Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de 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»)

(2009/C 128/04)

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,

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,

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,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

Toile de fond

1. Le 13 novembre 2007, la Commission européenne a adopté une proposition de directive (ci-après dénommée «proposition de la Commission») modifiant, entre autres, la directive «vie privée et communications électroniques» ([1]). Le 10 avril 2008, le CEPD a rendu un avis sur la proposition de la Commission dans lequel il a formulé des recommandations visant à l'améliorer afin que les modifications proposées aboutissent à la meilleure protection possible de la vie privée et des données à caractère personnel (ci-après dénommé «premier avis du CEPD») ([2]).

2. Le CEPD s'est félicité de la proposition de la Commission de créer un système de notification obligatoire des violations de la sécurité, exigeant que les sociétés informent les personnes lorsque leurs données à caractère personnel ont été compromises. En outre, le CEPD a également accueilli favorablement la nouvelle disposition permettant aux personnes morales (par exemple, aux associations de consommateurs et aux fournisseurs de services internet) d'engager des actions en justice contre les polluposteurs, en vue de compléter les instruments existants visant à lutter contre les pourriels.

3. Lors des débats parlementaires qui ont précédé la première lecture du Parlement européen, le CEPD a rendu un avis complémentaire en présentant ses observations sur certaines questions découlant des rapports établis par les commissions du Parlement européen compétentes pour procéder au réexamen des directives «service universel» ([3]) et «vie privée et communications électroniques» (ci-après dénommées «observations du CEPD») ([4]). Ces observations portent essentiellement sur des questions liées au traitement des données relatives au trafic et à la protection des droits de propriété intellectuelle.

4. Le 24 septembre 2008, le Parlement européen (ci-après dénommé «PE») a adopté une résolution législative sur la directive «vie privée et communications électroniques» (ci-après dénommée «première lecture du PE») ([5]). Le CEPD a accueilli favorablement plusieurs des amendements adoptés par le PE à la suite de l'avis et des observations du CEPD mentionnés précédemment. Parmi les modifications importantes figurait la soumission des fournisseurs de services de la société de l'information (c'est-à-dire de sociétés fournissant des services via l'internet) à l'obligation de notifier des violations de la sécurité. Le CEPD a également salué l'amendement permettant aux personnes morales et physiques d'intenter des actions en justice pour violation des dispositions de la directive «vie privée et communications électroniques» (et non seulement pour

([1]) Le réexamen de la directive «vie privée et communications électroniques» s'inscrit dans le cadre d'un processus de réexamen plus large ayant pour objectifs la création d'une autorité européenne des télécommunications, le réexamen des directives 2002/21/CE, 2002/19/CE, 2002/20/CE, 2002/22/CE et 2002/58/CE, ainsi que le réexamen du règlement (CE) n° 2006/2004 (ci-après dénommé collectivement «réexamen du paquet Télécom»).

([2]) Avis du 10 avril 2008 sur la 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 (directive «vie privée et communications électroniques»), JO C 181 du 18.7.2008, p. 1.

([3]) Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «service universel»), JO L 108 du 24.4.2002, p. 51.

([4]) Observations du CEPD sur certaines questions découlant du rapport de l'IMCO sur le réexamen de la directive 2002/22/CE (service universel) et de la directive 2002/58/CE (vie privée et communications électroniques), 2 septembre 2008, disponibles à l'adresse http://www.edps.europa.eu

([5]) Résolution législative du Parlement européen du 24 septembre 2008 sur la 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 [COM(2007) 698 — C6-0420/2007 — 2007/248(COD)].

violation des dispositions relatives au pollupostage comme le prévoyait initialement la proposition de la Commission). La première lecture du PE a été suivie de l'adoption par la Commission d'une proposition modifiée de directive relative à la directive «vie privée et communications électroniques» (ci-après dénommée «proposition modifiée de la Commission») ([6]).

5. Le 27 novembre 2008, le Conseil a dégagé un accord politique sur le réexamen des règles relatives au paquet Télécom, y compris de la directive «vie privée et communications électroniques», qui deviendra la position commune du Conseil (ci-après dénommée «position commune du Conseil») ([7]). Conformément à l'article 251, paragraphe 2, du traité instituant la Communauté européenne, la position commune du Conseil sera transmise au PE, qui pourra ensuite proposer des amendements à celle-ci.

Avis général concernant la position du Conseil

6. Le Conseil a modifié des éléments essentiels du texte de la proposition et a rejeté de nombreux amendements adoptés par le PE. Alors que la position commune du Conseil comporte certainement des éléments positifs, le CEPD est, dans l'ensemble, préoccupé quant à son contenu, compte tenu en particulier du fait que celle-ci ne reprend pas certaines des modifications constructives présentées par le PE ou dans la proposition modifiée de la Commission ou les avis du CEPD et des autorités européennes de protection des données, rendus dans le cadre du groupe «Article 29» ([8]).

7. En revanche, dans un certain nombre de cas, des dispositions figurant dans la proposition modifiée de la Commission et les amendements du PE, qui offrent des garanties aux citoyens, sont supprimées ou considérablement édulcorées. Par conséquent, le niveau de protection accordé aux personnes dans la position commune est considérablement affaibli. C'est pour ces raisons que le CEPD formule aujourd'hui un deuxième avis, dans l'espoir qu'au fur et à mesure de la progression de la directive «vie privée et communications électroniques» dans le processus législatif, de nouvelles modifications seront adoptées, qui rétabliront les garanties en matière de protection des données.

8. Le présent avis porte essentiellement sur certaines préoccupations centrales et ne reproduit pas l'ensemble des remarques formulées dans le premier avis ou les observations du CEPD, qui restent néanmoins toutes valables. Le présent avis traite en particulier des points suivants:

— Les dispositions relatives à la notification des violations de la sécurité;

— L'application de la directive «vie privée et communications électroniques» aux réseaux privés et aux réseaux privés accessibles au public;

— Le traitement des données relatives au trafic à des fins de sécurité;

— La capacité des personnes morales à agir en justice en cas de violation de la directive «vie privée et communications électroniques».

9. Dans le cadre de l'examen de ces points, le présent avis analyse la position commune du Conseil et la compare avec la première lecture du PE et la proposition modifiée de la Commission. Le présent avis contient des recommandations qui visent à rationaliser les dispositions de la directive «vie privée et communications électronique» et à s'assurer que celle-ci continue à protéger de manière adéquate la vie privée et les données à caractère personnel des intéressés.

II. DISPOSITIONS RELATIVES À LA NOTIFICATION DES VIOLATIONS DE LA SÉCURITÉ

10. Le CEPD est favorable à l'adoption d'un système de notification des violations de la sécurité dans le cadre duquel les autorités et les personnes seront informées lorsque leurs données à caractère personnel auront été compromises ([9]). Les notifications des violations de la sécurité peuvent aider les personnes à prendre les mesures qui s'imposent pour réduire les dommages susceptibles de résulter d'une telle compromission. En outre, l'obligation de notifier les violations de la sécurité incitera les sociétés à améliorer la sécurité des données et les rendra davantage comptables des données à caractère personnel dont elles sont responsables.

11. La proposition modifiée de la Commission, la première lecture du PE et la position commune du Conseil représentent trois approches différentes de la notification des violations de la sécurité en cours d'examen. Chacune de ces approches présente des aspects positifs. Toutefois, le CEPD estime que des améliorations peuvent être apportées à chacune d'entre elles et recommande de tenir compte des recommandations formulées ci-après dans le cadre de l'examen des dernières étapes de l'adoption d'un système de notification des violations de la sécurité.

([6]) Proposition modifiée 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, Bruxelles, 6 novembre 2008, COM(2008)723 final.

([7]) Disponible sur le site internet public du Conseil.

([8]) Avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), disponible sur le site internet du comité de l'article 29.

([9]) L'expression «compromises» est utilisée dans le présent avis pour désigner toute violation de la sécurité de données à caractère personnel résultant de la destruction, de la perte, de l'altération, de la divulgation non autorisée de telles données transmises, stockées ou traitées d'une autre manière, ou de l'accès non autorisé à ces données, survenus accidentellement ou de manière illicite.

12. Lors de l'analyse des trois systèmes de notification des violations de la sécurité, il convient d'examiner cinq points essentiels: *i)* la définition de la violation de la sécurité; *ii)* les entités concernées par l'obligation de notification (ci-après dénommées «entités concernées»); *iii)* le critère de déclenchement de l'obligation de notification; *iv)* la détermination de l'entité chargée de décider si une violation de la sécurité remplit ou non ce critère, et *v)* les destinataires de la notification.

Vue d'ensemble des approches respectives de la Commission, du Conseil et du PE

13. Le PE, la Commission et le Conseil n'ont pas adopté la même approche en matière de notification des violations de la sécurité. La première lecture du PE a modifié le système de notification des violations de la sécurité qui figurait à l'origine dans la proposition de la Commission ([10]). Dans le cadre de l'approche du PE, l'obligation de notification s'applique non seulement aux fournisseurs de services de communications électroniques accessibles au public (ci-après dénommés «FSCEP»), mais aussi aux fournisseurs de services de la société de l'information (ci-après dénommés «FSSI»). En outre, dans le cadre de cette approche, toutes les violations de données à caractère personnel devraient être notifiées à l'autorité règlementaire nationale ou aux autorités compétentes (ci-après collectivement dénommées «autorités»). Si les autorités devaient juger la violation *grave*, elles demanderaient aux FSCEP et aux FSSI d'avertir sans délai la personne affectée. En cas de violations représentant un danger imminent et direct, les FSCEP et les FSSI informeraient les personnes avant les autorités, sans attendre de décision règlementaire. Une exception à l'obligation de notification concerne les entités qui peuvent prouver aux autorités que «*les mesures de protection technologiques appropriées ont été appliquées*» et que ces mesures rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

14. Dans le cadre de l'approche du Conseil, la notification doit aussi être adressée à la fois aux abonnés et aux autorités, mais seulement lorsque l'*entité concernée* estime que la violation fait peser un *risque grave* sur la vie privée de l'abonné (par exemple en cas de vol ou d'usurpation d'identité, d'atteinte à l'intégrité physique, d'humiliation grave ou d'atteinte à la réputation).

15. La proposition modifiée de la Commission conserve l'obligation, proposée par le PE, de notifier toutes les violations aux autorités. Toutefois, contrairement à l'approche du PE, elle prévoit une exception à l'exigence de notification aux personnes concernées lorsque le FSCEP prouve à l'autorité compétente i) qu'il y a «*raisonnablement peu de chances*» pour que ladite violation cause un préjudice (par exemple, un préjudice économique ou social ou une usurpation d'identité) ou ii) que les «*mesures de protection technologiques appropriées*» ont été appliquées aux données concernées par la violation. Ainsi, l'approche de la Commission prévoit une analyse fondée sur le préjudice liée aux notifications individuelles.

([10]) En particulier, les amendements 187, 124 à 127, ainsi que 27, 21 et 32 du PE portent sur cette question.

16. Il importe de noter que, dans le cadre des approches du PE ([11]) et de la Commission, ce sont *les autorités* qui, en définitive, sont chargées de déterminer si la violation est grave ou s'il y a des chances raisonnables pour qu'elle cause un préjudice. En revanche, dans le cadre de l'approche du Conseil, la décision incombe aux *entités concernées*.

17. Les approches du Conseil et de la Commission ne s'appliquent qu'aux seuls FSCEP, et non aux FSSI, comme celle du PE.

Définition de la violation de la sécurité

18. Le CEPD se réjouit de constater que les trois propositions législatives contiennent la même définition de la violation de la sécurité, décrite comme une «*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 [...]*». ([12])

19. Comme il est précisé ci-après, il y a lieu de se féliciter de cette définition, car elle est suffisamment générale pour englober la plupart des situations pertinentes dans lesquelles la notification des violations de la sécurité pourrait être garantie.

20. En premier lieu, la définition inclut les cas dans lesquels un tiers a eu un *accès non autorisé* à des données à caractère personnel, par exemple lors du piratage d'un serveur contenant de telles données et de la récupération d'informations de ce type.

21. En deuxième lieu, cette définition couvrirait également des situations dans lesquelles il y a eu perte ou divulgation de données à caractère personnel, sans que l'accès non autorisé n'ait encore été prouvé. Cela comprendrait notamment des situations dans lesquelles les données à caractère personnel ont été perdues (par exemple, sur des CD-Rom, des clés USB ou d'autres appareils portatifs), ou rendues publiques par des utilisateurs réguliers (fichier de données d'un employé mis temporairement et par inadvertance à la disposition du public sur internet). Comme il n'existera souvent aucune preuve d'un accès ou d'une utilisation effectifs de ces données par des tiers non autorisés à un moment donné, il semble approprié que ces cas relèvent de la définition. Par conséquent, le CEPD recommande de conserver cette définition. Il recommande en outre d'inclure la définition de la violation de la sécurité à l'article 2 de la directive «vie privée et communications électroniques», ce qui ce serait plus conforme à la structure générale de la directive et apporterait davantage de clarté.

([11]) Sauf en cas de danger imminent et direct, les entités concernées devant alors d'abord informer les consommateurs.

([12]) Article 2, point i), de la position commune du Conseil et de la proposition modifiée de la Commission et article 4, paragraphe 3, de la première lecture du PE.

Entités qui devraient être soumises à l'obligation de notification

22. Dans le cadre de l'approche du PE, l'obligation de notification s'applique à la fois aux FSCEP et aux FSSI. Par contre, dans le cadre de celles du Conseil et de la Commission, seuls les FSCEP tels que les sociétés de télécommunications et les fournisseurs d'accès internet seront tenus d'informer les intéressés qui subiront des violations de la sécurité aboutissant à une compromission de leur données à caractère personnel. D'autres secteurs d'activité, notamment les banques, détaillants et fournisseurs de services de santé en ligne ne sont pas liés par cette obligation. Pour les raisons exposées ci-après, le CEPD estime que, dans une perspective de politique publique, il est essentiel de s'assurer que les services de la société de l'information, parmi lesquels figurent notamment les entreprises en ligne, les banques en ligne et les fournisseurs de services de santé en ligne, sont également soumis à l'obligation de notification.

23. En premier lieu, le CEPD fait observer que, même si les sociétés de télécommunications sont certainement la cible de violations de sécurité qui méritent de faire l'objet d'une obligation de notification, il en va de même pour d'autres types de sociétés et de fournisseurs. Les détaillants, banques et pharmacies en ligne sont tout autant susceptibles de subir des violations de sécurité que les sociétés de télécommunications, si ce n'est davantage. Par conséquent, les considérations relatives aux risques ne pèsent pas en faveur de la limitation de l'obligation de notification des violations aux seuls FSCEP. La nécessité d'une approche plus générale est illustrée par l'expérience de pays tiers. Par exemple, aux États-Unis, la quasi-totalité des États (plus de 40 à ce stade) ont adopté des législations relatives à la notification des violations de la sécurité et dont le champ d'application est plus large, englobant non seulement les FSCEP, mais aussi toutes les entités détenant les données à caractères personnelles concernées.

24. En deuxième lieu, même si une violation de la sécurité des catégories de données à caractère personnel régulièrement traitées par les FSCEP est à l'évidence susceptible d'avoir une incidence sur la vie privée d'une personne, il en va de même, si ce n'est davantage, en ce qui concerne les catégories de données à caractère personnel traitées par les FSSI. Les banques et d'autres institutions financières sont assurément susceptibles de détenir des informations hautement confidentielles (telles que les informations relatives aux comptes bancaires), dont la divulgation peut être utilisée à des fins d'usurpation d'identité. De même, la divulgation par des services de santé en ligne d'informations très sensibles relatives à la santé est susceptible d'être particulièrement préjudiciable aux intéressés. Par conséquent, les catégories de données à caractère personnel susceptibles d'être compromises sont telles que la notification des violations de la sécurité doit aussi faire l'objet d'une application plus large prévoyant au minimum d'y assujettir les FSSI.

25. Certains arguments d'ordre juridique ont été invoqués contre l'élargissement du champ d'application de cet article, en ce qui concerne les entités assujetties à cette obligation. En particulier, le fait que les seuls FSCEP relèvent du champ d'application général de la directive «vie privée et communications électroniques» a été présenté comme un obstacle au fait d'appliquer aussi l'obligation de notification aux FSSI.

26. À cet égard, le CEPD tient à rappeler que: *i)* aucun obstacle juridique d'aucune sorte ne s'oppose à ce que d'autres entités que les FSCEP ne relèvent de certaines dispositions de la directive. Le législateur communautaire a toute latitude à cet égard; *ii)* d'autres précédents d'application à des entités autres que les FSCEP existent dans la directive «vie privée et communications électroniques» actuellement en vigueur.

27. Par exemple, l'article 13 ne s'applique pas seulement aux FSCEP mais aussi à toutes les sociétés qui effectuent des communications non sollicitées nécessitant le consentement préalable du destinataire. En outre, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», qui interdit notamment le stockage d'informations telles que des cookies dans l'équipement terminal des utilisateurs, lie non seulement les FSCEP, mais aussi toute personne qui tente de stocker des informations ou d'accéder à des informations stockés dans l'équipement terminal des intéressés. En outre, dans le cadre du processus législatif actuel, la Commission a même proposé d'étendre l'application de l'article 5, paragraphe 3, aux cas de technologies similaires (cookies/logiciels espions) fournies non seulement par le biais des systèmes de communications électroniques, mais aussi par toute autre méthode possible (distribution par téléchargement à partir d'internet ou via des supports de stockage de données externes, tels que CD-ROM, clés USB, mémoires flash, etc.) Tous ces éléments sont bienvenus et devraient être conservés, mais constituent aussi des précédents à prendre en compte dans le cadre de la discussion actuelle sur le champ d'application.

28. En outre, dans le cadre du processus législatif actuel, la Commission et le PE, et dans un certain sens le Conseil, ont proposé un nouvel article 6, paragraphe 6 *bis*, examiné ci-après, qui s'applique à d'autres entités que les FSCEP.

29. Enfin, compte tenu de l'ensemble des éléments positifs résultant de l'obligation de notification des violations de la sécurité, il est fort probable que les citoyens s'attendront à en bénéficier non seulement lorsque leurs données à caractère personnel auront été compromises par les FSCEP, mais aussi lorsqu'elles l'auront été par les FSSI. Il se peut qu'il ne soit pas répondu aux attentes des citoyens si, par exemple, ceux-ci ne sont pas informés de la perte par une banque en ligne des informations relatives à leurs comptes bancaires.

30. En résumé, le CEPD est convaincu qu'il ne sera pleinement tiré parti de l'ensemble des avantages de la notification des violations de la sécurité que si les entités relevant de la directive comprennent à la fois les FSCEP et les FSSI.

Critère de déclenchement de la notification

31. En ce qui concerne le déclenchement de la notification, le CEPD estime, comme cela est expliqué plus en détail ci-après, que le plus approprié des trois critères proposés est celui retenu dans la proposition modifiée de la Commission, selon lequel *il y a des chances raisonnables pour que la violation porte préjudice*. Toutefois, il importe de s'assurer que la définition du terme «préjudice» est suffisamment générale pour couvrir tous les cas pertinents dans lesquels la violation a des effets négatifs sur la vie privée ou d'autres intérêts légitimes des personnes. Dans le cas contraire, il serait préférable de prévoir un nouveau critère de déclenchement de l'obligation de notification *s'il y a des chances raisonnables pour que la violation ait des effets négatifs pour les personnes*.

32. Comme indiqué au point précédent, les conditions dans lesquelles la notification aux intéressés est obligatoire (ci-après dénommées «critère de déclenchement» ou «critère») varient en fonction des approches adoptées par le PE, la Commission et le Conseil. Manifestement, la quantité des notifications que recevront les intéressés dépendra, en grande partie, du critère de déclenchement fixé pour la notification.

33. Dans le cadre des approches du Conseil et de la Commission, la notification doit être adressée si la violation «*fait peser un risque grave sur la vie privée de l'abonné*» (Conseil) ou «*s'il y a des chances raisonnables pour que la violation porte préjudice au consommateur*» (Commission). Dans le cadre de l'approche du PE, le critère de déclenchement de la notification aux intéressés est «*la gravité de la violation*» (la notification n'étant exigée que si la violation est jugée «*grave*»). La notification n'est pas nécessaire en deçà de ce seuil ([13]).

34. Le CEPD estime que si des données à caractère personnel ont été compromises, on peut soutenir que les personnes auxquelles ces données appartiennent ont le droit d'en être informées dans tous les cas. Toutefois, il est tout à fait légitime de s'interroger sur la question de savoir s'il s'agit d'une bonne solution à la lumière d'autres intérêts et considérations.

35. Il a été avancé que l'obligation d'adresser des notifications dans tous les cas de compromissions de données à caractère personnel, c'est-à-dire sans aucune limitation, pourrait conduire à trop notifier et engendrer une «lassitude face aux notifications» susceptible d'aboutir à une désensibilisation. Comme cela est précisé ci-après, le CEPD est sensible à cet argument. Toutefois, il tient dans le même temps à souligner sa crainte que trop notifier ne puisse être le signe d'un échec général des pratiques en matière de sécurité de l'information.

36. Comme indiqué précédemment, le CEPD est conscient des conséquences négatives que pourrait avoir le fait de trop notifier et il souhaite contribuer à faire en sorte que le cadre juridique adopté pour la notification des violations de la sécurité n'aboutisse pas à un tel résultat. Si les personnes devaient recevoir des notifications de violations trop fréquentes, y compris dans des situations non accompagnées d'effets négatifs ni de préjudices, c'est l'un des principaux objectifs des notifications qui risquerait d'être compromis car ces personnes pourraient paradoxalement négliger de prendre en considération les notifications dans des situations où la prise de mesure de protection par celles-ci pourraient en réalité s'imposer. Il importe dès lors de parvenir à un juste équilibre permettant de veiller à ce que les notifications soient utiles car si les personnes ne réagissent pas aux notifications qu'elles reçoivent, l'efficacité des systèmes de notification s'en trouverait fortement réduite.

37. Afin d'adopter un critère approprié qui ne conduise pas à trop notifier, il convient d'examiner d'autres éléments, en plus du critère de déclenchement de la notification, notamment la définition de la violation de la sécurité et les informations relevant de l'obligation de notification. À cet égard, le CEPD fait observer que dans le cadre des trois approches proposées, la quantité des notifications est susceptible d'être élevée compte tenu de la large définition de la violation de la sécurité dont il a été question précédemment. Cette crainte de trop notifier est en outre soulignée par le fait que la définition de la violation de la sécurité englobe tous les types de données à caractère personnel. Même si le CEPD estime qu'il s'agit là de la bonne approche (c'est-à-dire consistant à ne pas limiter les types de données à caractère personnel soumises à notification), par opposition à d'autres approches comme celles de la législation américaine, dans laquelle les prescriptions mettent l'accent sur le caractère sensible des informations, il s'agit néanmoins d'un élément à prendre en compte.

38. À la lumière de ce qui précède et compte tenu des différentes variables considérées en bloc, le CEPD juge approprié d'introduire un seuil ou un critère en deçà duquel la notification n'est pas obligatoire.

39. Les deux critères proposés, à savoir le fait que la violation «*fait peser un risque grave sur la vie privée*» ou qu'«*il y a des chances raisonnables pour que la violation porte préjudice*», semblent inclurent, par exemple, les dommages sociaux, l'atteinte à la réputation et les pertes économiques. Ainsi, ces critères couvriraient des cas d'exposition à une usurpation d'identité par la divulgation d'éléments d'identification non publics, tels que des numéros de passeport, ainsi que la divulgation d'informations relatives à la vie privée d'un individu. Le CEPD accueille favorablement cette approche. Il est convaincu que les avantages de la notification des violations de la sécurité ne seraient pas pleinement atteints si le système de notification ne portait que sur des violations entraînant un préjudice économique.

([13]) Cf. note de bas de page n° 11 concernant l'exception à cette règle.

40. Parmi les deux critères proposés, le CEPD préfère celui de la Commission, selon lequel «*il y a des chances raisonnables pour que la violation porte préjudice*», car il garantirait un niveau de protection des personnes plus approprié. La probabilité pour que des violations doivent faire l'objet d'une notification est bien plus élevée s'il y a des *chances raisonnables* pour qu'elles portent *préjudice* à la vie privée d'une personne que si elles doivent faire peser un «*risque grave*» de tel préjudice. Ainsi, le fait de ne couvrir que les violations faisant peser un risque grave sur la vie privée des personnes limiterait considérablement le nombre des violations qui devraient être notifiées. Cela donnerait aux FSCEP et aux FSSI un énorme pouvoir discrétionnaire pour décider si une notification est requise, dans la mesure où il leur serait bien plus facile de justifier la conclusion selon laquelle il n'existe pas de «*risque grave*» de préjudice que la conclusion selon laquelle il y a «*raisonnablement peu de chances*» qu'un préjudice survienne. Bien qu'il convienne assurément de se garder de trop notifier, le bénéfice du doute doit, en définitive, être accordé à la protection de la vie privée des personnes, et il convient que ces dernières soient protégées au moins lorsqu'il y a des chances raisonnables pour qu'une violation leur porte préjudice. Par ailleurs, l'expression «*chances raisonnables*» sera plus efficace en pratique, tant pour les entités concernées que pour les autorités compétentes, car elle exige une évaluation objective de la situation et du contexte correspondant.

41. En outre, les violations de données à caractère personnel peuvent causer un préjudice difficile à quantifier et susceptible de varier. En effet, la divulgation d'un même type de données peut, en fonction des circonstances individuelles, entraîner un préjudice important pour une personne donnée et moins important pour une autre. Un critère qui nécessiterait un préjudice important, substantiel ou grave ne serait pas approprié. Ainsi, l'approche adoptée par le Conseil, qui exige que la violation affecte *gravement* la vie privée de la personne, lui fournirait une protection inappropriée dans la mesure où un tel critère impose que l'effet sur la vie privée soit «grave». Ce point peut également donner lieu à une évaluation subjective.

42. Bien que, comme indiqué précédemment, le critère selon lequel «*il y a des chances raisonnables pour qu'une violation porte préjudice*» semble être adapté à la notification des violations de la sécurité, le CEPD demeure néanmoins préoccupé par le fait que ce critère est susceptible de ne pas englober toutes les situations dans lesquelles la notification aux personnes est garantie, c'est-à-dire toutes les situations dans lesquelles il y a des chances raisonnables pour que la violation ait des effets négatifs sur la vie privée ou d'autres droits légitimes des personnes. C'est la raison pour laquelle on pourrait envisager un critère qui imposerait la notification «*s'il y a des chances raisonnables pour que la violation ait des effets négatifs pour les personnes*».

43. Ce critère de remplacement présente l'avantage supplémentaire d'être conforme à la législation de l'UE relative à la protection des données. En effet, la directive relative à la protection des données mentionne souvent les atteintes aux droits et libertés des personnes concernées. Par exemple, l'article 18 et le considérant 49, qui concernent l'obligation de notifier les traitements de données aux autorités chargées de la protection des données, autorisent les États membres à prévoir des dérogations à cette obligation dans les cas où les traitements de données «*ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées*». Une formulation similaire est utilisée à l'article 16, paragraphe 6, de la position commune du Conseil afin de permettre aux personnes morales d'engager des actions en justice contre les polluposteurs.

44. En outre, compte tenu de ce qui précède, il faudrait également que les entités concernées et en particulier les autorités compétentes pour faire appliquer la législation relative à la protection des données connaissent mieux le critère susmentionné, ce qui faciliterait leur évaluation visant à déterminer si une violation donnée remplit ou non le critère requis.

Entité chargée de déterminer si une violation de la sécurité remplit ou non le critère

45. Dans le cadre de l'approche du PE (les cas de danger imminent étant exceptés) et de la proposition modifiée de la Commission, il appartiendra aux autorités des États membres de déterminer si une violation de la sécurité remplit ou non le critère de déclenchement de l'obligation d'informer les personnes concernées.

46. Le CEPD estime que la participation d'une autorité joue un rôle important pour déterminer si le critère est satisfait dès lors qu'elle constitue, dans une certaine mesure, une garantie de la bonne application de la législation. Un tel système est susceptible d'empêcher les sociétés d'évaluer à tort une violation comme non préjudiciable ou non grave et d'éviter ainsi qu'elles ne s'abstiennent d'adresser une notification alors que celle-ci est, en fait, nécessaire.

47. Par ailleurs, le CEPD craint qu'un régime qui impose aux autorités de procéder à l'évaluation ne puisse poser des difficultés d'ordre pratique et être malaisé à mettre en oeuvre, ou qu'il ne puisse s'avérer contre-productif en pratique. Il se peut même qu'il réduise les garanties des intéressés en matière de protection des données.

48. En effet, dans le cadre d'une telle approche, les autorités chargées de la protection des données seraient vraisemblablement inondées de notifications de violations de la sécurité et pourraient se trouver confrontées à de graves difficultés pour procéder aux évaluations nécessaires. Il importe de garder à l'esprit que pour évaluer si une violation remplit le critère, les autorités devront être en possession d'informations d'ordre interne suffisantes, souvent de nature complexe et technique, qu'elles devront traiter très rapidement. Compte tenu de la difficulté de l'évaluation et du fait que certaines autorités disposent de ressources limitées, le CEPD craint qu'il ne leur soit très difficile de respecter cette obligation et que cela ne puisse détourner des ressources qui auraient dû être consacrées à d'autres priorités importantes. En outre, un tel système est susceptible d'exercer une pression excessive sur les autorités, car si celles-ci décident que la violation n'est pas grave et que des personnes subissent néanmoins un préjudice, lesdites autorités pourraient éventuellement en être tenues pour responsables.

49. La difficulté décrite ci-dessus est encore soulignée si l'on tient compte du fait que le temps est un facteur essentiel pour réduire les risques résultant des violations de la sécurité. À moins que les autorités ne soient en mesure de procéder à l'évaluation dans des délais très courts, le temps supplémentaire qui leur est nécessaire pour y procéder est susceptible d'accroître les préjudices subis par les personnes concernées. Par conséquent, cette mesure supplémentaire qui vise à renforcer la protection des intéressés peut paradoxalement aboutir à une moindre protection que celle offerte par les systèmes fondés sur la notification directe.

50. Pour les raisons exposées ci-dessus, le CEPD estime qu'il serait préférable d'instaurer un système selon lequel ce serait aux entités concernées d'évaluer si la violation remplit ou non le critère, comme le prévoit l'approche du Conseil.

51. Néanmoins, afin d'éviter les risques d'abus éventuel, par exemple si des entités refusent d'adresser une notification dans des circonstances où celle-ci s'impose clairement, il est de la plus haute importance d'inclure certaines garanties, décrites ci-après, en matière de protection des données.

52. En premier lieu, l'obligation s'appliquant aux entités concernées de décider si elles doivent adresser une notification doit, à l'évidence, être accompagnée d'une autre obligation impérative de notifier aux autorités toutes les violations qui remplissent le critère requis. Les entités concernées devraient dans de tels cas être tenues d'informer les autorités de la violation et des raisons de leur décision relative à la notification, ainsi que du contenu de toute notification adressée.

53. En deuxième lieu, les autorités doivent se voir attribuer un réel rôle de supervision. Dans l'exercice de ce rôle, elles doivent être autorisées, mais non obligées, à enquêter sur les circonstances de la violation et à exiger toute mesure corrective susceptible d'être appropriée ([14]). Elles devraient non seulement être autorisées à adresser des notifications aux personnes (lorsque cela n'a pas encore été fait) mais également être capables d'imposer l'obligation de prendre certaines mesures afin d'éviter la poursuite des violations. Les autorités devraient se voir attribuer des ressources et des pouvoirs effectifs à cet effet et disposer de la marge de manœuvre nécessaire pour décider du bon moment pour réagir à une notification de violation de la sécurité. En d'autres termes, cela permettrait aux autorités d'être sélectives et de mener des enquêtes concernant, par exemple, des violations de sécurité de grande ampleur et véritablement préjudiciables, en vérifiant et contrôlant le respect des prescriptions légales.

54. Pour parvenir à ce résultat, le CEPD recommande, en plus des pouvoirs reconnus par la directive «vie privée et communications électroniques» comme ceux visés à l'article 15 *bis*, paragraphe 3, et par la directive relative à la protection des données, d'insérer la disposition suivante: «*Si l'abonné ou la personne concernée n'a pas encore été informé, l'autorité nationale compétente peut, après avoir examiné la nature de la violation, demander au FSCEP ou au FSSI de le faire*».

55. En outre, le CEPD recommande au PE et au Conseil de confirmer l'obligation proposée par le PE (amendement 122, article 4, paragraphe 1 *bis*) imposant aux entités de procéder à l'évaluation et à l'identification des risques concernant leurs systèmes et les données à caractère personnel qu'elles ont l'intention de traiter. Conformément à cette obligation, les entités établiront une définition adaptée et précise des mesures de sécurité qui seront appliquées dans leur cas, et qui devraient être à la disposition des autorités. Si une violation de la sécurité survient, cette obligation aidera les entités concernées — et à terme aussi les autorités dans leur rôle de supervision — à déterminer si la compromission des informations en cause est susceptible de nuire ou de porter préjudice aux intéressés.

56. En troisième lieu, l'obligation s'appliquant aux entités concernées de décider si elles doivent adresser une notification aux personnes doit s'accompagner d'une obligation de tenir à jour une piste de vérification interne, détaillée et complète, décrivant les violations qui se sont produites, ainsi que les notifications correspondantes et les mesures prises pour éviter de futures violations. Cette piste de vérification interne doit être à la disposition des autorités en vue d'éventuels contrôles et enquêtes réalisés par ces dernières, ce qui leur permettra de remplir leur rôle de supervision. Pour ce faire, on pourrait adopter une disposition dont la teneur s'inspirerait de celle-ci: «*Les FSCEP et les FSSI conservent et tiennent à jour des registres exhaustifs décrivant en détail toutes les violations de la sécurité qui se sont produites, ainsi que les informations techniques pertinentes relatives à ces violations et les mesures correctives qui ont été prises. Les registres mentionnent également toutes les notifications adressées aux abonnés ou aux personnes concernées, ainsi qu'aux autorités nationales compétentes, en précisant leur date et leur contenu. Les registres sont présentés à l'autorité nationale compétente à sa demande*».

57. Il va de soi que, pour garantir la cohérence de la mise en œuvre de ce critère ainsi que celle d'autres aspects pertinents du cadre relatif aux violations de la sécurité, tels que le format et les procédures de notification, il serait approprié que la Commission adopte des mesures de mise en œuvre technique, après consultation du CEPD, du groupe «Article 29» et des parties concernées.

([14]) L'article 15 *bis*, paragraphe 3, reconnaît ces pouvoirs de supervision en prévoyant que «*[l]es États membres veillent à ce que les autorités nationales compétentes et, le cas échéant, d'autres organismes nationaux disposent de tous les pouvoirs d'enquête et des ressources nécessaires, et notamment de la possibilité d'obtenir toute information pertinente dont elles peuvent avoir besoin, afin de surveiller et contrôler le respect des dispositions nationales adoptées en application de la présente directive.*»

Destinataires des notifications

58. En ce qui concerne les destinataires des notifications, le CEPD préfère la terminologie utilisée par le PE et la Commission, à celle du Conseil. En effet, le PE a remplacé le terme «abonnés» par «utilisateurs». La Commission utilise les termes «abonnés» et «particulier concerné». Les formulations utilisées par le PE et la Commission feraient figurer parmi les destinataires des notifications non seulement les abonnés actuels, mais aussi les anciens abonnés et des tiers, tels que des utilisateurs qui ont des relations avec certaines entités concernées sans y être abonnés. Le CEPD se félicite de cette approche et invite le PE et le Conseil à la conserver.

59. Néanmoins, le CEPD constate un certain nombre d'incohérences dans la terminologie employée dans la première lecture du PE qu'il conviendrait de corriger. Par exemple, le terme «abonnés» a été remplacé dans la plupart des cas, mais pas toujours, par le terme «utilisateurs» et, dans d'autres cas, par le terme «consommateurs». Il conviendrait d'harmoniser ce point.

III. CHAMP D'APPLICATION DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»: RÉSEAUX PUBLICS ET PRIVÉS

60. L'article 3, paragraphe 1, de la directive «vie privée et communications électroniques» actuelle établit que celle-ci s'applique principalement aux entités (dénommés plus haut «FSCEP») qui assurent le traitement de données «*dans le cadre de*» la fourniture de services de communications électroniques accessibles au public sur les réseaux publics ([15]). Parmi les activités des FSCEP, on peut citer la fourniture d'accès à internet, la transmission d'informations par des réseaux électroniques, les connexions de téléphonie mobile ou fixe, etc.

61. Le Parlement européen a voté l'amendement 121 modifiant l'article 3 de la proposition initiale de la Commission, qui vise à élargir le champ d'application de la directive «vie privée et communications électroniques» afin d'y inclure le «*traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics et privés et sur les réseaux privés accessibles au public dans la Communauté, […]*» (article 3, paragraphe 1, de la directive «vie privée et communications électroniques»). Malheureusement, ni le Conseil ni la Commission n'ont été en mesure d'accepter cet amendement, dont l'esprit n'apparaît dès lors ni dans la position commune du Conseil, ni dans la proposition modifiée de la Commission.

Application de la directive «vie privée et communications électroniques» aux réseaux privés accessibles au public

62. Pour les raisons exposées ci-après, et afin d'aider à dégager un consensus, le CEPD préconise de conserver l'esprit de l'amendement 121. Il suggère en outre d'inclure un amendement visant à mieux préciser les types de services couverts par le champ d'application élargi.

63. Les réseaux privés permettent souvent de fournir des services de communications électroniques, tels que l'accès à internet, par un nombre de personnes indéfini potentiellement important. C'est le cas, notamment, de l'accès à internet dans les cybercafés et les points Wi-Fi des hôtels, restaurants, aéroports, trains et autres lieux accessibles au public, où il est fréquent de proposer ce type de service en plus d'autres services (boissons, hébergement, etc.).

64. Dans tous ces cas, un service de communications, ici l'accès à internet, est mis à la disposition du public non par un réseau public, mais plutôt par ce qui peut être considéré comme un réseau privé, c'est-à-dire un réseau exploité de manière privée. Par ailleurs, bien que dans les exemples cités plus haut, ce service soit proposé au public, *il est possible de soutenir que* comme le type de réseau utilisé est privé et non public, la directive «vie privée et communications électroniques» ne s'applique pas, en tout ou partie, à la fourniture de ces services ([16]). Il en découle que, dans une telle situation, les droits fondamentaux des personnes garantis par la directive «vie privée et communications électroniques» ne sont pas protégés, et que les utilisateurs accédant à internet par des moyens de télécommunications publics se trouvent dans une situation juridique différente de ceux qui ont accès à internet via des réseaux privés, et ce malgré le fait que ces différents cas de figure exposent la protection de la vie privée et des données à caractère personnel aux mêmes risques que le service soit fourni par le biais de réseaux publics ou privés. Rien ne semble donc justifier de prévoir un traitement différent au niveau de la directive selon que les services de communications soient fournis par le biais d'un réseau privé ou d'un réseau public.

65. Par conséquent le CEPD appuierait un amendement, tel que l'amendement 121 du PE, en vertu duquel la directive «vie privée et communications électroniques» s'appliquerait également au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux *privés* de communications.

66. Le CEPD est conscient, toutefois, qu'une telle formulation pourrait avoir des conséquences imprévisibles, voire indésirables. En effet, la seule mention des réseaux privés pourrait être interprétée de manière à couvrir des situations auxquelles, de toute évidence, la directive n'est pas destinée à s'appliquer. Par exemple, bien que l'amendement 121 ne prévoie pas une telle interprétation, on pourrait défendre le point de vue selon lequel une interprétation littérale ou stricte de ce texte étendrait le champ

([15]) «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]) Au contraire, on pourrait faire valoir que, bien que le réseau soit privé, le service de communications étant fourni au public, il relève du cadre juridique existant. On peut citer l'exemple de la France, où les employeurs qui mettent un accès à internet à la disposition de leurs employés ont été assimilés à des fournisseurs d'accès internet à titre commercial. Toutefois, cette interprétation n'est pas généralisée.

d'application de la directive aux propriétaires d'un bien immobilier équipé d'une installation Wi-Fi ([17]) permettant à quiconque se trouvant à portée (en principe, dans l'immeuble en question) de se connecter. Pour éviter une telle lecture, le CEPD suggère de reformuler l'amendement 121 afin d'étendre le champ d'application de la directive «vie privée et communications électroniques» au «*traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications électroniques accessibles au public sur les réseaux de communications publics ou sur les réseaux privés accessibles au public dans la Communauté,…*»

67. Une telle formulation aiderait à mettre en évidence que seuls les réseaux privés accessibles au public entreraient dans le champ d'application de la directive «vie privée et communications électroniques». Le fait de n'appliquer les dispositions de cette directive *qu'aux seuls réseaux privés accessibles au public (et non à tous les réseaux privés)*, en limite le champ d'application et garantit que ladite directive ne concernera que les services de communication fournis par des réseaux privés volontairement rendus *accessibles* au public. Cette formulation contribuera en outre à souligner que *l'accessibilité* du réseau privé au *public en général* est un élément clé (en plus de la fourniture d'un service de communications accessible au public) pour déterminer si la directive s'applique ou non. En d'autres termes et indépendamment de sa nature publique ou privée, un réseau volontairement mis à la disposition du public afin de fournir un service de communications accessible au public, comme un accès à internet, y compris si un tel service s'ajoute à un autre (par exemple, un hébergement à l'hôtel), relèverait, ainsi que ce type de service, de la directive «vie privée et communications électroniques».

68. Le CEPD note que l'approche préconisée plus haut, selon laquelle les dispositions de la directive «vie privée et communications électroniques» s'appliquent aux *réseaux privés accessibles au public* correspond aux positions adoptées dans plusieurs États membres, dont les autorités ont déjà estimé que des services de ce type, ainsi que les services fournis dans le cadre de réseaux totalement privés, relevaient des dispositions nationales mettant en œuvre la directive «vie privée et communications électroniques» ([18]).

69. Afin d'améliorer la sécurité juridique concernant les entités couvertes par le nouveau champ d'application, il peut être utile de modifier la directive «vie privée et communications électroniques» de manière à y insérer une définition des «réseaux privés accessibles au public», qui pourrait être formulée comme suit: «*par réseau privé accessible au public, on entend un réseau exploité de manière privée auquel le public en général a, d'ordinaire, un accès illimité, que ce soit moyennant paiement ou conjointement avec d'autres services ou offres, sous réserve d'acceptation des conditions applicables.*»

70. En pratique, une telle approche impliquerait que les réseaux privés des hôtels et autres établissements fournissant au public en général un accès à internet entreraient dans le champ d'application de la directive. Par contre, la fourniture de services de communications par le biais de réseaux totalement privés, dans le cadre desquels ce service est réservé à un nombre limité de personnes données, ne serait pas couverte. Par conséquent, les réseaux privés virtuels et les domiciles de consommateurs équipés d'une installation Wi-Fi, par exemple, ne relèveraient pas de la directive, pas plus que les services fournis dans le cadre de réseaux d'entreprise purement professionnels.

Application de la directive «vie privée et communications électroniques» aux réseaux privés

71. L'exclusion des réseaux privés proprement dits devrait, comme on l'a suggéré plus haut, être considérée comme une mesure provisoire dont il conviendrait de continuer à débattre. En effet, étant donné les incidences sur la protection de la vie privée de l'exclusion des réseaux purement privés en tant que tels, d'une part, et le fait qu'une telle exclusion affecte directement le grand nombre de personnes qui ont habituellement accès à internet grâce à un réseau d'entreprise, d'autre part, il sera peut-être nécessaire, à l'avenir de réexaminer cette décision. C'est pourquoi le CEPD recommande, également dans un souci d'encourager le débat sur cette question, d'insérer un considérant dans la directive «vie privée et communications électroniques» selon lequel la Commission organiserait une consultation publique sur l'application de la directive «vie privée et communications électroniques» à tous les réseaux privés, avec la participation du CEPD, des autorités chargées de la protection des données et de toutes les autres parties concernées. Ce considérant pourrait en outre préciser qu'à la suite de cette consultation publique, la Commission serait invitée à faire toute proposition utile pour étendre ou limiter le type d'entités auxquelles devraient s'appliquer la directive «vie privée et communications électroniques».

72. Par ailleurs, les différents articles de la directive «vie privée et communications électroniques» devraient être modifiés en conséquence, de manière à ce que toutes les dispositions opérationnelles mentionnent explicitement les réseaux privés accessibles au public, en plus des réseaux publics.

IV. TRAITEMENT DES DONNÉES RELATIVES AU TRAFIC À DES FINS DE SÉCURITÉ

73. Au cours de la procédure législative relative au réexamen de la directive «vie privée et communications électroniques», les entreprises fournissant des services de sécurité ont affirmé qu'il était nécessaire de prévoir, dans cette directive, une disposition rendant légitime la collecte de données relatives au trafic afin de réellement garantir la sécurité en ligne.

([17]) Par exemple, les réseaux locaux sans fil (WLAN).
([18]) Voir note de bas de page n° 16.

74. Par conséquent, le PE a introduit l'amendement 181, qui prévoit un nouvel article 6, paragraphe 6 bis, autorisant explicitement le traitement des données relatives au trafic à des fins de sécurité: «*Sans préjudice du respect des dispositions autres que celles figurant à l'article 7 de la directive 95/46/CE et à l'article 5 de la présente directive, les données relatives au trafic peuvent être traitées dans l'intérêt légitime du contrôleur de données à des fins de mise en œuvre de mesures techniques propres à garantir la sécurité des réseaux et de l'information, au sens de l'article 4, point c), du règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, d'un service public de communications électroniques, d'un réseau public ou privé de communications électroniques, d'un service de la société de l'information ou de tout équipement terminal et de communication électronique y afférent, sauf lorsque les droits fondamentaux et les libertés de la personne concernée prévalent sur ledit intérêt. Ce traitement se limite au strict nécessaire pour l'accomplissement de ce type d'action de sécurité*».

75. Dans sa proposition modifiée, la Commission a accepté le principe de cet amendement, mais a supprimé une clause essentielle pour le respect des autres dispositions de la directive, à savoir le premier membre de phrase - «*Sans préjudice […] de la présente directive*» — Le Conseil a adopté une version remaniée qui fragilise encore un peu plus les protections et l'équilibre des intérêts dont l'amendement 181 reconnaît toute l'importance, formulée comme suit: «*Les données relatives au trafic peuvent être traitées dans la mesure strictement nécessaire pour garantir la sécurité des réseaux et de l'information, au sens de l'article 4, point c), du règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.*»

76. Comme on l'expliquera ci-après, l'article 6, paragraphe 6 *bis*, est inutile et présente des risques d'utilisation abusive, en particulier s'il est adopté sous une forme ne prévoyant ni les garanties importantes, ni les clauses de respect des autres dispositions de la directive, ni l'équilibre des intérêts. Dès lors, le CEPD recommande que cet article soit rejeté, ou au moins, que l'on veille à ce que tout article relatif à cette question prévoie des garanties du type de celles contenues dans l'amendement 181 adopté par le PE.

Motifs légaux justifiant le traitement des données relatives au trafic applicables aux services de communications électroniques et aux autres responsables du traitement des données au titre de la législation actuelle en matière de protection des données

77. La mesure dans laquelle les fournisseurs de services de communications électroniques accessibles au public peuvent procéder légalement au traitement des données relatives au trafic est réglementée par l'article 6 de la directive «vie privée et communications électroniques», qui limite le traitement de ce type de données à un nombre restreint de finalités, telles la facturation, l'interconnexion et la prospection. Ce traitement ne peut avoir lieu qu'à certaines conditions, par exemple, dans le cas de la prospection, le consentement des intéressés. En outre, d'autres responsables du traitement des données, tels les fournisseurs de services de la société de l'information, peuvent traiter des données relatives au trafic en vertu de l'article 7 de la directive sur la protection des données, qui prévoit que les responsables du traitement des données peuvent procéder au traitement de données à caractère personnel à condition de respecter au moins l'une des bases juridiques énumérées, également citées comme motifs légaux.

78. À titre d'exemple d'une telle base juridique, on peut citer l'article 7, point a), de la directive sur la protection des données, qui requiert le consentement de la personne concernée. Ainsi, si un détaillant en ligne souhaite procéder au traitement de données relatives au trafic à des fins d'envoi publicitaire ou de prospection, il doit obtenir le consentement de la personne concernée. Une autre base juridique citée à l'article 7 permet, dans certains cas, le traitement de données relatives au trafic à des fins de sécurité par, entre autres, des entreprises fournissant des services de sécurité. Le fondement en est l'article 7, point f), qui établit que les responsables des données peuvent effectuer le traitement de données à caractère personnel si ce traitement est «*nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée […]*». La directive sur la protection de la vie privée ne précise pas dans quels cas le traitement de données à caractère personnel répond à cette exigence. Ce sont donc les responsables du traitement des données qui prennent la décision, au cas par cas et souvent avec l'accord des autorités nationales chargées de la protection des données et d'autres autorités compétentes.

79. Il conviendrait d'examiner l'action conjuguée de l'article 7 de la directive sur la protection de la vie privée et de la proposition d'article 6, paragraphe 6 *bis*, de la directive «vie privée et communications électroniques». L'article 6, paragraphe 6 *bis*, proposé précise dans quelles situations les exigences énoncées à l'article 7, point f), décrites plus haut seraient respectées. En effet, en autorisant le traitement des données relatives au trafic afin de garantir la sécurité des réseaux et de l'information, l'article 6, paragraphe 6 *bis*, permet un tel traitement pour la réalisation de l'intérêt légitime poursuivi par le responsable du traitement des données.

80. Comme le CEPD l'explique ci-après, il estime que l'article 6, paragraphe 6 *bis*, proposé n'est ni nécessaire ni utile. En effet, d'un point de vue juridique, il est en principe inutile d'établir si un type particulier de traitement des données, dans ce cas-ci, le traitement des données relatives au trafic à des fins de sécurité, est conforme ou non aux exigences de l'article 7, point f), de la directive sur la protection de la vie privée, auquel cas le consentement de l'intéressé pourrait être requis en vertu de l'article 7, point a). Comme on l'a fait remarquer plus haut, ce sont généralement les responsables du traitement des données — c'est-à-dire les entreprises — qui décident si tel est le cas, au moment de la mise en œuvre, en consultation avec les autorités chargées de la protection des données, et s'il y a lieu, avec les tribunaux. De manière générale, le CEPD est d'avis que dans certains cas, le traitement légitime des données relatives au trafic à des fins de sécurité,

effectué sans mettre en péril les droits et libertés fondamentaux des intéressés, est susceptible de respecter les exigences de l'article 7, point f), de la directive sur la protection des données, et peut dès lors être effectué. En outre, la directive sur la protection des données et la directive «vie privée et communications électroniques» ne prévoient aucun précédent d'exception ou de traitement particulier pour certains types de traitement des données qui satisferaient aux exigences de l'article 7, point f), et la nécessité de ce genre d'exception n'a pas non plus été démontrée. En revanche, comme on l'a observé plus haut, il apparaît que dans de nombreuses situations, ce type d'activité serait amplement couvert par le texte actuel. Par conséquent, une disposition légale confirmant cette évaluation est en principe inutile.

Différentes versions de l'article 6, paragraphe 6 bis, présentées par le PE, le Conseil et la Commission

81. Comme expliqué plus haut, bien que l'amendement 181 soit inutile, il importe de souligner que, dans la formulation adoptée par le PE, il a néanmoins été rédigé pour, d'une certaine manière, tenir compte des principes de protection de la vie privée et des données inscrits dans la législation relative à la protection des données. Cet amendement pourrait également porter sur la protection des données et l'intérêt de la vie privée, par exemple, si l'on y faisait figurer les termes «dans certains cas», afin de garantir l'application sélective de cet article, ou si l'on y prévoyait une période de conservation des données précise.

82. L'amendement 181 comporte des éléments positifs. Il confirme que le traitement devrait respecter tous les autres principes de protection des données applicables au traitement des données à caractère personnel («*Sans préjudice du respect des dispositions […] de la directive 95/46/CE et […] de la présente directive*»). Par ailleurs, bien que cet amendement autorise le traitement de données relatives au trafic à des fins de sécurité, il parvient à assurer un équilibre entre les intérêts de l'entité qui effectue le traitement de ces données et ceux des personnes concernées, de telle manière que le traitement des données ne puisse avoir lieu que si les libertés et droits fondamentaux des intéressés ne sont pas bafoués par ceux de l'entité qui effectue le traitement des données («*sauf lorsque les droits fondamentaux et les libertés de la personne concernée prévalent sur ledit intérêt*»). Cette exigence est essentielle dans la mesure où elle peut permettre de traiter les données relatives au trafic dans certains cas particuliers, sans toutefois autoriser une entité à procéder au traitement de ces données en masse.

83. Dans sa version remaniée par le Conseil, cet amendement comporte des éléments dignes d'intérêt, par exemple le fait de conserver les termes «*strict nécessaire*» qui limitent le champ d'application de cet article. Cependant, la version du Conseil supprime les garanties visées plus haut en matière de protection de la vie privée et des données. Alors qu'en principe, les dispositions générales en matière de protection des données s'appliquent, qu'une mention spécifique soit faite dans chaque cas ou non, la version du Conseil peut néanmoins être interprétée comme donnant aux entités tout pouvoir discrétionnaire de procéder au traitement de données relatives au trafic sans avoir à respecter les garanties en matière de protection des données et de la vie privée qui s'appliquent chaque fois que des données relatives au trafic sont traitées. Dès lors, on peut affirmer que les données relatives au trafic pourraient être collectées, conservées et utilisées par la suite sans qu'il faille respecter les principes de protection des données et les obligations particulières qui s'appliquent par ailleurs aux parties responsables, comme le principe de qualité ou l'obligation de procéder à un traitement licite et loyal et d'assurer la confidentialité et la sécurité des données. De plus, comme cet article ne fait aucune mention des principes de protection des données applicables qui imposent des délais de conservation des informations ou des délais spécifiques, la version du Conseil pourrait être interprétée comme permettant la collecte et le traitement des données relatives au trafic à des fins de sécurité pour une période illimitée.

84. En outre, le Conseil a fragilisé les protections de la vie privée qui figuraient dans certaines parties du texte en donnant une portée potentiellement plus large à la formulation. Par exemple, la référence à «*l'intérêt légitime du contrôleur des données*» a été supprimée, ce qui sème le doute sur le type d'entité qui pourrait se prévaloir de cette exception. Il est crucial d'éviter que n'importe quel utilisateur ou n'importe quelle entité juridique ne puisse tirer parti de cet amendement.

85. Ce qui s'est passé récemment au PE et au Conseil montre qu'il est difficile de définir juridiquement dans quelle mesure et à quelles conditions le traitement des données à des fins de sécurité peut être effectué légalement. Aucun article, actuel ou futur, ne semble susceptible d'éliminer les risques évidents d'une interprétation excessivement large de l'exception pour des raisons autres que purement liées à la sécurité ou par des entités qui ne devraient pas pouvoir en bénéficier. Il ne s'agit pas d'en conclure qu'un tel traitement est interdit dans tous les cas. Toutefois, il semble préférable que l'opportunité et les limites d'un tel traitement soient évaluées au niveau de la mise en œuvre. Les entités qui souhaitent procéder à de tels traitements devraient en examiner la portée et les conditions avec les autorités chargées de la protection des données, et éventuellement, avec le groupe «Article 29». Sinon, la directive «vie privée et communications électroniques» pourrait prévoir un article permettant le traitement des données relatives au trafic à des fins de sécurité sous réserve d'une autorisation expresse des autorités chargées de la protection des données.

86. Compte tenu, d'une part, des risques que présente l'article 6, paragraphe 6 bis, pour le droit fondamental à la protection des données et de la vie privée des personnes, et d'autre part, du fait que, comme on l'a expliqué dans le présent avis, cet article est inutile d'un point de vue juridique, le CEPD conclut que la meilleure solution serait la suppression pure et simple de l'article 6, paragraphe 6 *bis*, proposé.

87. Si un texte dans l'esprit d'une des versions actuelles de l'article 6, paragraphe 6 bis, est adopté contre l'avis du CEPD, il devrait en tout cas prévoir les garanties en matière de protection des données dont il a été question plus haut. Ce texte devrait en outre être correctement inséré dans la structure actuelle de l'article 6, de préférence sous la forme d'un nouveau paragraphe 2 *bis*.

V. **CAPACITÉ DES PERSONNES MORALES À INTENTER UNE ACTION EN JUSTICE EN RÉPONSE À DES VIOLATIONS DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»**

88. Le PE a voté l'amendement 133 permettant aux fournisseurs d'accès internet et aux autres entités juridiques, telles les associations de consommateurs, d'intenter des actions en justice en cas de violation des dispositions de la directive «vie privée et communications électroniques» ([19]). Malheureusement, ni la Commission, ni le Conseil ne l'ont accepté. Le CEPD considère que cet amendement est très positif et recommande de le conserver.

89. Pour bien saisir l'importance de cet amendement, il faut comprendre que dans le domaine de la protection de la vie privée et des données, le préjudice subi par une personne donnée ne suffit généralement pas à pousser celle-ci à faire appel aux tribunaux. La plupart du temps, les personnes concernées n'intentent pas d'action en justice de leur propre initiative après avoir reçu des pourriels ou vu leur nom inclus à tort dans un fichier. Cet amendement permettrait aux associations de consommateurs et aux syndicats qui défendent les intérêts des consommateurs à un niveau collectif d'intenter une action en justice en leur nom. Une plus grande diversité de mécanismes répressifs pourrait aussi favoriser un meilleur niveau de respect et donc être dans l'intérêt d'une application efficace et effective des dispositions de la directive «vie privée et communications électroniques».

90. Il existe des précédents juridiques dans les cadres législatifs de certains États membres qui prévoient déjà la possibilité d'un recours collectif afin de permettre aux consommateurs ou aux groupes d'intérêt de réclamer des dommages à la partie responsable du préjudice.

91. De plus, dans certains États membres, le droit de la concurrence ([20]) autorise les consommateurs, les groupes d'intérêt, outre le *concurrent concerné*, à intenter une action en justice à l'encontre de l'entité qui commet l'infraction. Une telle approche se justifie par le risque de voir les compagnies violant le droit de la concurrence profiter de ce que les consommateurs qui ne subissent que des dommages marginaux sont en général peu disposés à engager des poursuites. Ce raisonnement peut s'appliquer, mutatis mutandis, au domaine de la protection des données et de la vie privée.

92. Plus important encore, permettre, comme on l'a mentionné plus haut, à des entités juridiques, telles les associations de consommateurs et les FSCEP, d'intenter une action en justice renforce la position des consommateurs et favorise le respect général de la législation sur la protection des données. Si le risque de poursuites judiciaires est plus élevé pour les compagnies qui violent le droit, il est probable que celles-ci investiront davantage pour se conformer la législation relative à la protection des données, ce qui à long terme améliorera le niveau de protection de la vie privée et des consommateurs. Pour toutes ces raisons, le CEPD invite le PE et le Conseil à adopter une disposition permettant aux entités juridiques de poursuivre en justice toute infraction aux dispositions de la directive «vie privée et communications électroniques».

([19]) Article 13, paragraphe 6, de la première lecture du PE.

([20]) Voir, par exemple, le paragraphe 8 de la LCD - Loi fédérale allemande sur la répression de la concurrence déloyale.

VI. **CONCLUSION**

93. La position commune du Conseil, la première lecture du PE et la proposition modifiée de la Commission comportent, à des degrés divers, des éléments positifs qui pourraient renforcer la protection de la vie privée des personnes et de leurs données à caractère personnel.

94. Le CEPD estime toutefois qu'il est possible d'améliorer ces textes, notamment la position commune du Conseil, qui n'a malheureusement pas conservé certains amendements du PE visant à garantir une protection adéquate de la vie privée et des données à caractère personnel. Le CEPD engage le PE et le Conseil à rétablir les garanties en matière de protection de la vie privée qui figuraient dans la première lecture du PE.

95. Par ailleurs, le CEPD est d'avis qu'il serait opportun de simplifier certaines dispositions de la directive. Il considère, en particulier, que les dispositions portant sur la notification des violations de la sécurité ne porteront tous leurs fruits que si le cadre législatif est correctement mis en place dès le départ. Enfin, selon le CEPD, il conviendrait d'améliorer et de clarifier la formulation de certaines dispositions de la directive.

96. Au vu de ce qui précède, le CEPD engage le PE et le Conseil à mettre davantage en œuvre pour améliorer et clarifier certaines dispositions de la directive «vie privée et communications électroniques» tout en rétablissant les amendements adoptés par le PE en première lecture visant à garantir un niveau approprié de protection de la vie privée et des données. À cette fin, les points 97 à 100 figurant ci-après résument les problèmes qui se posent et avancent certaines recommandations et propositions de libellés. Le CEPD invite toutes les parties concernées à en tenir compte au cours du processus menant à l'adoption de la directive «vie privée et communication électroniques».

Violation de la sécurité

97. Le PE, la Commission et le Conseil n'ont pas adopté la même approche en matière de notification des violations de la sécurité. Les trois systèmes présentent des différences notamment pour ce qui est des entités concernées par l'obligation de notification, le critère de déclenchement de l'obligation de notification, les personnes concernées destinataires de la notification etc. Le PE et le Conseil doivent s'efforcer d'établir un cadre législatif solide pour lutter contre les violations de la sécurité. À cette fin, le PE et le Conseil devraient:

— *Conserver* la définition de la violation de la sécurité dans les textes du PE, du Conseil et de la Commission, celle-ci étant suffisamment générale pour être appliquée à la plupart des situations pertinentes qui justifieraient la notification d'une violation de la sécurité.

— En ce qui concerne les entités auxquelles s'appliquera l'obligation de notification proposée, *inclure* les fournisseurs de services de la société de l'information. Les détaillants, banques et pharmacies en ligne sont tout autant susceptibles de subir des violations de sécurité que les sociétés de télécommunication, si ce n'est davantage. Les citoyens ne s'attendront pas seulement à recevoir une notification lorsque les fournisseurs d'accès à internet sont exposés à une violation de la sécurité, mais aussi en particulier lorsque c'est leur banque ou leur pharmacie en ligne qui est touchée.

— En ce qui concerne le déclenchement de la notification, le critère retenu dans la proposition modifiée de la Commission, selon lequel «*il y a des chances raisonnables pour que la violation porte préjudice*», est un critère approprié qui assure un bon fonctionnement du système. Toutefois, il importe de s'assurer que la définition du terme «préjudice» est suffisamment générale pour couvrir tous les cas pertinents dans lesquels la violation a des effets négatifs sur la vie privée ou d'autres intérêts légitimes des personnes. Dans le cas contraire, il serait préférable de prévoir un nouveau critère de déclenchement de l'obligation de notification «*s'il y a des chances raisonnables pour que la violation ait des effets négatifs pour les personnes*». L'approche adoptée par le Conseil, qui exige que la violation affecte *gravement* la vie privée de la personne, lui fournirait une protection inappropriée dans la mesure où un tel critère impose que l'effet sur la vie privée soit «grave». Ce point peut également donner lieu à une évaluation subjective.

— Bien que la participation d'une autorité pour déterminer si une entité concernée doit notifier des personnes est en soi positive, il se peut qu'une telle solution pose des difficultés d'ordre pratique et soit malaisée à mettre en œuvre, et qu'elle détourne des ressources qui auraient dû être consacrées à d'autres priorités importantes. Si les autorités ne sont pas en mesure de réagir très rapidement, le CEPD craint qu'un tel système ne diminue en fait le niveau de protection des personnes et qu'il ne soit susceptible d'exercer une pression excessive sur les autorités. Par conséquent, d'une manière générale, le CEPD conseille d'*instaurer* un système selon lequel ce serait aux entités concernées d'évaluer si elles doivent ou non notifier les personnes.

— Afin de permettre aux autorités de superviser les évaluations effectuées par les entités couvertes par la directive concernant la nécessité d'adresser ou non une notification, il convient de *mettre en œuvre* les garanties suivantes:

  — *veiller* à ce que ces entités soient obligées de notifier aux autorités toutes les violations qui remplissent le critère requis;

  — *attribuer* aux autorités un rôle de supervision qui leur permette d'être sélectives pour être efficaces; pour parvenir à ce résultat, insérer la disposition suivante: «*Si l'abonné ou la personne concernée n'a pas encore été informé, l'autorité nationale compétente peut, après avoir examiné la nature de la violation, demander au FSCEP ou au FSSI de le faire*»;

  — *adopter* une nouvelle disposition obligeant les entités à tenir à jour une piste de vérification interne, détaillée et complète. Pour ce faire, le texte suivant pourrait être adopté: «*Les FSCEP et les FSSI conservent et tiennent à jour des registres exhaustifs décrivant en détail toutes les violations de la sécurité qui se sont produites, ainsi que les informations techniques pertinentes relatives à ces violations et les mesures correctives qui ont été prises. Les registres mentionnent également toutes les notifications adressées aux abonnés ou aux personnes concernées, ainsi qu'aux autorités nationales compétentes, en précisant leur date et leur contenu. Les registres sont présentés à l'autorité nationale compétente à sa demande.*»

— Pour garantir la cohérence de la mise en œuvre du cadre relatif aux violations de la sécurité, *donner* à la Commission la possibilité d'adopter des mesures de mise en œuvre technique, après consultation préalable du CEPD, du groupe «Article 29» et des autres parties concernées.

— En ce qui concerne les destinataires des notifications, *utiliser* les termes «particuliers concernés» ou «utilisateurs concernés», préconisés par la Commission ou le PE, car ces termes incluent toutes les personnes dont les données personnelles ont été compromises.

Réseaux privés accessibles au public

98. Les services de communication sont souvent mis à la disposition du public non par le biais de réseaux publics, mais au moyen de réseaux exploités de manière privée (par exemple, les accès Wi-Fi des hôtels ou des aéroports), dont on peut soutenir qu'ils ne sont pas couverts par la directive. Le PE a adopté l'amendement 121 (article 3) élargissant le champ d'application de la directive pour y inclure les réseaux de communication publics et privés, ainsi que les réseaux privés accessibles au public. À cette fin, le PE et le Conseil devraient:

— *conserver* l'esprit de l'amendement 121, mais en*reformuler le texte* de manière à n'inclure dans le champ d'application de la directive «vie privée et communications électroniques» que le «*traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications électroniques accessibles au public sur les réseaux de communications publics ou sur les réseaux privés accessibles au public dans la Communauté*». Les réseaux purement privés (à l'inverse des réseaux privés accessibles au public) ne seraient pas explicitement couverts par la directive;

— *modifier* en ce sens toutes les dispositions opérationnelles de manière à ce qu'elles fassent explicitement référence, non seulement aux réseaux publics, mais aussi aux réseaux privés accessibles au public;

— *insérer* une définition formulée comme suit: «*par réseau privé accessible au public, on entend un réseau exploité de manière privée auquel le public en général a, d'ordinaire, un accès illimité, que ce soit moyennant paiement ou conjointement avec d'autres services ou offres, sous réserve d'acceptation des conditions applicables*». Une telle définition améliorera la sécurité juridique en ce qui concerne les entités relevant du nouveau champ d'application;

— *adopter* un nouveau considérant en vertu duquel la Commission organiserait une consultation publique sur l'application de la directive «vie privée et communications électroniques» à tous les réseaux privés, avec la participation du CEPD, du groupe «Article 29» et d'autres parties concernées. Ce considérant pourrait en outre préciser qu'à la suite de cette consultation publique, la Commission serait invitée à faire toute proposition utile pour étendre ou limiter le type d'entités auxquelles devraient s'appliquer la directive «vie privée et communications électroniques».

Traitement des données relatives au trafic à des fins de sécurité

99. Le PE a adopté en première lecture l'amendement 181 (article 6, paragraphe 6 *bis*) qui autorise le traitement des données relatives au trafic à des fins de sécurité. La position commune du Conseil en a adopté une nouvelle version qui affaiblit certaines des garanties en matière de protection de la vie privée. À cet égard, le CEPD recommande au PE et au Conseil:

— *de rejeter* cet article dans sa totalité, car il est inutile et risquerait, en cas d'utilisation abusive, de mettre inutilement en péril la protection des données et de la vie privée des personnes;

— toutefois, si une variante de la version actuelle de l'article 6, paragraphe 6 *bis*, devait être adoptée, de *prévoir* les garanties en matière de protection des données examinées dans le présent avis (semblables à celles qui figurent dans l'amendement du PE).

Recours en cas de violation de la directive «vie privée et communications électroniques»

100. Le PE a adopté l'amendement 133 (article 13, paragraphe 6) permettant aux entités juridiques d'intenter une action en justice en cas d'infraction aux dispositions de la directive. Malheureusement, le Conseil n'a pas conservé cet amendement. Le Conseil et le PE devraient:

— *adopter* la disposition permettant aux entités juridiques, telles les associations de consommateurs et les associations commerciales, d'intenter des actions en justice en cas de violation des dispositions de la directive (et non seulement en cas de violation des dispositions contre le pourriel, comme le préconisent la position commune du Conseil et la proposition modifiée de la Commission); une plus grande diversité de mécanismes répressifs favorisera un meilleur niveau de respect et d'application effective des dispositions de la directive «vie privée et communications électronique» dans son ensemble.

Défis à relever

101. Pour toutes les questions ci-dessus, le PE et le Conseil doivent relever le défi qui consiste à définir des règles et des dispositions adéquates, qui soient pratiques, opérationnelles, et respectueuses des droits en matière de vie privée des personnes et de protection des données. Le CEPD a bon espoir que les parties concernées mettront tout en œuvre pour relever ce défi et que le présent avis contribuera utilement à la réalisation de cette tâche.

Fait à Bruxelles, le 9 janvier 2009,

Peter HUSTINX

Contrôleur européen de la protection des données