CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition de décision du Parlement européen et du Conseil instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication

(2009/C 2/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [2], et notamment son article 41,

vu la demande d'avis formulée par la Commission européenne conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, reçue le 4 mars 2008,

A ADOPTÉ L'AVIS SUIVANT:

I. **INTRODUCTION**

Consultation du CEPD

1. Le 4 mars 2008, la Commission a soumis pour avis au CEPD la proposition de décision du Parlement européen et du Conseil instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication (ci-après dénommée «proposition»), conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Cette consultation devrait être explicitement mentionnée dans le préambule de la décision.

Contexte de la proposition

2. Le nouveau programme pluriannuel (ci-après dénommé «programme») est présenté dans le prolongement des programmes «Safer Internet» (1999-2004) et «Safer Internet plus» (2005-2008).

3. Il prévoit quatre lignes d'action:

   — réduire le volume de contenus illicites et s'attaquer aux comportements préjudiciables en ligne,

   — promouvoir un environnement en ligne plus sûr,

   — sensibiliser le public,

   — établir une base de connaissances.

4. Le programme est présenté comme étant cohérent et complémentaire par rapport aux politiques, programmes et actions communautaires pertinents. Compte tenu du nombre de mesures réglementaires existantes en matière de protection des enfants dans le cadre des nouvelles technologies, il privilégie l'action plutôt que la réglementation. L'accent est mis sur l'efficacité des initiatives à prendre et l'adaptation à l'évolution des nouvelles technologies. Dans cette optique, le programme prévoit le renforcement des échanges d'informations et de bonnes pratiques.

5. En tant qu'instrument cadre, le programme n'entre pas dans le détail des actions à prendre mais prévoit des appels à propositions et des appels d'offres dans le cadre des quatre lignes d'actions définies.

Éléments fondamentaux de l'avis du CEPD

6. Les lignes d'action générales du programme portent sur la protection des enfants qui utilisent l'internet et d'autres technologies de communication, sans s'attarder sur les aspects liés à la vie privée [3]. Tout en adhérant sans réserve à l'objectif de la proposition, le CEPD mettra en exergue les aspects précités dans le présent avis.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] Certaines références à la vie privée figurent dans l'analyse d'impact (3.2. Risques spécifiques: divulgation d'informations à caractère personnel; 3.3. Les groupes cibles; 5.2. Analyse de l'impact des options stratégiques), mais ces aspects ne sont pas développés en profondeur.

7. Le CEPD juge essentiel que les initiatives prévues soient compatibles avec le cadre juridique existant cité dans la proposition ([1]), en particulier la directive 2000/31/CE sur le commerce électronique, la directive 2002/58/CE «vie privée et communications électroniques» et la directive 95/46/CE relative à la protection des données ([2]).

8. Il convient de tenir compte de la protection des données à caractère personnel en ce qui concerne les différents aspects du programme et les différents acteurs qui y sont associés. La protection des données à caractère personnel des enfants constitue naturellement la principale préoccupation, mais elle n'est pas la seule: les données à caractère personnel liées à des personnes et à des contenus qui font l'objet d'un examen aux fins de la protection des enfants devraient également être prises en considération.

9. Ces questions seront développées comme suit dans le présent avis:

   — le chapitre II examinera le lien entre la protection des données et la sécurité des enfants, en se focalisant sur le fait que la protection des données relatives aux enfants est une mesure indispensable en vue d'une plus grande sécurité et de la prévention des abus,

   — au chapitre III, l'avis fera ressortir le fait que le traitement de données à caractère personnel est également inhérent au signalement, au filtrage et au blocage des contenus ou des personnes suspects sur l'internet:

      — au premier point, la question du signalement des personnes ou des faits suspects sera analysée sous l'angle de la protection des données,

      — le deuxième point s'attardera sur le rôle des outils techniques,

      — la responsabilité du secteur privé pour ce qui est du contrôle exercé sur les données des utilisateurs et sur le contenu des données fera l'objet du dernier point.

II. PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET SÉCURITÉ DES ENFANTS

10. Le CEPD approuve sans réserve l'objectif du programme et les lignes d'action définies pour améliorer la protection des enfants sur l'internet. En particulier, la réduction du volume de contenus illicites ou préjudiciables et la sensibilisation des enfants et des autres acteurs concernés sont des mesures décisives qu'il convient de développer.

11. Le CEPD souhaite rappeler qu'une protection appropriée des informations à caractère personnel relatives aux enfants constitue une première étape essentielle pour garantir la sécurité de ceux-ci lorsqu'ils naviguent sur l'internet. Ce lien entre vie privée et sécurité des enfants est mentionné explicitement dans la récente «Déclaration du Comité des ministres sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet» ([3]). Cette déclaration rappelle le droit des enfants à la «*dignité, à une protection et à une attention particulières nécessaires à leur bien-être, à une protection contre toutes formes de discrimination ou d'interférence arbitraire ou illicite dans leur vie privée et contre des attaques illégales à leur honneur et à leur réputation*».

12. Comme exemples de risques liés à la protection de la vie privée des enfants, la déclaration cite la traçabilité des activités des enfants, qui peut les exposer à des activités criminelles telles que des sollicitations à des fins sexuelles ou d'autres activités illégales. Elle considère également que les pratiques de profilage et la conservation des données à caractère personnel concernant les activités des enfants peuvent comporter des risques d'utilisation abusive, par exemple à des fins commerciales ou de recherche d'informations par des établissements d'enseignement ou des employeurs potentiels. La déclaration préconise dès lors le retrait ou la suppression, dans un délai raisonnablement court, des contenus et des traces laissés par les enfants sur l'internet, ainsi que le développement et la promotion de l'information des enfants, en particulier en ce qui concerne la maîtrise des outils d'accès àl'information, le développement de l'analyse critique des contenus qu'ils véhiculent et l'appropriation des compétences utiles en matière de communication.

13. Le CEPD souscrit à ces conclusions. Il considère notamment qu'il est essentiel de sensibiliser les enfants aux risques liés à la communication spontanée de coordonnées personnelles telles que le nom réel, l'âge ou le lieu de résidence.

14. Le points 3 des mesures ([4]) proposées dans le programme pluriannuel vise spécifiquement à «sensibiliser le public», par des actions ciblées sur les enfants, les parents, les gardiens et les éducateurs, aux possibilités et aux risques liés à l'utilisation de technologies en ligne et aux «moyens d'assurer la sécurité en ligne». Parmi les moyens cités dans la proposition, la diffusion d'informations appropriées et la mise à disposition de points de contact auprès desquels les parents et les enfants peuvent obtenir des réponses aux questions qu'ils se posent quant au moyen d'assurer la sécurité en ligne, constituent deux instruments utiles qui devraient tenir compte explicitement de cette dimension de la protection des données à caractère personnel des enfants.

15. Le CEPD souhaite souligner que les autorités chargées de la protection des données (DPA) sont des interlocuteurs appropriés dans ce contexte. Elles devraient être mentionnées en tant que telles dans la proposition, en particulier lorsque cette dernière prévoit la promotion de la coopération et du partage d'informations, d'expériences et de bonnes pratiques au niveau national et européen ([5]).

([1]) Exposé des motifs, 2.1. Contexte législatif; Résumé de l'analyse d'impact, 1.2. État de la situation: législation.

([2]) — directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») (JO L 178 du 17.7.2000, p. 1),
— directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37),
— directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

([3]) Déclaration adoptée par le Comité des Ministres le 20 février 2008, lors de la 1018ème réunion des Délégués des Ministres, disponible à l'adresse suivante: wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Ver=0001.

([4]) Actions, point 3.

([5]) Annexe I, Actions, point 1.

16. Plusieurs initiatives peuvent être citées pour illustrer les actions entreprises récemment à cet égard dans les États membres de l'UE ou de l'EEE. La DPA suédoise réalise une étude annuelle sur l'attitude des jeunes à l'égard de l'internet et la surveillance, tout comme la DPA du Royaume-Uni ([1]), qui a mené une enquête portant sur 2 000 enfants âgés de 14 à 21 ans. En janvier 2007, la DPA norvégienne a lancé, en collaboration avec le ministère de l'éducation, une campagne éducative à l'intention des écoles ([2]). Au Portugal, un protocole a été signé entre la DPA et le ministère de l'éducation en vue de promouvoir une culture de la protection des données sur l'internet et, en particulier, sur les réseaux sociaux ([3]). À la suite de ce projet, les réseaux sociaux portugais comportent désormais une interface et une mascotte destinées aux enfants âgés de 10 à 15 ans.

17. Ces exemples illustrent le rôle actif et décisif que jouent les acteurs de la protection des données lorsqu'il s'agit de la protection des enfants sur l'internet, ainsi que la nécessité de les inclure explicitement en tant qu'interlocuteurs dans le programme pluriannuel.

III. PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET DES DROITS DES AUTRES PARTIES PRENANTES

I. *Signalement et échange d'informations*

18. Parmi les principales actions détaillées au point 2 de la proposition («Lutter contre les contenus illicites et s'attaquer aux comportements préjudiciables en ligne» ([4])) figure la mise à la disposition du public de points de contact pour le signalement des contenus illicites et des comportements préjudiciables en ligne. Il ne fait aucun doute que si l'on veut que cette lutte soit efficace, il faut que les contenus illicites ou les comportements préjudiciables soient signalés aux services compétents. Des points de contact ont déjà été créés en ce qui concerne la protection des enfants, mais également, par exemple, dans le cadre de la lutte contre le spam ([5]).

19. Le CEPD constate néanmoins que la notion de «contenu illicite» reste imprécise: l'on ne sait pas qui est habilité à définir ce qu'est un contenu illicite, ni selon quels critères. Ceci est d'autant plus inquiétant que le signalement éventuel d'un tel contenu pourrait avoir des répercussions considérables.

20. En outre, comme on l'a souligné ci-dessus, dans le cadre d'un programme comme celui qui est à l'examen, les données à caractère personnel en jeu sont non seulement celles des enfants, mais aussi celles de l'ensemble des personnes liées d'une manière ou d'une autre aux informations circulant sur le réseau. Il peut s'agir, par exemple, des données de la personne soupçonnée de comportement préjudiciable et signalée comme suspecte, mais aussi de celles de la personne signalant un comportement ou un contenu suspect, ou de la victime. S'il est vrai que ces informations sont nécessaires pour que le système de signalement soit efficace, le CEPD considère qu'il importe de rappeler qu'elles devraient toujours être traitées conformément aux principes relatifs à la protection des données.

21. Certaines des données en question pourraient même nécessiter une protection particulière si elles devaient être considérées comme des données sensibles au sens de l'article 8 de la directive 95/46/CE. Tel pourrait être le cas des données relatives aux auteurs d'infractions ainsi qu'aux victimes d'abus, en particulier en ce qui concerne la pédopornographie. Soulignons qu'au niveau national, certains systèmes de signalement ont rendu nécessaire une modification de la législation sur la protection des données afin de permettre le traitement des données judiciaires d'auteurs présumés ou de victimes ([6]). Le CEPD insiste pour que tout système de signalement à mettre en place tienne compte du cadre existant en matière de protection des données. Afin que ce cadre soit respecté, il est essentiel de faire la preuve que le système présente une utilité publique et, également, qu'il y ait des garanties quant à son contrôle, qui doit être exercé en principe par les services répressifs.

II. *Le rôle des instruments techniques du point de vue de la vie privée*

22. L'utilisation d'instruments techniques est considérée comme l'une des solutions permettant de s'attaquer aux contenus illicites et aux comportements préjudiciables ([7]). L'analyse d'impact ([8]) comporte des exemples de ce type d'instruments, parmi lesquels figurent l'identification de l'âge, la reconnaissance des visages (pour que les services répressifs puissent identifier les victimes) ou les technologies de filtrage. Selon la proposition, ces instruments devraient être mieux adaptés aux besoins pratiques et être accessibles aux parties prenantes concernées.

23. Le CEPD a déjà pris clairement position ([9]) en faveur de l'utilisation des nouvelles technologies pour renforcer la protection des droits des personnes. Il estime que le principe de «privacy by design» (respect de la vie privée dès la conception) devrait faire partie intégrante de l'évolution technologique qui implique le traitement de données à caractère personnel. Le CEPD encourage dès lors résolument la mise en place de projets visant à développer les technologies dans ce sens.

24. Il importe en particulier de développer des systèmes qui permettront de faire en sorte que les données à caractère personnel des enfants soient dévoilées le moins possible en les protégeant de manière fiable, mais aussi de donner l'occasion aux enfants d'utiliser de manière plus sûre les nouveaux instruments de la société de l'information tels que les réseaux sociaux.

([1]) Voir Annexe I, «www.ico.gov.uk/youngpeople».
([2]) Voir «www.dubestemmer.no».
([3]) Voir «dadus.cnpd.pt/».
([4]) Annexe I de la proposition.
([5]) Voir, par exemple, le site internet créé par les autorités belges à cet effet: www.ecops.be.
([6]) Voir la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 3, paragraphe 6, qui concerne le traitement des données par le Centre européen pour enfants disparus et sexuellement exploités.
([7]) Annexe 1, actions, point 1.
([8]) Analyse d'impact, point 3.1.
([9]) Rapport annuel 2006 du CEPD, point 3.5.1 «Évolutions technologiques».

25. Il convient néanmoins de rappeler qu'en fonction de la manière dont ils sont utilisés, les instruments technologiques peuvent avoir des conséquences diverses pour les personnes. S'ils sont utilisés pour filtrer ou bloquer des informations, ils peuvent empêcher les enfants d'avoir accès à des contenus qui pourraient être préjudiciables, mais ils peuvent également empêcher une personne d'avoir accès à des informations légitimes.

26. Même si, en l'occurrence, la préoccupation principale concerne la liberté d'accéder à l'information, il y aura également des conséquences du point de vue de la vie privée. En effet, le filtrage, en particulier sous ses formes les plus récentes qui utilisent la gestion de l'identité, peut fonctionner sur la base de critères donnés, y compris des données à caractère personnel telles que l'âge de la personne connectée au réseau (afin d'éviter que des adultes ou des enfants aient accès à un contenu particulier), le contenu des informations et les données relatives au trafic liées à l'identité de l'auteur des informations. En fonction de la manière dont ces informations seront traitées (automatiquement), il pourrait y avoir, pour les personnes concernées, des conséquences sur leur droit à communiquer en ligne.

27. Il faut dès lors utiliser avec prudence les instruments de filtrage ou de blocage visant à contrôler l'accès aux réseaux, en tenant compte des effets pervers qu'ils pourraient avoir et en tirant pleinement parti des possibilités qu'offre la technologie pour renforcer le respect de la vie privée.

28. Le CEPD se félicite de la précision apportée dans l'analyse d'impact ([1]), selon laquelle aucune des options proposées ne devrait porter préjudice au droit au respect de la vie privée et à la liberté d'expression. Il partage également le point de vue selon lequel l'un des principaux objectifs est de responsabiliser l'utilisateur, et ce, pour qu'il pose de meilleurs choix et qu'il agisse de manière adéquate pour protéger les enfants ([2]).

III. *La responsabilité des fournisseurs de services*

29. Dans la proposition, la collaboration entre l'ensemble des parties prenantes est considérée comme un élément essentiel en vue de renforcer la protection des enfants qui utilisent les technologies de la communication. En ce qui concerne ces parties prenantes, la proposition ([3]) prévoit la participation des entreprises, en particulier par l'intermédiaire de l'autorégulation.

30. Responsables de la fourniture de services en matière de télécommunications et de contenu, ces entreprises pourraient avoir une certaine influence sur le signalement, le filtrage ou le blocage des informations lorsque celles-ci sont considérées comme illégales ou préjudiciables. Néanmoins, la mesure dans laquelle l'on peut, du point de vue juridique, leur confier une telle mission pourrait donner lieu à des divergences de vues.

31. Il va de soi que, dans une perspective de sensibilisation des enfants et des autres acteurs concernés, la collaboration des entreprises est la bienvenue. La mise en place, sur les sites internet, de systèmes d'alarme et de modérateurs afin d'exclure les contenus inappropriés constitue également un élément essentiel de la responsabilité des fournisseurs de contenu.

32. Pour ce qui est des fournisseurs de services de *télécommunications*, le contrôle des télécommunications, qu'il s'applique au contenu protégé par les droits de propriété intellectuelle ou à d'autres contenus illicites, constitue toutefois une question sujette à discussion. Ce problème soulève la question de l'intervention d'un acteur commercial, qui propose un service particulier (de télécommunications) dans un domaine où il n'est en principe pas censé intervenir, à savoir, le contrôle du contenu des télécommunications. Le CEPD rappelle qu'en principe, ce contrôle ne devrait pas être exercé par les fournisseurs de services, et certainement pas de manière systématique. Si ce contrôle s'avère nécessaire dans certaines circonstances particulières, il doit relever en principe des services répressifs.

33. Dans l'avis qu'il a rendu le 18 janvier 2005, le groupe «Article 29» a rappelé, à cet égard ([4]), qu'«aucune obligation systématique de surveillance et de collaboration ne peut être imposée aux fournisseurs d'accès, conformément à l'article 15 de la directive 2000/31/CE sur le commerce électronique. […] Comme indiqué à l'article 8 de la directive sur la protection des données, le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que dans des conditions strictes, telles que prévues par les États membres. Même si tout individu a naturellement le droit d'exploiter des données judiciaires dans le cadre de litiges le concernant, le principe ne va pas jusqu'à permettre l'examen approfondi, la collecte et la centralisation de données à caractère personnel par des tiers, y compris, notamment, la recherche systématique à grande échelle, comme le balayage d'Internet […]. De telles enquêtes sont de la compétence des autorités judiciaires».

34. Dans un domaine où la liberté d'expression, l'accès à l'information, le droit au respect de la vie privée et d'autres droits fondamentaux sont en jeu, cette intervention des acteurs privés soulève la question de la proportionnalité des moyens employés. Le Parlement européen a adopté récemment une résolution dans laquelle il souligne qu'il faut trouver une solution respectant les droits fondamentaux des personnes ([5]). Le point 23 de cette résolution dispose qu'«Internet est une vaste plate-forme pour l'expression culturelle, l'accès à la connaissance et la participation démocratique à la créativité européenne, créant des ponts entre générations dans la société de l'information; [le Parlement] engage la Commission et les États membres à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet».

([1]) Analyse d'impact, point 5.2.
([2]) À cet égard, les filtres devraient être placés par les parents et pourraient être désactivés afin que l'adulte garde pleinement le contrôle de l'effet de filtrage.
([3]) Considérant 8 du préambule; annexe 1, point 1. 4; résumé de l'analyse d'impact, point 3.1.
([4]) Document de travail du groupe «Article 29» sur les questions de protection des données liées aux droits de propriété intellectuelle, WP 104.
([5]) Résolution du Parlement européen du 10 avril 2008 sur les industries culturelles en Europe, (2007/2153(INI)), point 23.

35. Le CEPD estime qu'il convient de trouver un équilibre entre l'objectif, légitime, consistant à lutter contre les contenus illicites, et la nature des moyens employés, qui doit être adéquate. Il rappelle que toute action de surveillance des réseaux de télécommunications, si elle s'avère nécessaire dans des circonstances particulières, devrait relever de la compétence des services répressifs.

IV. **CONCLUSION**

36. Le CEPD soutient la proposition instituant un programme pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de la communication. Il note avec satisfaction que ce programme est axé sur le développement de nouvelles technologies et l'élaboration d'actions concrètes en vue de protéger plus efficacement les enfants.

37. Le CEPD rappelle que la protection des données à caractère personnel est une condition essentielle de la sécurité des enfants lorsqu'ils utilisent l'internet. Il faut éviter que les informations personnelles des enfants soient utilisées à mauvais escient, et ce, en suivant les lignes directrices proposées dans le programme, en particulier les suivantes:

   — sensibiliser les enfants et les autres parties prenantes telles que les parents et les éducateurs,

   — encourager l'élaboration de meilleurs pratiques par les entreprises,

   — encourager le développement d'instruments technologiques respectueux de la vie privée,

   — favoriser l'échange de bonnes pratiques et de connaissances pratiques entre les services concernés, et notamment ceux qui sont chargés de la protection des données.

38. Il convient de mettre ces actions en œuvre sans oublier que la protection des enfants se fait dans un environnement où les droits d'autres personnes peuvent être en jeu. Toute initiative en matière de collecte, de blocage ou de signalement d'informations devrait respecter les droits fondamentaux des personnes concernées et être conforme au cadre législatif concernant la protection des données. Le CEPD rappelle en particulier que la surveillance des réseaux de télécommunications, si elle s'avère nécessaire dans des circonstances particulières, devrait relever de la compétence des services répressifs.

39. Le CEPD note que le programme à l'examen constitue un cadre général dans lequel s'inscriront de nouvelles actions concrètes. Il considère que certaines des observations formulées dans le présent avis sont un premier pas et pourraient être développées en pratique, en fonction des projets qui doivent encore être mis en place conformément aux lignes directrices du programme. Il recommande que les services chargés de la protection des données soient étroitement associés à la conception de ces projets concrets. Il renvoie également aux activités du groupe «Article 29» sur le sujet, et en particulier au travail que ce groupe consacre actuellement aux réseaux sociaux ([1]).

Fait à Bruxelles, le 23 juin 2008.

Peter HUSTINX

Contrôleur européen de la protection des données

([1]) Voir le document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant, WP 147, et, pour un aperçu plus général, le programme de travail 2008-2009 du groupe de travail, notamment en ce qui concerne les réseaux sociaux, qui est disponible à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_fr.htm.