



Avis du Contrôleur européen de la protection des données

sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – «Stratégie européenne pour un Internet mieux adapté aux enfants»

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 ses articles 7 et 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 données¹,

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 données², et notamment son article 41, paragraphe 2,

A ADOPTÉ L'AVIS SUIVANT

I. INTRODUCTION

I.1. Consultation du CEPD

1. Le 2 mai 2012, la Commission a publié sa communication sur une «Stratégie européenne pour un Internet mieux adapté aux enfants»³ (ci-après la «communication»).
2. Avant l'adoption de cette communication, le CEPD a eu l'opportunité de formuler des commentaires informels. Le CEPD est satisfait de constater que certains de ses commentaires ont été pris en considération dans la communication. Compte tenu de l'importance du sujet, le CEPD souhaite néanmoins soumettre le présent avis de sa propre initiative.

¹ JO L 281 du 23.11.1995, p. 31.

² JO L 8 du 12.1.2001, p. 1.

³ COM (2012) 196 final.

I.2. Objectifs et contexte de la communication

3. L'objectif de la communication est de développer une stratégie visant à améliorer la protection des enfants en ligne. La communication est placée dans le contexte du Programme de l'Union européenne en matière de droits de l'enfant,⁴ de la Stratégie numérique pour l'Europe,⁵ et des conclusions du Conseil sur la protection des enfants dans le monde numérique.⁶
4. La communication est axée sur quatre grands piliers:
 - (1) promouvoir du contenu en ligne de qualité destiné aux jeunes;
 - (2) sensibiliser et responsabiliser davantage;
 - (3) créer un environnement en ligne sûr pour les enfants; et
 - (4) lutter contre les abus sexuels sur mineur et l'exploitation sexuelle des enfants.
5. La communication ébauche un certain nombre de mesures qui doivent être prises par les entreprises, les États membres et la Commission, respectivement. Elle couvre des questions telles que le contrôle parental, les paramètres de confidentialité, la classification en fonction de l'âge, les outils de signalement, les lignes d'urgence et les organes coercitifs.

I.3. Objectifs et portée de l'avis du CEPD

6. Le CEPD soutient pleinement les initiatives visant à renforcer la protection des enfants sur Internet et à améliorer les moyens de lutter contre les abus sur les enfants en ligne⁷. Dans deux avis précédents, le CEPD a souligné l'importance de la protection et de la sécurité des enfants en ligne d'un point de vue de la protection des données⁸. Le CEPD est satisfait de constater que cela a été reconnu dans la communication.
7. L'utilisation croissante de l'environnement numérique par les enfants et l'évolution constante de cet environnement posent de nouveaux risques en matière de protection de données et de protection de la vie privée, qui sont exposés au point 1.2.3 de la communication. Parmi ces risques citons, entre autres, l'utilisation abusive des données personnelles, la diffusion non désirée de leur profil personnel sur les sites de réseaux sociaux, l'utilisation croissante

⁴ Programme de l'Union européenne en matière de droits de l'enfant, COM(2011) 60 final.

⁵ Une Stratégie numérique pour l'Europe, COM(2010) 245 final.

⁶ Conclusions du Conseil sur la protection des enfants dans le monde numérique, 3128^e session du Conseil Éducation, jeunesse, culture et sport, Bruxelles, les 28 et 29 novembre 2011.

⁷ Il existe également un certain nombre d'initiatives au niveau international telles que la Stratégie du Conseil de l'Europe sur les droits de l'enfant (2012-2015), CM(2011)171 final, 15 février 2012.

⁸ Voir 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, publié au JO C2, 7.01.2009, p. 2, et l'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, publié au JO C 323, 30.11.2010, p. 6.

de services de géolocalisation, l'exposition directe et croissante à la publicité et à des crimes sérieux tels que les abus d'enfants. Ce sont là des risques particuliers qui doivent être abordés de manière adaptée à la spécificité et à la vulnérabilité de la catégorie des individus concernés.

8. Le CEPD est satisfait de constater que les mesures envisagées dans la communication sont tenues de respecter le cadre actuel de la protection des données (notamment la directive 95/46/CE et la directive 2002/58/CE⁹ sur la vie privée et les communications électroniques), la directive 2000/31/CE sur le commerce électronique¹⁰ et la Charte des droits fondamentaux de l'UE, et que la communication tient également compte du nouveau cadre proposé relatif à la protection des données¹¹. Le CEPD souligne que toutes les mesures déployées ultérieurement à la communication doivent être conformes à ce cadre.
9. Le présent avis souligne les questions spécifiques relatives à la protection des données soulevées par les mesures prévues dans la communication, qui doivent être dûment abordées par tous les destinataires pertinents de la communication, à savoir la Commission, les États membres et les entreprises, le cas échéant. Plus particulièrement, le chapitre II met en exergue les moyens spécifiques pouvant aider à améliorer la protection et la sécurité des enfants en ligne du point de vue de la protection des données. Au chapitre III, l'avis expose certains problèmes relatifs à la protection des données qui doivent être abordés pour la mise en œuvre des mesures visant à lutter contre les abus sexuels sur mineur et l'exploitation sexuelle des enfants sur Internet, en particulier en ce qui concerne l'utilisation des outils de signalement et la coopération entre les entreprises, les organes coercitifs et les lignes d'urgence.

II. LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DES ENFANTS SUR L'INTERNET

II.1. La reconnaissance de droits renforcés à la protection des données pour les enfants en ligne

10. L'utilisation de l'Internet par les enfants soulève des problèmes spécifiques en matière de protection des données. Sur Internet, les enfants sont plus vulnérables que d'autres groupes d'utilisateurs puisqu'ils sont encore moins bien équipés que d'autres pour comprendre pleinement la valeur des données qu'ils divulguent et les dangers associés à cette divulgation. Les jeunes enfants peuvent ne pas réaliser les conséquences de leurs actions, ou ne pas savoir gérer leurs paramètres de confidentialité. Il peut s'avérer difficile pour eux de

⁹ 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, JO L 201, 31/07/2002, p. 37-47.

¹⁰ Directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques du commerce électronique dans le marché intérieur, JO 178 L, 17/07/2000, p. 1-16.

¹¹ Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final.

comprendre que les services web peuvent être conçus de façon à inciter les enfants à divulguer des données à caractère personnel (les coordonnées par exemple) à un public plus large que prévu, avec des conséquences assez vastes en termes d'utilisation abusive de leurs données personnelles, depuis le ciblage comportemental, jusqu'à la cyber-intimidation et l'exploitation sexuelle.

11. D'un point de vue juridique, les enfants sont considérés comme une catégorie spécifique d'individus qui mérite une protection particulière et renforcée. Des droits spécifiques ont été accordés aux enfants dans de nombreuses chartes et conventions internationales¹², notamment en leur reconnaissant un droit à la protection de la vie privée¹³. D'un point de vue de la protection des données, la législation européenne ne stipule aucun régime spécifique pour les enfants; les enfants bénéficient de la protection générale garantie dans la directive 95/46/CE relative à la protection des données. Toutefois, les autorités de protection des données en Europe ont reconnu les besoins spécifiques de ce groupe d'individus et ont appelé au respect de leurs droits à la protection de la vie privée et à la protection des données d'une manière adaptée à leur niveau de maturité et de compréhension, et dans l'intérêt supérieur de l'enfant¹⁴.
12. En outre, dans la proposition de règlement général en matière de protection des données, les enfants bénéficieraient d'une reconnaissance spécifique. L'article 4, paragraphe 18, définit expressément un enfant comme une personne de moins de 18 ans. Le règlement proposé prévoit des mesures spécifiques pour garantir une protection adéquate des données de l'enfant. Ces mesures exigent que les responsables du traitement fournissent des informations et communiquent dans un langage facilement compréhensible par un enfant, qu'ils respectent des conditions spécifiques pour le traitement des données des enfants, qu'ils mettent en place des formulaires spéciaux pour obtenir l'autorisation pour le traitement des données, qu'ils leur accordent un «droit à l'oubli» en ligne, et qu'ils les protègent contre le profilage¹⁵. Le CEPD a salué ces mesures dans son avis sur le paquet de mesures pour une réforme de la protection des données¹⁶.
13. Dans l'UE, la mesure dans laquelle les enfants peuvent agir valablement en leur nom, et sans le consentement parental, eu égard au traitement de leurs données personnelles, est souvent liée à leur capacité d'agir en justice en vertu du droit civil ou pénal. L'âge à partir duquel les enfants peuvent agir valablement sur l'Internet varie en fonction des États membres. Dans une

¹² Voir entre autres la déclaration universelle des droits de l'homme, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, et la Charte des droits fondamentaux de l'Union européenne.

¹³ Par exemple, l'article 16 de la Convention des NU relative aux droits de l'enfant.

¹⁴ Voir avis 2/2009 du groupe de travail «Article 29» sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particuliers des écoles), 11 février 2009, WP 160, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_fr.pdf.

¹⁵ Voir, entre autres, les considérants 29, 38, 46 et l'article 6, paragraphe 1, point f), l'article 6, paragraphe 5, l'article 8, l'article 11, paragraphe 2, l'article 17, l'article 33, paragraphe 2, point d), l'article 38, paragraphe 1, point e), et l'article 52, paragraphe 2.

¹⁶ Avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012, JO C 137, 12.05.2012, p. 1.

certaine mesure, cela a été une source d'insécurité juridique pour les organisations ciblant les enfants sur l'Internet. Ces organisations n'étaient pas sûres des exigences concernant le traitement des données à caractère personnel relatives aux enfants. Le règlement sur la protection des données proposé a abordé la question de l'âge en précisant que le traitement des données personnelles des enfants en-dessous de 13 ans dans le contexte des services de la société de l'information ne serait licite que dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par une personne qui en a la garde. A contrario, les enfants de plus de 13 ans seraient en mesure de prendre des décisions relatives au traitement de leurs données à caractère personnel.

14. La communication a totalement intégré l'importance de donner aux enfants des moyens spécifiques et efficaces de protéger leurs données à caractère personnel en ligne, adaptés à leur groupe d'âge. Plus particulièrement, elle prévoit un certain nombre d'actions que les entreprises peuvent mettre en œuvre pour fournir aux enfants des paramètres de confidentialité par défaut adaptés à l'âge et des informations appropriées avant qu'ils ne changent ces paramètres, pour reconnaître les besoins spécifiques de ce groupe d'individus lorsqu'ils font de la publicité en ligne à leur intention, et permettre aux enfants de signaler un contenu ou une conduite préjudiciable.
15. Ce chapitre de l'avis met l'accent sur les piliers 2 et 3 de la communication (comme mentionné au point 4 ci-dessus), qui envisagent des mesures particulièrement pertinentes pour améliorer la protection des données à caractère personnel et de la vie privée des enfants. Ces mesures visent à habiliter davantage les enfants tout en préservant dans le même temps leur sécurité lors de l'utilisation de l'Internet. Elles comprennent la sensibilisation, le déploiement d'un outil de signalement à l'échelle de l'UE pour les enfants, le développement d'outils techniques pour garantir la sécurité et le respect de la vie privée, et l'accès à des informations claires sur la manière d'assurer que leurs données sont protégées. Le CEPD analyse ces mesures ci-après et formule des suggestions pour améliorer ces initiatives d'un point de vue de la protection des données. L'outil de signalement pour enfants est analysé avec d'autres outils de signalement au chapitre III.

II.2. Sensibilisation

16. Le CEPD salue les initiatives présentées aux sections 2.2.1 et 2.2.2 de la communication visant à développer les activités de sensibilisation. Sensibiliser davantage les enfants aux risques auxquels ils peuvent être exposés en ligne ainsi qu'aux moyens qu'ils peuvent utiliser pour se protéger est particulièrement important pour améliorer leur protection et sécurité en ligne. Le CEPD souligne que puisque la protection des données est un composant essentiel de la sécurité d'un enfant en ligne, des mesures visant à sensibiliser davantage les individus sur la «sécurité en ligne» devraient également inclure des informations sur les risques et droits en matière de protection de la vie privée et des données.
17. Par exemple, la divulgation de données à caractère personnel par des enfants sur les sites de réseaux sociaux est un problème qui peut avoir des

conséquences à long terme pour eux, puisque ces données peuvent être consultables pour une durée indéterminée et peuvent laisser des «traces» tout au long de leur vie d'adulte. Cela peut également avoir des conséquences pour d'autres, par exemple lorsque des commentaires ou photographies sont publiés sur d'autres individus. Ce risque particulier a incité la Commission à suggérer le renforcement du «droit à l'oubli numérique» dans le règlement sur la protection des données¹⁷. Ce droit permettrait aux individus de demander à tout moment au fournisseur d'accès du site web où les données à caractère personnel ont été rendues publiques de les effacer et de cesser de les diffuser. Toutefois, en pratique, la suppression ou la rectification des informations qui ont été mises en ligne peut s'avérer problématique et ne doit pas être considérée comme une solution remplaçant les mesures préventives: les campagnes de sensibilisation seraient très utiles pour sensibiliser les enfants aux dangers, pour eux et pour autrui, posés par la divulgation de données à caractère personnel (sur eux-mêmes ou sur d'autres) sur Internet, et pour leur permettre de faire preuve de diligence dans leurs interactions avec d'autres et lorsqu'ils divulguent des informations sur l'Internet. Il serait donc particulièrement utile pour les États membres d'inclure des informations et matériaux sur les risques relatifs à la protection des données dans leurs programmes scolaires ainsi que des informations sur la manière dont les enfants peuvent éviter ces risques en agissant avec précaution et diligence, et sur la manière de remédier à ces risques en utilisant des outils techniques ou en exerçant leurs droits.

18. En outre, le rôle des autorités nationales de protection des données est également important dans le contexte de l'échange de bonnes pratiques de protection des données en rapport avec les campagnes de sensibilisation. Les autorités de protection des données en Europe ont soutenu la mise en place d'initiatives conjointes en matière de sensibilisation et d'éducation des plus jeunes.¹⁸ Par exemple, le «Safer Internet Day»¹⁹, qui est célébré chaque année en février, a été l'occasion de présenter les campagnes et concours impliquant des enfants partout en Europe. Des projets spécifiques ont été développés par les autorités nationales de protection des données ou en collaboration avec elles dans plusieurs États membres de l'UE, tels que le Portugal²⁰, la République tchèque²¹ et la France²², ainsi que dans les pays de l'EEE tels que la Norvège²³. Le CEPD souligne donc que le développement de synergies entre les autorités de protection des données, les gouvernements nationaux, la Commission et les entreprises sera bénéfique pour promouvoir la sensibilisation en matière de sécurité en ligne pour les enfants.

¹⁷ Article 17 du règlement proposé, COM(2012) 11 final.

¹⁸ Voir résolution adoptée à Prague les 29-30 avril 2010 lors de la Conférence des commissaires européens à la protection des données et à la vie privée, disponible à l'adresse: <http://www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=690>.

¹⁹ <http://www.saferinternet.org/web/guest/safer-internet-day>.

²⁰ <http://dadus.cnpd.pt/>.

²¹ <http://www.uoou.cz/uoou.aspx?loc=661>.

²² <http://www.internetsanscrainte.fr/>.

²³ «You decide»: <http://www.teknologiradet.no/FullStory.aspx?m=3&amid=4736>.

II.3. Paramètres de confidentialité adaptés à l'âge

19. Le CEPD salue l'initiative mentionnée à la section 2.3.1 de la communication concernant la mise en œuvre par les entreprises de moyens techniques pour améliorer la protection de la vie privée des enfants en ligne, plus particulièrement le développement et la mise en œuvre de paramètres de confidentialité par défaut adaptés à l'âge. Intégrer des paramètres de confidentialité par défaut va de pair avec le principe de respect de la vie privée dès la conception, qui vise à considérer la protection de la vie privée et la protection des données dès les premières étapes de la conception de l'outil de traitement. Le respect de la vie privée dès la conception et l'utilisation de technologies renforçant le respect de la vie privée ont toujours été encouragés par les autorités de protection des données, en particulier en ce qui concerne les activités de traitement ciblant les enfants.
20. Une première considération importante pour les fournisseurs de services en ligne est de vérifier et de délimiter la mesure dans laquelle les enfants peuvent participer à certaines activités en ligne, en particulier sur les sites des réseaux sociaux. En mai 2010²⁴, le groupe de travail «Article 29» a appelé les acteurs privés ayant signé les «Principes de l'UE pour des réseaux sociaux plus sûrs» rédigés par la Commission²⁵ à prêter davantage attention aux questions liées aux mineurs, et notamment aux conditions visant à obtenir le consentement de leurs parents avant qu'ils puissent s'engager dans des activités en ligne. Comme mentionné précédemment, la proposition de règlement sur la protection des données exigerait le consentement parental pour les enfants de moins de 13 ans. Actuellement, cependant, il n'y a pas d'harmonisation de l'âge auquel le consentement parental est requis, et ce consentement doit par conséquent être obtenu conformément aux exigences nationales applicables.
21. Le CEPD salue le fait que des paramètres de confidentialité par défaut spécifiques doivent être mis en œuvre en fonction de l'âge de l'enfant. S'il considère que le niveau de protection le plus élevé soit requis pour les plus jeunes, le CEPD souligne toutefois que des paramètres de confidentialité doivent être établis par défaut pour toutes les tranches d'âge, et pas seulement pour les plus jeunes. Le groupe de travail «Article 29» a souligné que des paramètres par défaut de base doivent être définis sur les sites des réseaux sociaux pour tous les utilisateurs, qu'ils soient enfants ou adultes²⁶. À cet égard, les paramètres de confidentialité par défaut pour les enfants doivent prévoir des mécanismes plus protecteurs que ceux qui doivent être intégrés

²⁴ http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010-others_en.htm.

²⁵ «Principes de l'UE pour des réseaux sociaux plus sûrs», 10 février 2009: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

²⁶ Voir l'avis 5/2009 du groupe de travail «Article 29» sur les réseaux sociaux en ligne, p. 7: «seule une minorité des utilisateurs modifie les paramètres par défaut en s'inscrivant à ce genre de service. Les SRS devraient donc mettre en place des paramètres par défaut respectueux de la vie privée, qui permettent aux utilisateurs d'accepter librement et spécifiquement que des personnes autres que leurs contacts choisis accèdent à leur profil, afin de réduire le risque d'un traitement non autorisé. Les profils à accès limité ne devraient pas être repérables par les moteurs de recherche internes, y compris par la fonction de recherche par paramètres tels que l'âge ou le lieu. Les décisions d'extension de l'accès ne doivent pas être implicites, par exemple avec un «opt out» fourni par le responsable du SRS».

pour tous les utilisateurs. Par exemple, il serait particulièrement opportun d'avoir des paramètres spécifiques appliqués sur les sites de réseaux sociaux en ligne utilisés par des enfants, tels qu'un outil vérifiant l'âge des amis avant qu'un enfant puisse les accepter, conjugué à des paramètres prévoyant une vérification supplémentaire par les parents ou les tuteurs légaux des enfants, leur permettant de valider l'acceptation d'amis adultes.

Changement des paramètres par défaut

22. Le CEPD est également satisfait de constater que les entreprises sont encouragées à fournir des informations et avertissements clairs aux enfants sur les conséquences potentielles de tout changement apporté aux paramètres de confidentialité par défaut. Pour que ces avertissements soient utiles, il convient de préciser clairement au mineur quel pourrait être l'impact d'un changement des paramètres de confidentialité sur sa vie privée ainsi que le préjudice potentiel qu'il pourrait subir. Il serait utile que les entreprises développent une taxonomie pour expliquer en termes simples ces préjudices potentiels (par exemple en expliquant quels sont les préjudices potentiels du fait d'être identifié, profilé, de recevoir des cookies, etc.).
23. La mesure dans laquelle un enfant peut changer les paramètres de confidentialité par défaut devrait également être liée à l'âge et au niveau de maturité de l'enfant. Il convient d'examiner dans quelle mesure, et au sein de quel groupe d'âge, le consentement parental serait requis pour valider un changement des paramètres de confidentialité.

Vérification de l'âge

24. L'application de ces paramètres par défaut reste problématique en raison de la difficulté pour les fournisseurs de services de déterminer avec une certitude suffisante que les individus utilisant leur site web appartiennent à une tranche d'âge spécifique. Il existe plusieurs approches pour vérifier l'âge des utilisateurs, avec des avantages et inconvénients concernant l'exactitude et l'ampleur de la collecte de données. La manière la moins intrusive de déterminer l'âge des individus se fait par les informations volontairement communiquées. Toutefois, les informations volontairement communiquées peuvent ne pas être fiables. D'autres modèles, tels que l'identification complète de l'individu ou des systèmes conçus pour déduire l'âge de l'individu à partir de son comportement, entendent résoudre ce problème mais peuvent impliquer un niveau disproportionné de collecte et de traitement de données. Bien que des systèmes automatiques déduisant l'âge d'un utilisateur à partir de son comportement aient été suggérés par des chercheurs, ces systèmes d'analyse comportementale sont à la merci d'une fausse identification de l'âge de l'utilisateur, en particulier lorsqu'il s'agit d'enfants, puisque ceux-ci présentent différents niveaux de maturité et un large éventail de comportements à mesure qu'ils grandissent et qu'ils se développent. Le CEPD a noté dans son avis sur le paquet de mesures pour une réforme de la protection des données que les outils de vérification de l'âge exigeront que des

garanties spécifiques soient prises afin que seules les données nécessaires soient collectées et conservées.²⁷

25. À cet égard, le CEPD salue les efforts de la Commission visant à aborder la vérification de l'âge dans un cadre juridique futur de l'UE sur l'authentification électronique, de façon à ce que les opérateurs de site web soient en mesure de vérifier si les personnes actives sur leur site sont des mineurs et, dans ce cas, d'activer les paramètres par défaut nécessaires. Le 4 juin 2012, la Commission a présenté une proposition pour un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur²⁸, qui énonce les principes et modalités des systèmes d'authentification électroniques. Le CEPD insiste pour que ce cadre juridique proposé soit totalement conforme aux exigences de la protection des données et, plus particulièrement, qu'il n'implique pas le traitement de données à caractère personnel dépassant ce qui est strictement nécessaire aux fins de l'authentification. Ce cadre pourrait préciser, par exemple, la tranche d'âge d'une personne devant être certifiée par un tiers, sans qu'aucune donnée sur la personne ne soit transmise au fournisseur du site web. Le CEPD émettra un avis sur le règlement proposé sur l'identification électronique et les services de confiance, pour analyser plus en profondeur les aspects relatifs à la protection des données qui doivent être considérés dans ce cadre.

II.4. Fournir aux enfants des informations claires sur le traitement de leurs données pour leur permettre de prendre des décisions informées

26. La communication recommande que les entreprises mettent en œuvre des «informations contextuelles» sur le «niveau de confidentialité» de chaque élément requis ou suggéré pour créer un profil en ligne. La communication ne définit cependant pas ce que signifient les «informations contextuelles sur le niveau de confidentialité de chaque élément». Cela peut être compris comme exigeant que les fournisseurs de services informent les enfants concernant le niveau de sensibilité de chaque information qu'ils fournissent au moment de créer un profil en ligne. Cela peut également exiger de les informer des risques ou préjudices potentiels qu'ils peuvent rencontrer lorsqu'ils divulguent ces informations à un nombre de personnes restreint, plus important ou indéterminé. Comme indiqué ci-dessus au point 22, il pourrait s'avérer utile pour les entreprises de développer une taxonomie commune sur la manière de décrire le niveau de sensibilité de chaque information.
27. Ces informations contextuelles sont les bienvenues parce qu'elles peuvent sensibiliser davantage les individus à la protection des données au point de collecte. Le CEPD, cependant, insiste pour qu'elles soient considérées comme un complément et non pas un substitut à la politique relative à la protection de la vie privée qui peut être consultée par les utilisateurs lorsqu'ils souhaitent examiner la politique relative à la protection de la vie privée du fournisseur de services dans sa globalité. Les fournisseurs de services qui agissent en tant que responsables du traitement ont l'obligation en vertu de la législation sur la

²⁷ Voir note de bas de page 16, paragraphe 321.

²⁸ COM(2012) 238 final.

protection des données, et plus particulièrement au titre de l'article 10 de la directive 95/46/CE, de fournir aux utilisateurs des informations détaillées sur le traitement de leurs données, en décrivant les activités de traitement qu'ils peuvent réaliser avec ces données (par exemple utiliser ces données ultérieurement pour le profilage, l'extraction de données, etc.), ainsi que sur les droits des individus et sur la manière dont ils peuvent les exercer. En outre, les fournisseurs de services agissant en tant que responsables du traitement doivent garantir qu'ils respectent d'autres exigences relatives à la protection des données. Dans le règlement général sur la protection des données proposé, ils seront tenus pour «responsables» du respect de la législation sur la protection des données.

II.5. La publicité destinée aux enfants

28. La section 2.3.4 de la communication décrit les mesures à prendre pour mieux protéger les enfants de la publicité et des dépenses excessives. Le CEPD salue l'initiative relative à la publicité en ligne destinée aux enfants, qui exige que les entreprises respectent la loi en matière de profilage en ligne et qu'elles mettent en œuvre des mesures de manière proactive pour éviter l'exposition des enfants à de la publicité inappropriée, quel que soit le média en ligne.
29. Le traitement des données à caractère personnel des enfants dans le contexte de la publicité soulève deux questions d'un point de vue de la protection des données: il convient de vérifier d'abord si le traitement de leurs données est légitime au regard de la finalité, et lorsque cela est le cas, il convient d'assurer que des garanties adéquates ont été fournies, ou qu'un consentement valide a été obtenu pour ce traitement.
30. Dans un premier temps, la légitimité de la publicité destinée aux enfants en tant que telle peut être remise en question. Compte tenu de la vulnérabilité des enfants, la collecte de leurs données personnelles à des fins de publicité directe pourrait les exposer au risque d'être influencés de manière excessive par ces publicités. Certaines autorités de protection des données ont clairement précisé que toute collecte à des fins de marketing de données relatives à des mineurs qui n'ont pas atteint la maturité nécessaire doit être considérée comme non légitime²⁹. En outre, la collecte via un mineur de données concernant les habitudes de son entourage apparaît également déloyale et illicite³⁰. En conséquence, le groupe de travail «Article 29» a particulièrement insisté sur le fait qu'il ne devrait pas y avoir de marketing direct spécifiquement destiné aux mineurs³¹ et que les données ne devraient pas être collectées auprès d'enfants

²⁹ Voir l'avis 38/2002 de l'Autorité belge de la protection des données relatif à la protection de la vie privée des mineurs sur Internet, p. 5: «*De façon générale, toute collecte à des fins de marketing de données relatives à des mineurs qui n'ont pas atteint l'âge de discernement doit ainsi être considérée comme non légitime. Il apparaît également déloyal et illicite de collecter via un mineur des données concernant son entourage, telles que les centres d'intérêts ou les habitudes de consommation des membres de sa famille. Il en va de même pour toute collecte de données qui serait effectuée par le truchement d'un jeu ou d'un cadeau.*». Cet avis est disponible à l'adresse: http://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002.pdf.

³⁰ Voir l'avis de l'Autorité belge de la protection des données référencé dans la note de bas de page 26.

³¹ Voir l'avis 5/2009 du groupe de travail «Article 29» sur les réseaux sociaux en ligne, 12 juin 2009, p. 12, disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_fr.pdf.

dans l'intention de diffuser des publicités comportementales ou de les influencer (comme par exemple, la collecte de données sur leurs centres d'intérêts)³². Le Parlement européen a formulé la même demande³³. Le CEPD salue le fait que la communication ait spécifiquement abordé la question de la publicité comportementale destinée aux enfants en recommandant au secteur qu'«aucun segment de marché ne soit créé pour cibler les enfants». En d'autres termes, seul le traitement de données à des fins de publicité plus innocente ou destinée à des tranches d'âge plus élevées pourrait être considéré comme étant légitime, sauf si la personne concernée s'y est opposée³⁴ ou sous réserve d'autres restrictions.³⁵ Cette recommandation nécessite une grande vigilance et de l'autodiscipline de la part des entreprises.

31. En outre, la mesure dans laquelle les enfants peuvent donner leur consentement de manière valable à la publicité est liée aux exigences légales en vigueur en matière d'obtention du consentement des enfants, qui peut nécessiter l'accord de la part d'un parent ou d'un représentant légal (comme décrit au point 13 ci-dessus). L'obtention d'un consentement valide exige également que les prescriptions en matière de protection des données prévues par la loi soient respectées, notamment que le consentement soit une manifestation de volonté libre, spécifique et informée de la part de la personne concernée, au sens de l'article 2, point h), de la directive 95/46/CE³⁶.
32. Le CEPD note que la communication de la Commission invite les entreprises à s'appuyer sur des tentatives d'autorégulation, telles que le code de bonnes pratiques de l'AEEP en matière de publicité comportementale en ligne³⁷. Il rappelle toutefois que le groupe de travail «Article 29» a constaté que le respect de l'approche actuelle encouragée par ce code ne permettait pas d'être en conformité avec la législation européenne en matière de protection des données³⁸. Le CEPD estime que la Commission devrait encourager davantage les entreprises du secteur à élaborer des mesures d'autorégulation respectueuses de la vie privée à l'échelle européenne, en encourageant les bonnes pratiques en matière de publicité en ligne destinée aux enfants, qui devraient se fonder sur le respect total des législations applicables.

³² Voir l'avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne, 22 juin 2010, disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf.

³³ Résolution du Parlement européen du 15 décembre 2010 sur l'effet de la publicité sur le comportement des consommateurs, disponible à

l'adresse : <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0484+0+DOC+XML+V0//FR>

³⁴ Article 14, point b), deuxième alinéa, de la directive 95/46/CE et article 19, paragraphe 2 de la proposition de règlement général sur la protection des données qui prévoient un droit spécifique d'opposition au traitement de données à caractère personnel à des fins de marketing direct.

³⁵ Voir par ex. l'article 8 de la Directive 95/46/CE sur les données sensibles et l'article 13 de la directive 2002/58/CE (vie privée et communications électroniques) relatif aux communications non sollicitées.

³⁶ Voir également l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement, disponible à l'adresse: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf.

³⁷ <http://www.easa-alliance.org/page.aspx/2>.

³⁸ Voir l'avis 16/2011 du groupe de travail «Article 29» sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne à l'adresse: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_fr.pdf.

33. À cet égard, le CEPD salue le fait que la Commission confirme sa détermination à envisager une législation plus poussée si les mesures d'autorégulation s'avéraient inefficaces. La nécessité d'appliquer un niveau renforcé de protection des enfants pourrait exiger de prendre des mesures législatives supplémentaires à l'échelle européenne pour garantir le respect des droits des enfants en matière de vie privée et de protection des données dans le contexte de la publicité.

III. PROTECTION DES DONNÉES DANS LE CADRE DE LA LUTTE CONTRE LES ABUS SEXUELS ET L'EXPLOITATION SEXUELLE DES ENFANTS

III.1. L'utilisation d'outils de signalement

34. L'Internet a facilité la diffusion auprès du grand public de contenus illicites relatifs aux abus sexuels et à l'exploitation sexuelle des enfants. En outre, à mesure que les enfants sont de plus en plus actifs sur Internet, les risques d'établir des contacts préjudiciables ou d'être exposés à du contenu préjudiciable sont d'autant plus importants.
35. Une des façons dont les politiques de l'UE se sont attaquées au problème du contenu illicite sur Internet a été de mettre en place, ou d'exiger des entreprises du secteur, qu'elles mettent en place, des outils permettant aux internautes, et à tout un chacun, de signaler du contenu illicite sur Internet (par ex., signalements effectués par les utilisateurs sur des sites Internet, politiques de notification et de retrait, numéros d'urgence comme le réseau de numéros d'urgence INHOPE³⁹)⁴⁰.
36. Cette communication vise à améliorer la visibilité et l'efficacité de ces outils de signalement. En outre, la section 2.2.3 de la communication encourage les entreprises à instaurer et à déployer à l'échelle de l'UE un outil de signalement permettant aux enfants qui utilisent leurs services et leurs outils en ligne de signaler un contenu ou une conduite préjudiciable.
37. Le CEPD salue le fait que la communication indique clairement que les initiatives prévues pour renforcer la notification et le retrait d'un contenu pornographique doivent respecter les dispositions de la directive 2011/92/UE⁴¹ relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, de la directive sur le commerce électronique, de la législation sur la protection des données et la Charte des droits fondamentaux de l'UE.

³⁹ L'association internationale des lignes directes Internet. Elle a adopté un code de bonnes pratiques le 12 mai 2010 disponible à l'adresse:

http://www.inhope.org/Libraries/Best_Practice_Papers/Code_of_Practice_updated_2010.sflb.ashx.

⁴⁰ La Commission a mis en évidence quelques-uns des principes applicables en rapport avec les outils de signalement sur les réseaux sociaux dans le document «Principes de l'UE pour des réseaux sociaux plus sûrs, 10 février 2009, disponible à l'adresse:

http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

⁴¹ Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *JO L 335, 17.12.2011, p. 1-14*.

38. En revanche, le CEPD note que bien que les mécanismes de signalement à concevoir dans le contexte de la directive 2011/92/UE bénéficient d'un minimum d'harmonisation (en particulier au niveau des définitions des infractions et des modalités de signalement), il n'existe pas de base juridique ni de définitions claires sur ce qui pourrait être signalé, dans le contexte de l'outil de signalement à l'échelle de l'UE pour les enfants prévu dans la section 2.2.3, concernant «tout contenu ou contact qui semble préjudiciable». Dès lors, le CEPD recommande que l'utilisation de l'outil de signalement à l'échelle de l'UE pour les enfants soit clairement énoncée dans la loi.
39. Le respect des exigences en matière de protection des données est particulièrement important dans le cadre de l'utilisation d'outils de signalement puisque ces signalements pourraient contenir non seulement les données personnelles de l'enfant ou de la personne ayant effectué le signalement, mais aussi celles de la personne soupçonnée et des victimes éventuelles. En outre, les données traitées par le biais de ces outils de signalement pourraient être sensibles, comme le définit l'article 8 de la directive 95/46/CE (par exemple, les données relatives aux suspicions d'activités illégales, les données sur la vie sexuelle, etc.). Ces données peuvent être traitées uniquement dans des conditions strictes. Le CEPD salue le fait que la communication souligne que ces signalements doivent être traités conformément à la législation en vigueur en matière de protection des données.
40. La conformité avec le principe de proportionnalité du traitement effectué par le biais de cet outil de signalement doit être garantie. À cet égard, il convient de saluer la recommandation formulée par la Commission aux entreprises d'élaborer un modèle normalisé de signalement minimum «avec des types de signalement clairs et ne donnant pas lieu à interprétation» dans le cadre de l'outil de signalement à l'échelle de l'UE pour les enfants. D'un point de vue de la protection des données, une bonne pratique serait d'ajouter dans le modèle de signalement des types d'infraction et/ou de préjudice prédéfinis à cocher et de limiter les questions et les commentaires dans les champs libres. Ce genre de modèle devrait être conçu de manière à limiter le traitement de données personnelles uniquement à celles qui s'avèrent strictement nécessaires.
41. L'élaboration d'un modèle de signalement commun pour d'autres outils de signalement, et pas uniquement ceux destinés spécifiquement aux enfants, s'avérerait également utile. Par exemple, il n'existe pas de procédure harmonisée commune pour le traitement des signalements soumis via les lignes d'urgence. En outre, il existe un large éventail de politiques de protection de la vie privée, plutôt qu'une approche commune. Dans certains cas, les signalements peuvent être effectués de manière anonyme, tandis que dans d'autres, les informations personnelles et les coordonnées sont indispensables. En cas de transfert de données à caractère personnel, les normes en matière de protection des données ne sont peut-être pas identiques à celles en vigueur au moment où les informations ont été envoyées, et il peut être plus difficile en pratique pour les personnes concernées d'exercer leurs droits en matière de protection des données s'ils ne savent pas où leurs

données sont traitées. Par conséquent, le traitement de données à caractère personnel dans le cadre des signalements effectués via des lignes d'urgence représente un domaine supplémentaire qui pourrait fortement bénéficier d'une coopération plus étroite à l'échelle européenne vers un code de bonnes pratiques établissant des procédures de signalement plus claires, à l'image des normes exigeantes en matière de protection des données.

42. Enfin, le CEPD souligne qu'il serait très utile pour les entreprises du secteur de faire appel aux autorités nationales chargées de la protection des données dans le cadre de l'élaboration de ces outils de signalement pour promouvoir la conception d'outils de signalement efficaces et respectueux des normes en matière de protection des données.

III.2. Coopération entre les entreprises, les lignes d'urgence et les organes coercitifs

43. La communication prévoit une coopération étroite entre les entreprises, les lignes d'urgence et les organes coercitifs pour un retrait plus efficace du contenu pédopornographique d'Internet. Toutefois, le manque de clarté entourant la portée et les modalités de la coopération entre les fournisseurs de services et les organes coercitifs demeure particulièrement préoccupant. Il conviendrait de veiller à ce que les modalités de cette coopération soient suffisamment définies dans un instrument juridique, qui fournirait également les garanties nécessaires en matière de protection des données.
44. Le CEPD rappelle que la mesure dans laquelle les fournisseurs de services de télécommunications et de contenu peuvent être chargés de signaler et de bloquer du contenu considéré comme illicite ou préjudiciable reste discutable⁴². Le CEPD souligne que les activités de traitement des données entourant l'enquête, le signalement et la poursuite des abus sexuels sur enfants sur Internet sont particulièrement intrusives d'un point de vue de la protection des données et peuvent être uniquement menées conformément à une base juridique solide.
45. Même si la coopération avec les organes coercitifs est couverte dans une certaine mesure par la directive sur le commerce électronique et les législations nationales, d'autres formes de coopération, comme par exemple la coopération avec le futur Centre européen de la cybercriminalité⁴³, ne font pas l'objet d'une base sûre suffisante à l'heure actuelle.⁴⁴
46. Il est indispensable de clarifier avec une certitude juridique suffisante les modalités de la coopération entre les entreprises, les lignes d'urgence et les

⁴² Voir avis du CEPD référencé dans la note de bas de page 8.

⁴³ Le futur Centre européen de la cybercriminalité est une initiative proposée dans la communication par la Commission européenne au Conseil et au Parlement européen prévoyant l'établissement d'un Centre européen de lutte contre la cybercriminalité, COM(2012) 140 final.

⁴⁴ Il existe également un manque de clarté au niveau des modalités de la coopération entre le Centre européen de la cybercriminalité, d'une part, et les organismes privés, d'autre part. Voir l'avis du CEPD du 29 juin 2012 sur la communication de la Commission européenne au Conseil et au Parlement européen sur la mise en place d'un Centre européen de la cybercriminalité, disponible à l'adresse www.edps.europa.eu.

organes coercitifs en ce qui concerne les procédures de notification et de retrait du contenu pédopornographique sur Internet. À cet égard, le CEPD salue l'initiative annoncée par la Commission européenne concernant une mesure horizontale sur les mécanismes de notification et de retrait, qui permettrait d'obtenir davantage de clarifications sur le rôle des différents intervenants et les modalités de leurs actions, au sein du cadre juridique en vigueur.

47. Le CEPD insiste sur le fait que cette coopération doit pleinement respecter la législation européenne, et en particulier la directive sur le commerce électronique et la Charte fondamentale des droits fondamentaux de l'UE⁴⁵. Le CEPD estime qu'il convient de trouver un juste équilibre entre l'objectif légitime consistant à lutter contre le contenu illicite et la nature appropriée des moyens utilisés. Il rappelle que ces tâches impliquent la surveillance des télécommunications, ce qui en principe ne devrait pas être effectué par les fournisseurs de services et certainement pas de manière systématique. Lorsque cela s'avère nécessaire et dans le cadre de circonstances bien spécifiques, cette tâche devrait en principe être l'apanage des organes coercitifs.
48. À l'échelle internationale, le CEPD soutient les efforts de la Commission en vue de définir une approche mondiale qui permettrait d'aborder ces problèmes sur une base plus coordonnée et durable. Le CEPD souligne que l'élargissement de la portée du réseau de lignes d'urgence INHOPE dans les pays en dehors de l'UE nécessitera d'offrir des garanties appropriées au regard de la protection des données pour les échanges de données à caractère personnel effectués entre eux, conformément aux articles 25 et 26 de la directive 95/46/CE.

IV. CONCLUSION

49. Le CEPD soutient les initiatives de la communication en vue de rendre l'Internet plus sûr pour les enfants, et de lutter contre les abus sexuels sur mineurs et l'exploitation sexuelle des enfants. Plus particulièrement, il salue la reconnaissance de la protection des données comme un élément clé pour assurer la protection des enfants sur l'Internet et pour les habiliter à profiter de ses avantages en toute sécurité.
50. Le CEPD insiste pour que les exigences en matière de protection des données soient correctement prises en compte par les entreprises, les États membres et la Commission au moment de mettre en œuvre des initiatives visant à améliorer la sécurité en ligne des enfants, plus particulièrement:
 - les États membres doivent veiller à inclure dans leurs campagnes et matériaux didactiques des références aux risques posés à la protection des données ainsi que des informations sur la manière dont les enfants et les parents peuvent les éviter. Les synergies entre les autorités chargées de la

⁴⁵ La Cour a souligné les limites de la coopération des fournisseurs de services Internet dans l'affaire C-70/10, *Scarlet Extended SA contre la Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, arrêt du 24 novembre 2011, et dans l'affaire C-360/10, *la Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) contre Netlog NV*, arrêt du 16 février 2012.

protection des données et les entreprises doivent également être développées afin de sensibiliser enfants et parents à la sécurité en ligne;

- les entreprises doivent veiller à traiter les données à caractère personnel des enfants conformément à la législation en vigueur, et à obtenir le consentement parental lorsque nécessaire. Elles doivent mettre en œuvre des paramètres de confidentialité par défaut pour les enfants qui fournissent des mécanismes plus proactifs que ceux configurés par défaut pour tous les utilisateurs. Elles doivent également mettre en œuvre des avertissements appropriés pour alerter les enfants qui veulent changer leurs paramètres de confidentialité par défaut et veiller à ce qu'un tel changement soit validé par un consentement parental lorsque nécessaire. Elles doivent s'efforcer de déployer des outils appropriés pour la vérification de l'âge qui ne soient pas intrusifs du point de vue de la protection des données;
- s'agissant des informations communiquées aux enfants, les entreprises doivent examiner comment développer une taxonomie pour fournir des informations aux enfants de manière simple et les informer des risques potentiels d'un changement de leurs paramètres de confidentialité par défaut;
- en ce qui concerne la publicité destinée aux enfants, le CEPD rappelle qu'aucune campagne de marketing direct ne peut cibler spécifiquement les mineurs et que les enfants ne peuvent faire l'objet d'une publicité comportementale. Le CEPD considère que la Commission devrait encourager davantage les entreprises à développer des mesures d'autorégulation respectueuses de la vie privée au niveau de l'UE, en promouvant des bonnes pratiques eu égard à la publicité en ligne destinée aux enfants, qui doivent être totalement conformes à la législation relative à la protection des données. Il encourage également la Commission à examiner la possibilité de légiférer davantage au niveau de l'UE pour garantir que les droits à la protection de la vie privée et à la protection des données à caractère personnel soient pris en compte comme il se doit dans le contexte de la publicité.

51. Les initiatives présentées dans la communication eu égard à la lutte contre les abus sexuels sur mineurs et l'exploitation sexuelle des enfants soulèvent un certain nombre de questions sur la protection des données, qui doivent être minutieusement considérées par toutes les parties prenantes dans leur domaine d'action respectif:

- en raison de leur sensibilité du point de vue de la protection des données, le déploiement des outils de signalement devrait se fonder sur une base juridique appropriée. Le CEPD recommande que le déploiement de l'outil de signalement pour les enfants à l'échelle de l'UE, prévu à la section 2.2.3, soit clairement énoncé dans la loi. Il conseille en outre de clairement définir ce que constitue un «contenu ou une conduite préjudiciable» pouvant être signalé par le biais du futur outil de signalement pour enfants à l'échelle de l'UE;

- le CEPD encourage les entreprises à développer des modèles normalisés de signalement minimum, qui doivent être conçus de manière à limiter le traitement des données à caractère personnel uniquement aux données strictement nécessaires;
- les procédures de signalement par le biais de lignes d'urgence pourraient être mieux définies. Un code européen de bonnes pratiques, comprenant des procédures de signalement communes et des garanties de protection des données, y compris en ce qui concerne les échanges internationaux de données à caractère personnel, devrait améliorer la protection des données dans ce domaine;
- afin d'assurer le développement d'outils de signalement garantissant un niveau élevé de protection des données, les autorités chargées de la protection des données doivent engager un dialogue constructif avec les entreprises et les autres parties prenantes;
- la coopération entre les entreprises et les organismes coercitifs en ce qui concerne les procédures de notification et de retrait du matériel pédopornographique diffusé sur Internet ne doit se faire que conformément à une base juridique appropriée. Les modalités d'une telle coopération doivent être définies plus clairement. C'est également le cas en ce qui concerne la coopération entre les entreprises et le futur Centre européen de la cybercriminalité;
- le CEPD estime qu'il faut trouver un juste équilibre entre l'objectif légitime de lutter contre le contenu illégal et la nature appropriée des moyens utilisés. Il rappelle que toute action de surveillance des réseaux de télécommunications, qui peut s'avérer nécessaire dans des cas spécifiques, est une tâche réservée aux organes coercitifs.

Fait à Bruxelles, le 17 juillet 2012

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données