

Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI

(2010/C 323/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

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,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 29 mars 2010, la Commission a adopté une proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI ⁽³⁾ (ci-après la proposition).
2. La proposition vise à abroger une décision-cadre adoptée le 22 décembre 2003, au motif que celle-ci présente un certain nombre de lacunes. Le nouveau texte améliorerait la lutte contre les abus concernant des enfants sous les aspects suivants: érection en infractions pénales des formes graves d'abus concernant des enfants, comme le tourisme sexuel impliquant des enfants; protection des enfants non accompagnés; enquêtes pénales et coordination des poursuites pénales; nouvelles infractions pénales dans l'environnement des technologies de l'information; protection des victimes; prévention des infractions.
3. En ce qui concerne la prévention des infractions, cet objectif serait notamment réalisé par la limitation de l'accès à la pédopornographie sur l'internet.
4. Le Contrôleur européen de la protection des données (CEPD) a pris acte du principal objectif de la proposition.

Il n'entend pas remettre en cause la nécessité de mettre en place un meilleur cadre prévoyant des mesures adéquates pour protéger les enfants contre les abus. Il tient toutefois à mettre en évidence l'incidence de certaines des mesures envisagées dans la proposition, notamment le blocage de sites web et la mise en place de lignes directes, sur les droits fondamentaux au respect de la vie privée et à la protection des données des différentes personnes concernées. C'est pourquoi il a décidé d'émettre ce bref avis de sa propre initiative.

II. ANALYSE DE LA PROPOSITION

5. Deux aspects de la proposition, qui ne sont pas spécifiques à la lutte contre les abus concernant des enfants mais à toute initiative visant la collaboration du secteur privé à des fins de répression, soulèvent des questions en matière de protection des données. Le CEPD a déjà analysé ces questions dans différents contextes, en particulier dans le cadre de la lutte contre les contenus illicites sur l'internet ⁽⁴⁾.
6. Pour ce qui est de la proposition, les deux éléments préoccupants sont énoncés au considérant 13 et à l'article 21. Ils peuvent être décrits comme suit:
 - II.1. Le rôle des fournisseurs d'accès à l'internet dans le blocage de sites web**
7. La proposition envisage deux solutions possibles pour bloquer l'accès, depuis le territoire de l'Union, aux pages internet dont il a été établi qu'elles contenaient ou diffusaient des contenus pédopornographiques: soit des systèmes permettant aux autorités judiciaires ou policières compétentes d'ordonner un tel blocage, soit le blocage volontaire par les fournisseurs d'accès sur la base de codes de bonne conduite ou de lignes directrices.
8. Le CEPD s'interroge sur les critères et les conditions devant donner lieu à une décision de blocage: alors qu'il pourrait approuver les mesures prises par les autorités judiciaires ou policières dans un cadre juridique bien défini, il a des doutes sérieux quant à la sécurité juridique d'un blocage opéré par des parties privées.

⁽⁴⁾ En particulier, le CEPD a émis les avis suivants, qui comportent des observations pertinentes au regard de la présente initiative:

— avis du 23 juin 2008 sur la proposition de décision instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication (JO C 2 du 7.1.2009, p. 2),
 — avis du 22 février 2010 sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC).

Voir également le document de travail du groupe de travail «Article 29» sur les questions de protection des données liées aux droits de propriété intellectuelle (document de travail n° 104 adopté le 18 janvier 2005).

⁽¹⁾ JO L 281 du 23.11.1995, p. 31.

⁽²⁾ JO L 8 du 12.1.2001, p. 1.

⁽³⁾ COM(2010) 94 final.

9. Le CEPD s'interroge surtout sur les types de contrôle de l'internet susceptibles de conduire à un tel blocage. Cela peut en effet supposer différentes activités, notamment l'exploration de l'internet, le recensement des sites web illicites ou suspects et le blocage de l'accès des utilisateurs finaux, mais aussi le contrôle du comportement en ligne des utilisateurs qui cherchent à accéder à ce type de contenus ou à les télécharger. Si les instruments utilisés sont différents et supposent différents degrés d'intrusion, ils soulèvent des questions similaires quant au rôle des fournisseurs d'accès à l'internet en ce qui concerne le traitement des informations.
10. Ces activités de surveillance ne sont pas sans conséquences sur le plan de la protection des données, puisqu'elles supposent le traitement des données à caractère personnel de différents types de personnes, qu'il s'agisse de victimes, de témoins, d'utilisateurs ou de fournisseurs de contenus. Le CEPD a exprimé dans de précédents avis ses préoccupations concernant la surveillance des individus par des acteurs du secteur privé (fournisseurs d'accès à l'internet ou titulaires de droits d'auteur) dans des domaines qui relèvent en principe de la compétence des autorités répressives ⁽¹⁾.

— Le CEPD souligne que la surveillance du réseau et le blocage de sites constitueraient une finalité sans rapport avec les préoccupations d'ordre commercial des fournisseurs d'accès à l'internet: cela soulèverait des questions quant au caractère licite et compatible du traitement des données à caractère personnel au regard de l'article 6, paragraphe 1, point b), et de l'article 7 de la directive relative à la protection des données ⁽²⁾.

— Le CEPD s'interroge sur les critères de blocage et souligne qu'un code de conduite ou des lignes directrices volontaires ne garantiraient pas un niveau suffisant de sécurité juridique à cet égard.

— Le CEPD insiste également sur les risques que présente l'éventuel établissement d'une «liste noire» de personnes et sur les possibilités de recours devant une instance indépendante.

11. Le CEPD a déjà fait observer à plusieurs reprises que «la surveillance des comportements des internautes et la collecte de leur adresse IP équivalent à une interférence dans leur droit au respect de la vie privée et de leur correspondance (...). Ce point de vue est en adéquation avec la jurisprudence de la Cour européenne des droits de l'homme ⁽³⁾». Compte tenu de cette interférence, des dispositions plus appropriées sont nécessaires pour garantir que la surveillance ou le blocage ne seront exercés que de

manière strictement ciblée et sous contrôle judiciaire, et que des mesures de sécurité appropriées empêchent toute utilisation abusive de ce mécanisme.

II.2. La mise en place d'un réseau de lignes directes

12. Le réseau de lignes directes mentionné au considérant 13 de la proposition est prévu par le programme pour un internet plus sûr, concernant lequel le CEPD a émis l'avis évoqué ci-dessus. L'une des observations du CEPD concerne précisément les conditions selon lesquelles les informations seraient collectées, centralisées et échangées: il est nécessaire de définir précisément la notion de contenu illicite ou préjudiciable, les personnes habilitées à collecter et conserver des informations, ainsi que les conditions dans lesquelles elles y sont autorisées.
13. Cela est particulièrement important compte tenu des conséquences d'un signalement: 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, par exemple les informations concernant une personne soupçonnée de comportement préjudiciable, qu'il s'agisse d'un internaute ou d'un fournisseur de contenus, mais aussi celles concernant une personne signalant un contenu suspect ou la victime de l'abus. Il importe de ne pas perdre de vue les droits de toutes ces personnes lors de l'élaboration de procédures de signalement: leurs droits doivent être pris en compte conformément au cadre existant en matière de protection des données.
14. Par ailleurs, les informations recueillies par les lignes directes seront très probablement utilisées à des fins de poursuites judiciaires. S'agissant des exigences de qualité et d'intégrité, il conviendrait de mettre en œuvre des mesures supplémentaires afin de garantir que ces informations, considérées comme des preuves numériques, ont été dûment recueillies et conservées et qu'elles seront donc recevables en justice.
15. Les garanties liées à la supervision du système, qui doit en principe être assurée par les autorités répressives, sont des éléments incontournables. La transparence et la mise à disposition de possibilités de recours devant une instance indépendante sont d'autres éléments essentiels à intégrer dans un tel mécanisme.

III. CONCLUSION

16. Bien qu'il n'y ait pas lieu de s'opposer à la mise en place d'un cadre solide et efficace pour lutter contre l'exploitation et les abus sexuels concernant des enfants et la pédopornographie, le CEPD insiste sur la nécessité de garantir la sécurité juridique en ce qui concerne toutes les parties concernées, y compris les fournisseurs d'accès à l'internet et les personnes utilisant le réseau.

⁽¹⁾ Voir les deux avis du CEPD mentionnés précédemment.

⁽²⁾ 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⁾ Avis du CEPD sur l'ACAC, p. 6.

17. Le CEDP se réjouit que la proposition mentionne la nécessité de prendre en compte les droits fondamentaux des utilisateurs finaux mais estime que cela n'est pas suffisant. Il conviendrait d'y ajouter l'obligation pour les États membres de veiller à la mise en place de procédures harmonisées, claires et détaillées dans le cadre de la lutte contre les contenus illicites, et ce sous la supervision d'autorités publiques indépendantes.

Fait à Bruxelles, le 10 mai 2010.

Peter HUSTINX

Contrôleur européen de la protection des données
