoritățile belgiene în acest scop, www.ecops.be
([6]) A se vedea articolul 3 alineatul (6) din Legea belgiană privind protecția datelor din 8 decembrie 1992, referitor la prelucrarea datelor de către Centrul de raportare a copiilor dispăruți sau victime ale abuzului sexual.
([7]) Anexa 1, acțiuni, punctul 1.
([8]) Evaluarea impactului, punctul 3.1.
([9]) Raportul anual al AEPD pentru anul 2006, partea 3.5.1. Evoluții tehnologice.

25. Cu toate acestea, ar trebui reamintit faptul că, în funcție de modul de utilizare, instrumentele tehnologice pot avea o varietate de impacturi asupra oamenilor. Când sunt folosite pentru filtrarea sau blocarea informațiilor, acestea pot împiedica accesul copiilor la informații potențial dăunătoare, dar pot bloca și accesul la informații legitime al unei persoane.

26. Deși principala preocupare în acest caz privește libertatea accesului la informații, mai apare o consecință din perspectiva confidențialității. Într-adevăr, filtrarea, în special în urma evoluțiilor recente care fac apel la gestionarea identității, poate funcționa pe baza unor criterii date, inclusiv a unor date cu caracter personal precum vârsta persoanei conectate în rețea (pentru a împiedica accesul adulților sau al copiilor la anumite conținuturi), a conținutului informațiilor și a datelor legate de trafic, corelate cu identitatea autorului informației. În funcție de modul de prelucrare — automată — a acestor informații cu caracter personal, persoanele implicate ar putea suferi consecințe legate de dreptul de a comunica on-line.

27. Recurgerea la instrumente de blocare sau de filtrare în vederea controlării accesului la rețele ar trebui, prin urmare, să se facă cu prudență, ținând seama de posibilul efect advers al acestora și cu valorificarea deplină a posibilităților de consolidare a confidențialității oferite de tehnologie.

28. AEDP salută precizia evaluării impactului ([1]), în care se afirmă că niciuna dintre opțiunile propuse nu ar trebui să afecteze dreptul la confidențialitate și nici libertatea de exprimare. De asemenea, AEPD împărtășește opinia exprimată în evaluarea impactului, potrivit căreia unul din obiectivele principale îl reprezintă responsabilizarea utilizatorului, respectiv „responsabilizarea în vederea luării unor decizii mai bune și a întreprinderii unor acțiuni adecvate" în vederea protejării copiilor ([2]).

III. *Responsabilitatea furnizorilor de servicii*

29. Propunerea consideră colaborarea cu factorii interesați ca fiind un element necesar pentru sporirea protecției copiilor care utilizează tehnologii de comunicare. Printre factorii interesați, propunerea ([3]) prevede participarea și implicarea sectorului în cauză, în special prin autoreglementare.

30. Fiind responsabilă de furnizarea serviciilor de telecomunicații și de servicii legate de conținut, industria acestui sector își poate exercita influența asupra raportării, filtrării sau blocării informațiilor considerate ilegale sau dăunătoare. Cu toate acestea, măsura în care i-ar putea fi încredințată cu adevărat o astfel de sarcină, din punct de vedere juridic, rămâne discutabilă.

31. Colaborarea industriei în vederea unei mai bune conștientizări în rândul copiilor și al altor factori interesați implicați, precum părinții sau educatorii, este desigur binevenită. Instalarea unor sisteme de alertare și existența moderatorilor pe site-urile web, care permit excluderea conținuturilor inadecvate, reprezintă un alt aspect esențial al responsabilității furnizorilor de conținut.

32. În ceea ce privește furnizorii de servicii de *telecomunicații*, monitorizarea telecomunicațiilor este o chestiune discutabilă, fiind legată de controlul conținutului protejat prin drepturi de proprietate intelectuală sau al altor conținuturi ilegale. Acest aspect ridică problema intervenției unui factor comercial, care oferă un serviciu (specific de telecomunicații), într-un domeniu în care, în principiu, acesta nu ar avea dreptul să intervină, respectiv controlul conținutului telecomunicațiilor. AEPD reamintește că, în principiu, acest control nu ar trebui exercitat de furnizorii de servicii și în niciun caz în mod sistematic. Atunci când devine necesar într-un context dat, acesta ar trebui, în principiu, să fie de competența autorităților de aplicare a legii.

33. În avizul său din 18 ianuarie 2005, Grupul de lucru pentru articolul 29 a reamintit, în legătură cu acest aspect ([4]), că „FSI-urilor nu le poate fi impusă obligația sistematică de supraveghere și colaborare în temeiul articolului 15 din Directiva 2000/31/CE privind comerțul electronic. (…) După cum se afirmă în articolul 8 din directiva privind protecția datelor, prelucrarea datelor referitoare la infracțiuni, condamnări penale sau măsuri de securitate se poate efectua numai în condiții stricte, puse în aplicare de statele membre. 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.".

34. Într-un domeniu în care sunt în joc libertatea de exprimare, accesul la informații, confidențialitatea și alte drepturi fundamentale, intervenția unor factori privați ridică întrebarea privind proporționalitatea măsurilor adoptate. Parlamentul European a adoptat recent o rezoluție în care subliniază nevoia unei soluții în conformitate cu drepturile fundamentale ale persoanelor ([5]). La punctul 23 al rezoluției, se afirmă că „internetul reprezintă o platformă vastă pentru expresia culturală, accesul la cunoștințe și participarea democratică la procesul de creație europeană, construind punți între generații cu ajutorul societății informaționale; [Parlamentul] invită astfel Comisia și statele membre să evite adoptarea de măsuri care contravin drepturilor omului și libertăților civile, principiilor proporționalității, eficacității și efectului de descurajare, precum întreruperea accesului la internet".

([1]) Evaluarea impactului, punctul 5.2.

([2]) În acest sens, filtrele ar trebui concepute astfel încât să fie inițializate de părinți și să poată fi dezactivate, astfel încât adultul să controleze integral efectul de filtrare.

([3]) Considerentul 8 din preambul; anexa 1, punctul 1.4.; rezumatul evaluării impactului, punctul 3.1.

([4]) Document de lucru al Grupului de lucru pentru articolul 29 privind aspecte de protecție a datelor aferente drepturilor de proprietate intelectuală, WP 104.

([5]) Rezoluția Parlamentului European din 10 aprilie 2008 privind industriile culturale din Europa [2007/2153(INI)], punctul 23.

35. AEPD consideră că trebuie să se ajungă la un echilibru între obiectivul legitim de combatere a conținutului ilegal și natura adecvată a mijloacelor utilizate. AEPD reamintește că orice acțiune de supraveghere a rețelelor de telecomunicații, necesară în anumite cazuri, ar trebui să fie de resortul autorităților de aplicare a legii.

IV. **CONCLUZIE**

36. AEPD susține propunerea privind programul multianual privind protecția copiilor care utilizează internetul și alte tehnologii de comunicare. AEPD salută faptul că programul intenționează să se axeze asupra unor noi tehnologii și a derulării unor acțiuni concrete pentru sporirea eficacității în protecția copiilor.

37. AEPD reamintește faptul că protecția datelor cu caracter personal este o premisă esențială a siguranței copiilor în mediul on-line. Trebuie împiedicată folosirea frauduloasă a informațiilor cu caracter personal ale copiilor, făcându-se apel la orientările menționate în program, în special:

— conștientizarea în rândul copiilor și al altor factori interesați, precum părinții și cadrele didactice,

— promovarea dezvoltării de cele mai bune practici de către sectorul în cauză,

— promovarea dezvoltării unor instrumente tehnologice care respectă confidențialitatea,

— favorizarea schimbului de bune practici și de experiențe practice între autoritățile competente, inclusiv cele de protecție a datelor.

38. Aceste acțiuni ar trebui dezvoltate fără a se pierde din vedere faptul că protecția copiilor se desfășoară într-un mediu care ar putea periclita drepturile celorlalți. Orice inițiativă de colectare, blocare sau raportare a informațiilor ar trebui adoptată numai cu respectarea drepturilor fundamentale ale tuturor persoanelor implicate și a cadrului legal de protecție a datelor. AEPD reamintește în special faptul că orice supraveghere a rețelelor de telecomunicații, necesară în anumite cazuri, ar trebui să fie de resortul autorităților de aplicare a legii.

39. AEPD constată că programul reprezintă un cadru general pentru viitoare acțiuni concrete. AEPD consideră că anumite observații din cuprinsul prezentului aviz sunt un prim pas și ar putea fi dezvoltate practic, cu referire la proiectele care urmează să fie demarate și în conformitate cu orientările programului. AEPD recomandă o implicare profundă a autorităților de protecție a datelor în definirea acestor proiecte practice. De asemenea, AEPD face trimitere la activitățile pe marginea acestui subiect ale Grupului de lucru pentru articolul 29, în special la activitatea curentă a Grupului de lucru cu privire la rețelele sociale ([1]).

Adoptat la Bruxelles, 23 iunie 2008.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

([1]) A se vedea documentul de lucru 1/2008 din 18 februarie cu privire la protecția datelor cu caracter personal ale copiilor, WP 147 și pentru o perspectivă mai generală, programul de lucru 2008-2009 al grupului de lucru care include rețele sociale, disponibil la: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm