I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE 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»)

(2008/C 181/01)

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 la 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 ([2]),

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, et notamment son article 41 ([3]),

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, reçue le 16 novembre 2007,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 13 novembre 2007, la Commission a adopté une proposition de directive modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après dénommée «la proposition» ou «les modifications proposées»). La version actuelle de la directive 2002/58/CE est généralement, et ce sera le cas également dans le présent avis, désignée par les termes suivants: directive «vie privée et communications électroniques».

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

2. La proposition vise à renforcer la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques, non pas en transformant entièrement la directive «vie privée et communications électroniques» actuelle, mais plutôt en proposant d'y apporter des modifications appropriées, destinées essentiellement à renforcer les dispositions liées à la sécurité et à améliorer les mécanismes coercitifs.

3. Cette proposition s'inscrit dans une réforme plus large des cinq directives de l'UE sur les télécommunications («le paquet Telecom»). Outre les propositions de réexamen du «paquet Telecom» ([1]), la Commission a simultanément adopté une proposition de règlement instituant une Autorité européenne du marché des communications électroniques ([2]).

4. Les observations figurant dans le présent avis sont limitées aux modifications qu'il est proposé d'apporter à la directive «vie privée et communications électroniques», sauf lorsque les modifications proposées reposent sur des notions ou des dispositions figurant dans les propositions de réexamen du paquet Telecom. Par ailleurs, certaines observations figurant dans le présent avis portent sur des dispositions de la directive «vie privée et communications électroniques» qui ne sont pas modifiées par la proposition.

5. Le présent avis traite des questions suivantes: *i)* le champ d'application de la directive «vie privée et communications électroniques», en particulier les services concernés (proposition de modification de l'article 3, paragraphe 1); *ii)* la notification des violations de la sécurité (modification proposée créant les paragraphes 3 et 4 de l'article 4); *iii)* les dispositions relatives aux témoins de connexion («cookies»), logiciels espions et dispositifs analogues (proposition de modification de l'article 5, paragraphe 3); *iv)* les actions en justice engagées par des fournisseurs de services de communications électroniques et d'autres personnes morales (modification proposée créant, à l'article 13, un paragraphe 6) et *v)* le renforcement des dispositions relatives au contrôle de l'application (modification proposée créant l'article 15 *bis*).

Consultation du CEPD et consultation publique plus large

6. La Commission a adressé la proposition au CEPD le 16 novembre 2007. Le CEPD interprète cette communication comme une demande d'avis à formuler à l'intention des institutions et organes communautaires, comme le prévoit l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 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 (ci-après dénommé «règlement (CE) n° 45/2001»).

7. Préalablement à l'adoption de la proposition, la Commission a consulté le CEPD de façon informelle sur le projet de proposition, ce dont le CEPD s'est félicité puisque cela lui a donné la possibilité de formuler certaines suggestions sur le projet de proposition avant son adoption par la Commission. Le CEPD constate avec satisfaction que la proposition tient compte de certaines de ses suggestions.

8. L'adoption de la proposition a été précédée d'une consultation publique de grande envergure, une pratique appréciée par le CEPD. De fait la Commission a lancé, en juin 2006, une consultation publique sur sa communication concernant le réexamen du «paquet Telecom» et a, dans ce cadre, exposé son point de vue sur la situation et présenté certaines propositions de modifications ([3]). Le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (ci-après dénommé «Groupe de l'article 29»), dont le CEPD fait partie, a profité de cette occasion pour donner son point de vue sur les modifications proposées, dans un avis adopté le 26 septembre 2006 ([4]).

([1]) Les modifications qu'il est proposé d'apporter aux directives sur les télécommunications sont présentées dans les propositions suivantes: *i)* proposition de directive du Parlement européen et du Conseil modifiant la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, la directive 2002/19/CE relative à l'accès aux réseaux et services de communications électroniques ainsi qu'à leur interconnexion, et la directive 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, 13.11.2007, doc. COM (2007) 697 final; *ii)* proposition de directive du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs, 13.11.2007, doc. COM(2007) 698 final.

([2]) Proposition de règlement du Parlement européen et du Conseil instituant une Autorité européenne du marché des communications électroniques, 13.11.2007, doc. COM(2007) 699 final.

([3]) Communication concernant le cadre réglementaire de l'UE pour les réseaux et services de communications électroniques (doc. SEC(2006) 816) adoptée le 29 juin 2006. Cette communication était complétée par un document de travail des services de la Commission [doc. COM (2006) 334 final].

([4]) Avis 8/2006 concernant le réexamen du cadre réglementaire pour les réseaux et services de communications électroniques, axé sur la directive sur la protection de la vie privée dans le secteur des communications électroniques, adopté le 26 septembre 2006.

Avis général du CEPD

9. L'avis du CEPD sur la proposition est globalement positif. Le CEPD souscrit totalement aux objectifs que vise la Commission en adoptant une proposition qui renforce la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques. Le CEPD se félicite en particulier de l'adoption d'un système de notification obligatoire des violations de la sécurité (modification apportée à l'article 4 de la directive «vie privée et communications électroniques», ajoutant les paragraphes 3 et 4). En cas d'atteinte aux données, la notification présente des avantages manifestes: elle accroît, pour les organisations, l'obligation de rendre des comptes, elle incite les entreprises à mettre en application des mesures strictes, et permet de déterminer quelles sont les technologies les plus fiables en matière de protection des informations. De plus, elle donne aux personnes victimes de ce type de violation la possibilité de prendre des mesures pour se protéger contre une usurpation d'identité ou d'autres formes d'utilisation abusive des données à caractère personnel les concernant.

10. Le CEPD accueille favorablement d'autres modifications apportées par la proposition, telles que la possibilité, pour les personnes morales ayant un intérêt légitime à le faire, d'engager une action en justice contre les personnes qui violent certaines dispositions de la directive «vie privée et communications électroniques» (modification apportée à l'article 13, ajoutant le paragraphe 6). Le CEPD juge également positif le renforcement des pouvoirs d'enquête des autorités règlementaires nationales, qui leur permettra d'évaluer si un traitement de données est bien effectué dans le respect de la loi, et d'identifier les personnes qui ne la respecteraient pas (ajout de l'article 15 *bis*, paragraphe 3). La possibilité de mettre fin dès que possible au traitement illicite de données à caractère personnel et aux atteintes à la vie privée est une mesure nécessaire afin de protéger les droits et libertés des personnes. À cet effet, le CEPD juge très intéressant l'article 15 *bis*, paragraphe 2, proposé, qui reconnaît aux autorités règlementaires nationales le pouvoir d'ordonner la cessation des infractions, car cette disposition permettra auxdites autorités de faire cesser immédiatement les traitements portant gravement atteinte à la loi.

11. La manière dont est conçue la proposition et la plupart des modifications qui y sont proposées sont conformes au point de vue sur la future politique en matière de protection des données que le CEPD a déjà exprimé dans des avis antérieurs tels que l'avis relatif à la mise en application de la directive sur la protection des données ([1]). Cette conception est notamment fondée sur la conviction qu'il n'est pas nécessaire d'élaborer de nouveaux principes en matière de protection des données, mais qu'il faut adopter des règles plus spécifiques permettant d'apporter une solution aux problèmes de protection des données suscités par les nouvelles technologies comme Internet ou la RFID, etc., ainsi que des instruments qui contribuent à faire respecter la législation relative à la protection des données et à en garantir l'efficacité, tels que la possibilité donnée aux personnes morales de former des recours en cas de violation de la protection des données et l'obligation faite aux responsables du traitement de signaler les violations de la sécurité.

12. Bien que l'approche suivie par la proposition soit globalement positive, le CEPD regrette que la proposition ne soit pas aussi ambitieuse qu'elle aurait pu l'être. De fait, depuis 2003, la mise en œuvre des dispositions de la directive «vie privée et communications électroniques», ainsi qu'une analyse attentive du sujet, ont montré que certaines des dispositions précitées sont loin d'être claires, ce qui est générateur d'insécurité juridique et de problèmes de respect des dispositions. C'est par exemple le cas en ce qui concerne la question de savoir dans quelle mesure les fournisseurs semi-publics de services de communications électroniques sont couverts par la directive en question. On aurait pu espérer que la Commission profiterait du réexamen du «paquet Telecom», et en particulier de la directive «vie privée et communications électroniques», pour résoudre certains des problèmes encore en suspens. De plus, lorsqu'elle traite de questions nouvelles, telles que l'instauration d'un système de notification obligatoire des violations de la sécurité, la proposition n'offre qu'une solution partielle, car elle n'inclut pas dans la sphère des organisations tenues de notifier ces violations les entités qui traitent des catégories très sensibles de données, telles que les banques en ligne ou les fournisseurs de services de santé en ligne. Le CEPD regrette qu'une telle approche ait été suivie.

13. Le CEPD a bon espoir que, au fur et à mesure de la progression de la proposition dans le processus législatif, le législateur tiendra compte des observations et propositions figurant dans le présent avis, en vue de résoudre les problèmes que la proposition de la Commission n'a pas réglés.

([1]) Avis du contrôleur européen de la protection des données du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1).

II. ANALYSE DE LA PROPOSITION

II.1. Champ d'application de la directive «vie privée et communications électroniques» et, plus particulièrement, des services concernés

14. L'un des problèmes essentiels posés par l'actuelle directive «vie privée et communications électroniques» est celui de son champ d'application. La proposition contient des éléments intéressants qui permettraient de définir et de préciser son champ d'application, pour ce qui est en particulier des services concernés, qui seront examinés ci-dessous au point i). Malheureusement, les modifications proposées ne résolvent pas tous les problèmes. Comme nous le verrons ci-dessous au point ii), les modifications ne visent malheureusement pas à étendre le champ d'application de la directive aux services de communications électroniques accessibles sur les réseaux privés.

15. L'article 3 de la directive «vie privée et communications électroniques» décrit les services concernés par la directive, en d'autres termes les services auxquels s'appliquent les obligations énoncées dans la directive: «La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications».

16. Les services concernés par la directive «vie privée et communications électroniques» sont donc les fournisseurs de services de communications électroniques publics accessibles sur les réseaux publics (ci-après dénommés «FSCEP»). La définition d'un FSCEP figure à l'article 2, point c), de la directive-cadre ([1]). Les réseaux de communications publics sont définis à l'article 2, point d), de la directive-cadre ([2]). Parmi les exemples d'activités des FSCEP figurent la fourniture d'accès Internet, la transmission d'informations par des réseaux électroniques, les connexions de téléphonie mobile ou fixe, etc.

i) *Modification qu'il est proposé d'apporter à l'article 3 de la directive «vie privée et communications électroniques»: les «services concernés» comprendraient désormais les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification*

17. La proposition modifie l'article 3 de la directive «vie privée et communications électroniques» en précisant que les réseaux publics de communications électroniques comprennent les «réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification». Le considérant 28 explique que le développement d'applications qui engendrent la collecte de données, y compris de données à caractère personnel, en exploitant les radiofréquences, par exemple les dispositifs d'identification par radiofréquence (RFID), est obligatoirement soumis à la directive «vie privée et communications électroniques» lorsque ces dispositifs sont connectés à des réseaux ou services de communications accessibles au public ou font usage de ces réseaux ou services.

18. Le CEPD juge cette disposition positive dans la mesure où elle précise qu'un certain nombre d'applications RFID relèvent du champ d'application de la directive «vie privée et communications électroniques», ce qui atténue l'insécurité juridique sur ce point et supprime définitivement tout risque de malentendu ou d'interprétation erronée de la législation.

19. En fait, en vertu de l'article 3 de l'actuelle directive «vie privée et communications électroniques», celle-ci couvre déjà certaines applications RFID, et ce pour plusieurs raisons. La première est que les applications RFID relèvent de la définition des services de communications électroniques. La deuxième est que ces applications sont fournies via un réseau de communications électroniques dans la mesure où elles sont prises en charge par un système de transmission qui achemine des signaux par des dispositifs

([1]) Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (JO L 108 du 24.4.2002, p. 33). La directive-cadre délimite ce qu'il convient d'entendre par «service de communications électroniques», en précisant ce qui suit: i) Un «service de communications électroniques» est un service fourni normalement contre rémunération et consistant en la transmission de signaux sur des réseaux de communications électroniques, qui comprend les services de télécommunications et les services de transmission sur les réseaux. ii) Les services qui consistent à fournir des contenus à l'aide de réseaux et de services de communications électroniques n'entrent pas dans la définition des services de communications électroniques. iii) La fourniture de services signifie la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau. iv) Les services de communications électroniques ne comprennent pas les services de la société de l'information, qui sont définis dans la directive sur le commerce électronique comme des services prestés normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

([2]) Un «réseau de communications public» est un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public.

sans fil. Enfin, le réseau peut être public ou privé. S'il est public, les applications RFID seront considérées comme des «services concernés» et relèveront donc du champ d'application de la directive «vie privée et communications électroniques». Cependant, la modification proposée ne laissera plus subsister le moindre doute sur cette question et améliorera ainsi la sécurité juridique.

20 Bien entendu, comme l'a souligné le CEPD dans un avis antérieur sur les RFID ([1]), cette disposition n'exclut pas qu'il puisse être nécessaire d'adopter des instruments juridiques supplémentaires en ce qui concerne les RFID. Néanmoins, ces mesures devraient être adoptées dans un autre contexte et non pas dans le cadre de la proposition à l'examen.

ii) *La nécessité d'inclure les services de communications électroniques accessibles sur les réseaux privés ou semi-privés*

21. Si le CEPD salue les clarifications décrites plus haut, il regrette que la proposition n'ait pas abordé la question de la distinction de moins en moins nette entre réseaux privés et réseaux publics. Il déplore en outre que la définition des services visés par la directive «vie privée et communications électroniques» n'ait pas été étendue aux réseaux privés. Dans sa version actuelle, l'article 3, paragraphe 1, de la directive «vie privée et communications électroniques» s'applique uniquement aux *services de communications électroniques accessibles sur les réseaux publics*.

22. Le CEPD constate que les services ont de plus en plus tendance à combiner des caractéristiques privées et publiques. Prenons l'exemple des universités qui permettent à des milliers d'étudiants d'utiliser Internet et le courrier électronique. La capacité de ces réseaux semi-publics (ou semi-privés) d'empiéter sur la vie privée des personnes est évidente et justifie donc que ce type de services soit soumis aux mêmes règles que les réseaux exclusivement publics. De plus, des réseaux privés tels que ceux d'employeurs fournissant à leurs employés un accès Internet, de propriétaires d'hôtels ou d'appartements offrant à leurs hôtes un accès au téléphone et au courrier électronique, ainsi que ceux des cybercafés, ont une incidence sur la protection des données et la vie privée de leurs utilisateurs, ce qui laisse à penser qu'ils devraient également être couverts par le champ d'application de la directive «vie privée et communications électroniques».

23. En fait, la jurisprudence de certains États membres a déjà indiqué que les services de communications électroniques fournis sur des réseaux privés devaient satisfaire aux mêmes obligations que ceux fournis sur des réseaux publics ([2]). Par ailleurs, en vertu du droit allemand, les autorités chargées de la protection des données ont estimé qu'une société autorisant une utilisation du courrier électronique à titre privé en son sein peut être considérée comme un opérateur de services de télécommunications publics et relever, de ce fait, du champ d'application de la directive «vie privée et communications électroniques».

24. En résumé, l'importance croissante des réseaux mixtes (privés/publics) et des réseaux privés dans la vie quotidienne, et le risque accru qui en découle pour les données à caractère personnel et la vie privée, justifient la nécessité d'appliquer à ces services les mêmes règles que celles qui s'appliquent déjà aux services de communications électroniques publics. À cet effet, le CEPD estime qu'il convient de modifier la directive afin d'en étendre le champ d'application à ce type de services privés; ce point de vue est également celui du Groupe de l'article 29 ([3]).

II.2. **Notification des violations de la sécurité: modification de l'article 4**

25. L'article 4 de la directive «vie privée et communications électroniques» est modifié par l'ajout de deux paragraphes (3 et 4) qui énoncent l'obligation de notifier les violations de la sécurité. En effet, conformément à l'article 4, paragraphe 3, les FSCEP sont tenus, d'une part, d'informer les autorités réglementaires nationales, sans retard indu, de toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques (globalement, la «mise en péril des données») et, d'autre part, d'en informer leurs clients.

([1]) Avis du 20 décembre 2007 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique», document COM(2007) 96.

([2]) La Cour d'appel de Paris a par exemple conclu, dans son arrêt *BNP Paribas c/World Press Online*, rendu le 4 février 2005, qu'il n'y avait pas de distinction entre les fournisseurs de services Internet offrant un accès Internet à titre commercial et les employeurs offrant un accès Internet à leur personnel.

([3]) Avis 8/2006 concernant le réexamen du cadre réglementaire pour les réseaux et services de communications électroniques, axé sur la directive sur la protection de la vie privée dans le secteur des communications électroniques, adopté le 26 septembre 2006.

Avantages de cette obligation

26. Le CEPD salue ces dispositions (paragraphes 3 et 4 de l'article 4) qui introduisent la notification obligatoire des violations de la sécurité. La notification des violations de la sécurité a, du point de vue de la protection des données à caractère personnel et de la vie privée, des effets bénéfiques qui ont déjà été vérifiés aux États-Unis, où la législation sur la notification des violations est déjà en vigueur depuis plusieurs années au niveau des États.

27. Premièrement, la législation sur la notification des violations accroît, pour les FSCEP, l'obligation de rendre des comptes à l'égard des informations mises en péril. Dans le cadre des mesures relatives à la protection des données ou à la vie privée, l'obligation de rendre des comptes signifie que chaque organisation est responsable des informations qui lui sont confiées ou qui sont sous son contrôle. L'obligation de notification revient à réaffirmer, d'une part, que les données qui ont été mises en péril étaient sous le contrôle du FSCEP et, d'autre part, qu'il incombe à cette organisation de prendre les mesures nécessaires à l'égard de ces données.

28. Deuxièmement, il s'est avéré que l'existence d'un système de notification des violations de la sécurité amène les organisations traitant des données à caractère personnel à investir dans la sécurité. En effet, le simple fait d'avoir à notifier publiquement les violations de la sécurité incite les organisations à appliquer, en matière de sécurité, des normes plus strictes destinées à protéger les informations à caractère personnel et à empêcher les violations. De plus, la notification des violations de la sécurité permettra de repérer quels sont les solutions et dispositifs les plus efficaces pour la sécurité et d'effectuer une analyse statistique fiable en ce qui les concerne. On a manqué depuis longtemps de données précises sur les défaillances en matière de sécurité de l'information et sur les technologies de protection les plus appropriées. L'obligation de notification des violations de la sécurité devrait résoudre ce problème, comme cela a été le cas aux Etats-Unis, car la notification donnera des indications sur les technologies les plus exposées aux violations ([1]).

29. Enfin, la notification des violations de la sécurité sensibilise les personnes aux risques qu'elles courent lorsque les données à caractère personnel les concernant sont mises en péril, et les aide à prendre les mesures nécessaires pour atténuer ces risques. À titre d'exemple, si des informations bancaires ont été mises en péril, la personne qui en est informée peut décider de modifier ses codes d'accès à son compte bancaire pour empêcher toute autre personne d'accéder à ces informations et de les utiliser à des fins illicites (pratique généralement qualifiée d'«usurpation d'identité»). En somme, cette obligation réduit la probabilité que des personnes soient victimes d'une usurpation d'identité et peut en outre aider les victimes à prendre les mesures nécessaires pour résoudre les problèmes.

Inconvénient de la modification proposée

30 Si le CEPD est satisfait du système de notification des violations de la sécurité exposé aux paragraphes 3 et 4 de l'article 4, il aurait néanmoins préféré que son application se fasse à plus grande échelle et s'étende aux prestataires de services de la société de l'information. Ainsi les banques en ligne, les entreprises en ligne, les fournisseurs de services de santé en ligne, etc., auraient-ils également été couverts par la législation ([2]).

31. Les raisons qui justifient que soit imposée aux fournisseurs de services de communications électroniques publics, c'est-à-dire aux FSCEP, l'obligation de notifier les violations de la sécurité, valent également pour d'autres organisations qui traitent aussi d'importantes quantités de données à caractère personnel dont la divulgation pourrait être particulièrement préjudiciable aux personnes concernées. Parmi ces organisations figurent les banques en ligne, les courtiers en information et d'autres fournisseurs en ligne tels que ceux qui traitent des données sensibles (sur la santé, les opinions politiques, etc.). La mise en péril d'informations détenues par des banques en ligne et des entreprises en ligne, parmi lesquelles peuvent figurer non seulement des numéros de comptes bancaires mais également des renseignements précis sur les cartes de crédits, peut entraîner des usurpations d'identité, auquel cas il est essentiel que les personnes soient informées pour pouvoir prendre les dispositions nécessaires. Dans le cas des services de santé en ligne, si les personnes ne subissent pas un préjudice d'ordre financier, il est néanmoins fort probable qu'elles subissent un préjudice moral lorsque des informations sensibles les concernant sont mises en péril.

([1]) Voir le rapport intitulé «Security Economics and the Internal Market», commandé par l'ENISA à Ross Anderson, Rainer Böhme, Richard Clayton et Tyler Moore. Le rapport peut être consulté à l'adresse suivante: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Les services de la société de l'information sont définis dans la directive sur le commerce électronique comme des services prestés normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

32. De surcroît, grâce à l'extension du champ de l'obligation, les effets bénéfiques — décrits ci-dessus — que l'on peut attendre de l'instauration de cette obligation ne seront pas limités à un seul secteur d'activité, celui des fournisseurs de services de communications électroniques accessibles au public, mais seront étendus aux services de la société de l'information considérés dans leur ensemble. Le fait que des services de la société de l'information tels que des banques en ligne soient obligés de notifier les violations de la sécurité les rendra davantage comptables de leurs actes, mais cela les incitera aussi à renforcer leurs mesures de sécurité, ce qui permettra d'éviter de futures violations de la sécurité.

33. Il existe déjà des cas dans lesquels la directive «vie privée et communications électroniques» s'applique à des entités autres que les FSCEP: ces cas sont prévus par l'article 5 sur la confidentialité des communications et l'article 13 relatif aux communications non sollicitées («pourriels»). Cela confirme que, par le passé, le législateur, dans sa grande sagesse, a pris la décision d'étendre le champ d'application de certaines dispositions de la directive «vie privée et communications électroniques» parce qu'il l'a jugé opportun et nécessaire. Le CEPD espère que, à présent, le législateur n'hésitera pas à faire preuve du même bon sens et de la même souplesse et qu'il étendra le champ d'application de l'article 4 aux prestataires de services de la société de l'information. Il suffirait, pour ce faire, d'ajouter à l'article 4, paragraphe 3, les termes ci-après faisant référence aux prestataires de services de la société de l'information: «En cas de violation de la sécurité entraînant accidentellement ou (…), le fournisseur de services de communications électroniques accessibles au public et le prestataire de services de la société de l'information informent (…) l'abonné concerné et l'autorité réglementaire nationale de cette violation».

34. Le CEPD considère cette obligation et son application tant aux FSCEP qu'aux prestataires de services de la société de l'information comme la première étape d'un processus qui pourrait en fin de compte s'étendre à l'ensemble des responsables du traitement de données.

Cadre juridique propre aux violations de la sécurité, à examiner dans le cadre de la procédure de comité

35. La proposition omet d'examiner un certain nombre de questions relatives à l'obligation de notifier les violations de la sécurité. Parmi les points qu'il serait nécessaire d'aborder, on peut citer par exemple les circonstances de la notification, ainsi que le format et les procédures applicables. L'article 4, paragraphe 4, de la proposition prévoit plutôt que ces décisions seront adoptées par l'intermédiaire d'un comité du type prévu par la procédure de comité ([1]), à savoir le comité des communications institué par l'article 22 de la directive-cadre, en conformité avec la décision du Conseil du 28 juin 1999. Plus précisément, ces mesures seraient adoptées conformément à l'article 5 de la décision du Conseil du 28 juin 1999 qui fixe les règles pour la procédure de réglementation, concernant «les mesures de portée générale ayant pour objet de mettre en application les éléments essentiels d'actes de base».

36. Le CEPD ne s'oppose pas au choix consistant à laisser aux dispositions d'exécution le soin de régler toutes ces questions. Il est probable que le recours à la procédure de comité raccourcira la procédure législative. De plus, la procédure de comité sera facteur d'harmonisation, objectif qu'il convient indubitablement de chercher à atteindre.

37. Compte tenu du nombre élevé de questions qui devront être traitées dans les mesures d'exécution et de leur importance — que nous avons déjà soulignés —, il semble approprié de les aborder toutes ensemble dans un seul instrument législatif plutôt que dans le cadre d'une approche fractionnée consistant à traiter certaines de ces questions dans la directive «vie privée et communications électroniques» et à laisser les dispositions d'exécution régler les autres. La solution proposée par la Commission, qui consiste à dire que ces décisions seront régies par des dispositions d'exécution qui devront être adoptées après consultation du CEPD et, il faut l'espérer, d'autres parties prenantes (voir ci-dessous), doit donc être saluée.

Questions qui devront être traitées dans des mesures d'exécution

38. L'importance des mesures d'exécution apparaît clairement lorsqu'on prévoit avec un certain détail, quelles sont les questions qui devront être traitées par cette voie. En effet, les mesures d'exécution pourront déterminer les modalités selon lesquelles les notifications devront être effectuées. À titre d'exemple, elles préciseront ce qui constitue une violation de la sécurité, ainsi que les conditions et les délais dans lesquels les personnes et les autorités devront recevoir une notification.

([1]) Procédures législatives de la CE qui font intervenir des comités composés des représentants des gouvernements des États membres au niveau des fonctionnaires.

39. Le CEPD estime que la directive «vie privée et communications électroniques», et en particulier son article 4, ne devraient prévoir aucune exception à l'obligation de notification. À cet égard, le CEPD est satisfait de la solution de la Commission figurant à l'article 4, qui prévoit une obligation de notification sans l'assortir d'aucune exception, mais qui laisse aux dispositions d'exécution le soin de régir ce point, parmi d'autres. Bien qu'il connaisse les arguments qui pourraient justifier l'instauration de certaines exceptions à cette obligation, le CEPD est favorable à ce que ce point, et d'autres, fassent l'objet d'un examen attentif dans le cadre des dispositions d'exécution, au terme d'un débat approfondi et global de toutes les questions en jeu. Comme indiqué ci-dessus, la complexité des questions liées à l'obligation de notifier les violations de la sécurité, y compris l'opportunité de prévoir des exceptions ou des restrictions, exige un traitement unifié, c'est-à-dire dans le cadre d'un seul acte législatif portant exclusivement sur cette question.

Consultation du CEPD et nécessité d'élargir la consultation

40. Compte tenu de l'impact qu'auront les mesures d'exécution sur la protection des données à caractère personnel, il est important que, préalablement à l'adoption de ces mesures, la Commission entreprenne un véritable exercice de consultation. C'est pourquoi le CEPD se félicite de l'article 4, paragraphe 4, de la proposition qui prévoit explicitement que, la Commission le consultera avant d'adopter les mesures d'exécution. En plus de concerner la protection des données à caractère personnel et la vie privée des personnes, ces mesures auront sur cette protection un impact important. Il importe donc de demander l'avis du CEPD, comme l'exige l'article 41 du règlement (CE) n° 45/2001.

41. Outre la consultation du CEPD, il pourrait être opportun d'insérer une disposition établissant que le projet de mesures d'exécution fera l'objet d'une consultation publique, afin de recueillir des avis et d'encourager l'échange d'expériences en matière de meilleures pratiques dans ces domaines. Les milieux professionnels, mais aussi d'autres parties prenantes, y compris les autres autorités chargées de la protection des données et le Groupe de l'article 29, auront ainsi une réelle possibilité de faire connaître leur point de vue. La nécessité d'une consultation publique est d'autant plus forte que l'adoption de la législation s'effectuera selon une procédure de comité, avec une intervention limitée du Parlement européen.

42. Le CEPD note que, aux termes de l'article 4, paragraphe 4, de la proposition, la Commission consultera également l'Autorité européenne du marché des communications électroniques avant d'adopter les dispositions d'exécution, principe auquel le CEPD est attaché puisque cette autorité sera dépositaire de l'expérience et des connaissances de l'ENISA sur les questions de sécurité des réseaux et de l'information. Tant que cette autorité n'est pas créée, il pourrait être judicieux, à titre provisoire, de prévoir, dans la modification proposée (l'article 4, paragraphe 4), la consultation de l'ENISA.

II.3. **Disposition relative aux témoins de connexion («cookies»), aux logiciels espions et aux autres dispositifs analogues: modification de l'article 5, paragraphe 3**

43. L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» porte sur la question des technologies qui permettent d'accéder à des informations et de les stocker dans l'équipement terminal des utilisateurs, via des réseaux de communications électroniques. L'article 5, paragraphe 3, s'applique par exemple à l'utilisation de cookies ([1]). Parmi les autres exemples, on peut également citer l'utilisation de technologies telles que les logiciels espions (programmes d'espionnage cachés) et les chevaux de Troie (programmes dissimulés dans des messages ou d'autres logiciels inoffensifs en apparence). Les objectifs et finalités de ces technologies sont très variables: si certains sont parfaitement inoffensifs ou même utiles à l'utilisateur, d'autres sont sans conteste très nuisibles et menaçants.

([1]) Les cookies sont placés par des ISSP (sites web) dans l'équipement terminal des utilisateurs, dans différents buts, dont celui de reconnaître un visiteur lorsqu'il se rend de nouveau sur un site web. En pratique, lorsqu'un cookie est envoyé à un internaute par un site web, un numéro unique est attribué à son ordinateur (l'ordinateur ayant reçu des cookies du site web A devient «l'ordinateur détenteur du cookie 111»). Le site web conserve ce numéro comme référence. Si l'utilisateur (ou les utilisateurs) de l'ordinateur ayant reçu le cookie 111 ne supprime(nt) pas le fichier du cookie, lors de sa (ou de leur) prochaine visite sur le même site web, celui-ci sera capable d'identifier l'ordinateur comme le détenteur du cookie 111. Le site web en déduit naturellement que l'ordinateur en question l'a déjà visité. Le dispositif qui permet à un site web de reconnaître un ordinateur comme visiteur «fidèle» est simple. Lorsque l'ordinateur «visiteur» détient des cookies, tels que le cookie 111, et qu'il effectue une visite sur le site qui a, lors d'une visite antérieure, généré ce cookie, il recherchera sur le disque dur de l'utilisateur le numéro de fichier du cookie. Si le navigateur de l'utilisateur trouve un fichier de cookie correspondant au numéro de référence conservé par le site web, il informe le site web que l'ordinateur détient un cookie 111.

44. L'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» énonce les conditions dans lesquelles il est autorisé d'accéder à des informations ou d'en stocker dans l'équipement terminal d'utilisateurs en utilisant, notamment, les technologies susmentionnées. En particulier, en vertu de l'article 5, paragraphe 3, *i)* les internautes doivent recevoir, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement, et *ii)* ils doivent avoir le droit de refuser un tel traitement, c'est-à-dire le droit de rejeter le traitement des informations extraites de leur équipement terminal.

Avantages de la modification proposée

45. L'article 5, paragraphe 3, de l'actuelle directive «vie privée et communications électroniques» limite son champ d'application aux situations dans lesquelles l'accès aux informations et leur stockage dans l'équipement terminal des utilisateurs sont effectués via des *réseaux de communications électroniques*. Cela comprend la situation décrite ci-dessus concernant l'utilisation de cookies, ainsi que d'autres technologies telles que les logiciels espions transférés via des réseaux de communications électroniques. Cependant, il n'est absolument pas précisé si l'article 5, paragraphe 3, s'applique aux situations dans lesquelles des technologies analogues (cookies/logiciels espions et dispositifs apparentés) sont diffusées par l'intermédiaire de logiciels installés sur des supports de stockage de données externes et téléchargées dans l'équipement terminal des utilisateurs. Étant donné que la menace sur la vie privée existe indépendamment du moyen de communication, la limitation de l'article 5, paragraphe 3, à un seul moyen de communication est regrettable.

46. Le CEPD se félicite donc de la modification apportée à l'article 5, paragraphe 3, qui, en supprimant la mention des «réseaux de communications électroniques», élargit de fait le champ d'application de cette disposition. En effet, la version modifiée de l'article 5, paragraphe 3, englobe à la fois les situations dans lesquelles l'accès aux informations et leur stockage dans l'équipement terminal des utilisateurs sont effectués via des réseaux de communications électroniques et les cas dans lesquels ils sont effectués via d'autres supports de stockage de données externes tels que CD, CD-ROM, clés USB, etc.

Stockage technique visant à faciliter la transmission

47. La dernière phrase de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» n'est pas modifiée par la proposition. Conformément à cette dernière phrase, les exigences énoncées dans la première phrase du même paragraphe «ne [font] pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information (…)». Par conséquent, les règles impératives énoncées dans la première phrase de l'article 5, paragraphe 3 (la nécessité d'informer et d'offrir la possibilité de refuser) ne s'appliqueront pas lorsque l'accès à l'équipement terminal de l'utilisateur ou le stockage d'informations viseront exclusivement à *faciliter* une transmission ou lorsqu'ils seront strictement nécessaires à la fourniture de services de la société de l'information demandés par l'utilisateur.

48. La directive ne précise pas dans quels cas l'accès à des informations ou leur stockage vise exclusivement à faciliter une transmission ou à fournir des informations. Il est une situation qui relèverait de toute évidence de cette exception: il s'agit de l'établissement d'une connexion à Internet. En effet, pour établir une connexion à Internet, il est nécessaire d'obtenir une adresse IP ([1]). L'ordinateur de l'utilisateur final sera amené à divulguer au fournisseur d'accès Internet certaines informations le concernant et, en retour, le fournisseur d'accès Internet lui attribuera une adresse IP. Les informations stockées dans l'équipement terminal de l'utilisateur final seront alors transférées au fournisseur d'accès Internet en vue de l'octroi à l'utilisateur d'un accès à Internet. Dans ce cas, le fournisseur d'accès Internet est exempté à la fois de l'obligation de déclarer cette collecte d'informations et de l'obligation d'accorder un droit de refus, dans la mesure où cette opération est nécessaire à la fourniture du service.

49. Une fois connecté à Internet, si un utilisateur souhaite accéder à un site web, il doit adresser une demande au serveur hébergeant le site en question. Celui-ci répondra s'il sait où envoyer l'information, c'est-à-dire s'il connaît l'adresse IP de l'utilisateur. En raison du mode de stockage de cette adresse, il faudra à nouveau que le site web sur lequel l'utilisateur souhaite se rendre accède à des informations sur l'équipement terminal des internautes. Cette opération relèverait elle aussi, manifestement, du champ d'application de l'exception. De fait, il semble approprié que ces cas ne tombent pas dans le champ d'application des exigences de l'article 5, paragraphe 3.

([1]) Une adresse IP est une adresse unique que certains dispositifs électroniques utilisent afin de s'identifier et de communiquer entre eux sur un réseau informatique utilisant la norme «Internet Protocol». Il s'agit donc, pour parler plus simplement, d'une adresse informatique. Tout dispositif appartenant au réseau — y compris les routeurs, les commutateurs, les ordinateurs, les serveurs d'infrastructure (par ex. NTP, DNS, DHCP, SNMP, etc.), les imprimantes, les télécopieurs Internet, et certains téléphones — peut avoir sa propre adresse, unique au sein du réseau donné. Certaines adresses IP sont destinées à être uniques dans le cadre de l'Internet mondial, tandis que d'autres n'ont besoin d'être uniques que dans le cadre d'une entreprise.

50. Le CEPD juge approprié que l'obligation d'informer et de donner la possibilité de refuser ne s'applique pas aux cas, illustrés ci-dessus, dans lesquels le stockage technique ou l'accès à l'équipement terminal d'un utilisateur est *nécessaire* à la seule fin d'effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques. Il en va de même lorsque le stockage ou l'accès techniques sont strictement nécessaires à la fourniture d'un service de la société de l'information. Toutefois, le CEPD ne juge pas nécessaire d'exclure du champ de l'obligation d'informer et d'accorder un droit de refus les situations dans lesquelles le stockage ou l'accès techniques visent uniquement à *faciliter* la transmission d'une communication. À titre d'exemple, conformément à la dernière phrase de cet article, une personne concernée pourrait ne pas jouir du droit d'être informée et de s'opposer au traitement des données la concernant si un cookie recueille ses préférences linguistiques ou le lieu où elle se trouve (par ex. la Belgique ou la Chine), puisque ce type de cookie pourrait être présenté comme ayant pour objectif de faciliter la transmission d'une communication. Le CEPD sait que, au niveau des logiciels, les personnes concernées ont, en pratique, la possibilité de refuser ou de moduler le stockage de cookies. Cependant, cette pratique n'est appuyée suffisamment clairement par aucune disposition légale qui autoriserait formellement la personne concernée à défendre ses droits dans le contexte décrit ci-dessus.

51. Pour éviter cette issue, le CEPD suggère d'apporter une légère modification à la dernière partie de l'article 5, paragraphe 3, en supprimant le mot «faciliter» dans la phrase suivante: «ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information (…)».

II.4. **Actions en justice engagées par des FSCEP et d'autres personnes morales: ajout d'un paragraphe 6 à l'article 13**

52. Le paragraphe 6 qu'il est proposé d'ajouter à l'article 13 introduit la possibilité de recours civils pour toute personne physique ou morale, en particulier les fournisseurs de services de communications électroniques, ayant un intérêt professionnel à lutter contre les infractions à l'article 13 de la directive «vie privée et communications électroniques». Cet article porte sur l'envoi de communications commerciales non sollicitées.

53. La modification proposée permettra par exemple aux fournisseurs d'accès Internet de lutter contre les polluposteurs qui utilisent abusivement leurs réseaux, de poursuivre les entités qui contrefont les adresses d'expéditeurs ou qui pénètrent dans les serveurs pour les utiliser comme relais de pourriels, etc.

54. La directive «vie privée et communications électroniques» n'indiquait pas clairement si elle accordait aux FSCEP le droit de saisir la justice à l'encontre des polluposteurs, et les FSCEP n'ont que très rarement intenté des actions en justice pour violation de l'article 13, tel que mis en œuvre dans la législation des États membres ([1]). En reconnaissant aux fournisseurs de services de communications électroniques le droit d'engager une action en justice pour protéger leurs intérêts commerciaux, la proposition confirme que la directive «vie privée et communications électroniques» vise à protéger non seulement les abonnés individuels, mais également les fournisseurs de services de communications électroniques.

55. Le CEPD constate que la proposition introduit la possibilité, pour les fournisseurs de services de communications électroniques ayant un intérêt professionnel, de saisir la justice à l'encontre des polluposteurs. Sauf dans des circonstances exceptionnelles, les abonnés individuels n'ont ni l'argent ni la motivation pour engager ce type d'action. À l'inverse, les fournisseurs d'accès Internet et les autres FSCEP ont la force financière et la capacité technologique d'enquêter sur les campagnes de pollupostage et d'en identifier les auteurs, et il semble aller de soi qu'ils aient le droit d'engager des actions en justice contre les polluposteurs.

56. Le CEPD est particulièrement favorable à la modification proposée dans la mesure où elle permettrait également aux associations de consommateurs et aux syndicats représentant les intérêts des consommateurs victimes de pollupostage d'engager des actions en justice en leur nom. Comme nous l'avons souligné plus haut, le préjudice infligé à une personne concernée victime de pollupostage, considéré isolément, n'est généralement pas suffisant en soi pour que cette personne saisisse la justice. En fait, le CEPD avait déjà proposé cette mesure à l'égard du non-respect de la vie privée et de la protection des

([1]) On peut citer l'affaire Microsoft corporation c/Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

données, d'une manière générale, dans son avis sur le suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données ([1]). Selon le CEPD, la proposition aurait pu aller plus loin et proposer des recours collectifs, qui permettraient à des groupes de citoyens de saisir la justice dans des affaires relatives à la protection des données à caractère personnel. En cas de pollupostage, puisque beaucoup de personnes reçoivent des pourriels, il existe un potentiel de regroupement des personnes en vue d'engager des recours collectifs contre les polluposteurs.

57. Le CEPD regrette particulièrement que la proposition limite la possibilité offerte aux personnes morales de saisir la justice aux situations dans lesquelles il y a violation de l'article 13 de la directive, c'est-à-dire aux violations de la disposition relative aux communications non sollicitées par courriel. En effet, en vertu de la modification proposée, les personnes morales ne seraient pas habilitées à saisir la justice pour des violations d'autres dispositions de la directive «vie privée et communications électroniques». À titre d'exemple, la disposition actuelle ne permet pas à une personne morale comme une association de consommateurs d'engager une action en justice contre un fournisseur d'accès Internet qui aurait divulgué des données à caractère personnel concernant des millions de clients. La mise en œuvre de la directive «vie privée et communications électroniques» dans sa globalité, et non d'un seul article donné, se trouverait sensiblement amélioré si la disposition énoncée à l'article 13, paragraphe 6, devenait une disposition de portée générale permettant aux personnes morales de saisir la justice en cas de violation de toute disposition de la directive.

58. Pour régler ce problème, le CEPD suggère de transformer le paragraphe 6 de l'article 13 en un article distinct (l'article 14). Le libellé de cette disposition serait en outre légèrement modifié, les termes «en application du présent article» étant remplacés par «en application de la présente directive».

II.5. **Renforcement des dispositions relatives au contrôle de l'application: ajout d'un article 15 *bis***

59. La directive «vie privée et communications électroniques» ne comporte pas de dispositions explicites sur le contrôle de l'application, et se borne à renvoyer à la section pertinent de la directive relative à la protection des données ([2]). Le CEPD se félicite du nouvel article 15 *bis* de la proposition, qui traite explicitement du contrôle de l'application dans le cadre de cette directive.

60. Premièrement, le CEPD fait observer que, dans ce domaine, une politique efficace en matière de contrôle de l'application suppose, comme le prévoit l'article 15 *bis*, paragraphe 3, que les autorités nationales disposent de pouvoirs d'enquête leur permettant de recueillir les informations nécessaires. Très souvent, les preuves des violations des dispositions de la directive sont de nature électronique et il se peut qu'elles soient stockées sur différents ordinateurs et dispositifs ou réseaux. Dès lors, il est important que les organismes de contrôle aient la possibilité d'obtenir des mandats de perquisition leur donnant le pouvoir d'effectuer des perquisitions et des saisies.

61. Deuxièmement, le CEPD se réjouit particulièrement du paragraphe 2 du nouvel article 15 *bis*: en vertu de cette disposition, les autorités réglementaires nationales doivent avoir le pouvoir de prononcer des injonctions, c'est-à-dire d'ordonner la cessation des infractions, et disposer des pouvoirs d'enquête et des ressources nécessaires. Les autorités réglementaires nationales, y compris les autorités nationales chargées de la protection des données, devraient avoir le pouvoir de prononcer des injonctions imposant aux auteurs d'infractions de cesser toute activité contraire à la directive «vie privée et communications électroniques». L'injonction ou le pouvoir d'ordonner la cessation d'une infraction est un instrument utile en cas de comportement persistant violant les droits des personnes. Les injonctions seront très utiles pour faire cesser les atteintes à la directive «vie privée et communications électroniques» telles que la violation de l'article 13 relatif aux communications commerciales non sollicitées qui constituent, par nature, un comportement persistant.

62. Troisièmement, la proposition permet à la Commission d'adopter des mesures de mise en œuvre techniques afin d'assurer une coopération transfrontalière effective dans le contrôle de l'application des législations nationales (nouvel article 15 *bis*, paragraphe 4). Jusqu'à présent, la coopération s'effectuait notamment dans le cadre de l'accord conclu à l'initiative de la Commission et instaurant une procédure commune pour le traitement des plaintes transnationales concernant le pollupostage.

([1]) Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données (JO C 255 du 27.10.2007, p. 1).

([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.

62. Le CEPD estime que, si la législation contribue à ce que les autorités de contrôle aident leurs homologues dans d'autres pays, l'application transfrontalière des règles s'en trouvera indéniablement facilitée. Il est donc judicieux que la proposition permette à la Commission de créer les conditions propices à la mise en œuvre d'une coopération transfrontalière, y compris les procédures applicables à l'échange d'informations.

III. **CONCLUSIONS ET RECOMMANDATIONS**

64. Le CEPD est totalement favorable à cette proposition. Les modifications proposées renforcent la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques; cela est fait avec discernement, sans faire peser de charges injustifiées et inutiles sur les organisations. Plus précisément, le CEPD estime que la plupart des modifications proposées ne devraient pas être remaniées dans la mesure où elles répondent bien à l'objectif visé. Le point 69 ci-dessous dresse la liste des modifications dont le CEPD souhaiterait qu'elles restent inchangées.

65. Si son avis est globalement positif, le CEPD considère néanmoins qu'il convient d'améliorer certaines des modifications proposées, afin qu'elles assurent une réelle protection des données à caractère personnel et de la vie privée. C'est notamment le cas des dispositions relatives à la notification des violations de la sécurité et de celles qui portent sur les actions en justice engagées par des fournisseurs de services de communications électroniques pour violation des dispositions relatives au pollupostage. Par ailleurs, le CEPD regrette que la proposition n'omette pas certaines questions qui ne sont pas correctement traitées dans la directive en vigueur, et qu'elle manque ainsi l'occasion — offerte par cet exercice de réexamen — de résoudre les problèmes en suspens.

66. Pour résoudre les deux problèmes, à savoir les questions qui ne sont pas traitées de façon satisfaisante dans la proposition et celles qui n'y sont pas abordées du tout, le présent avis a formulé des propositions d'ordre rédactionnel. Les points 67 et 68 synthétisent les problèmes et proposent des libellés spécifiques. Le CEPD invite le législateur à en tenir compte au fur et à mesure de la progression de la proposition dans le processus législatif.

67. Les modifications figurant dans la proposition que le CEPD souhaiterait vivement voir remaniées sont les suivantes:

i) **Notification des violations de la sécurité**: Telle qu'elle est libellée, la modification visant à ajouter un *paragraphe 4 à l'article 4* s'applique aux fournisseurs de services de communications électroniques publics accessibles sur les réseaux publics (fournisseurs de services Internet, opérateurs de réseaux) qui sont tenus, en cas de violation de la sécurité, d'en informer les autorités réglementaires nationales et leurs clients. Le CEPD souscrit sans réserve à cette obligation. Il estime cependant qu'elle devrait également s'appliquer aux prestataires de services de la société de l'information qui traitent souvent des informations à caractère personnel sensibles. Ainsi, cette obligation devrait également s'appliquer aux banques et assureurs en ligne, aux fournisseurs de services de santé en ligne et à toute autre entreprise en ligne.

À cet effet, le CEPD suggère d'ajouter à l'article 4, paragraphe 3, les termes ci-après faisant référence aux prestataires de services de la société de l'information: «En cas de violation de la sécurité (…), le fournisseur de services de communications électroniques accessibles au public *et le prestataire de services de la société de l'information informent* (…) l'abonné concerné et l'autorité réglementaire nationale de cette violation».

ii) **Actions en justice engagées par des fournisseurs de services de communications électroniques publics accessibles sur les réseaux publics**: Telle qu'elle est libellée, la modification proposée, consistant à ajouter un *paragraphe 6 à l'article 13*, introduit la possibilité pour toute personne physique ou morale, en particulier les fournisseurs de services de communications électroniques, de former un recours civil contre les infractions à l'article 13 de la directive «vie privée et communications électroniques» relatif au pollupostage. Le CEPD accueille favorablement cette disposition. Toutefois, il ne comprend pas pourquoi cette nouvelle possibilité est limitée à la violation de l'article 13. Le CEPD suggère de donner aux personnes morales la possibilité de saisir la justice en cas de violation de toute disposition de la directive «vie privée et communications électroniques».

À cette fin, le CEPD suggère de transformer le paragraphe 6 de l'article 13 en un article distinct (l'article 14). Le libellé de cette disposition serait en outre légèrement modifié, les termes «en application du présent article» étant remplacés par «en application de la présente directive».

68. Le fait que le champ d'application de la directive «vie privée et communications électroniques» soit actuellement limité aux fournisseurs de réseaux de communications électroniques publics est, parmi les questions ignorées par la proposition, l'une des plus préoccupantes. Le CEPD estime qu'il convient de modifier la directive afin d'en étendre l'application aux fournisseurs de services de communications électroniques accessibles sur des réseaux mixtes (privés/publics) et des réseaux privés.

69. Les modifications dont le CEPD souhaiterait vivement qu'elles restent inchangées sont les suivantes:

i) **RFID**: La modification qu'il est proposé d'apporter à l'*article 3*, précisant que les réseaux de communications électroniques comprennent les «réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification», est pleinement satisfaisante. Cette disposition est très positive car elle précise qu'un certain nombre d'applications RFID doivent être conformes à la directive «vie privée et communications électroniques», ce qui atténue l'insécurité juridique sur ce point.

ii) **Cookies/logiciels espions**: La modification qu'il est proposé d'apporter à l'*article 5, paragraphe 3*, est la bienvenue car, grâce à elle, l'obligation d'informer et d'accorder le droit de refuser le stockage de cookies ou de logiciels espions dans son équipement terminal sera également applicable lorsque ces dispositifs sont installés via des supports de stockage de données externes tels que des CD-ROM ou des clés USB. Néanmoins, le CEPD suggère d'apporter une légère modification à la dernière partie de l'article 5, paragraphe 3, en supprimant de la phrase le mot «faciliter».

iii) **Choix de la procédure de comité avec consultation du CEPD, et détermination des conditions/restrictions dont doit être assortie l'obligation de notification**: La modification proposée ajoutant un paragraphe 4 à l'article 4, qui concerne la notification des violations de la sécurité, prévoit que les questions complexes relatives aux circonstances, au format et aux procédures applicables au système de notification seront tranchées dans le cadre de la procédure de comité, après consultation du CEPD. Celui-ci est extrêmement favorable à cette approche unifiée. La législation relative à la notification des violations de la sécurité est une question à part entière, qu'il convient de régler au terme d'un débat et d'une analyse approfondis.

Il convient d'évoquer, à cet égard, la demande de certaines parties prenantes qui souhaitent des dérogations à l'obligation de notifier les violations de la sécurité figurant à l'article 4, paragraphe 4. Le CEPD est farouchement opposé à cette approche. Il souhaite au contraire que la question globale de la notification, de ses modalités, des circonstances dans lesquelles elle peut être abrégée ou quelque peu limitée, fasse l'objet d'une analyse globale, après la tenue d'un véritable débat.

iv) **Contrôle de l'application**: La modification proposée consistant à ajouter l'*article 15 bis* comporte de nombreux éléments utiles qu'il convient de conserver et qui contribueront au respect effectif des règles: il s'agit notamment des dispositions renforçant les pouvoirs d'enquête des autorités réglementaires nationales (paragraphe 3 de l'article 15 *bis*) et conférant auxdites autorités le pouvoir d'ordonner la cessation des infractions.

Fait à Bruxelles, le 10 avril 2008.

Peter HUSTINX

Contrôleur européen de la protection des données