GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

01611/06/FR
WP 126

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 de communication électroniques

Adopté le

26 septembre 2006

Ce groupe de travail a été créé en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la Direction C (Justice civile, Droits fondamentaux et citoyenneté) de la Commission européenne, Direction générale Justice, Liberté et Sécurité de la Commission européenne, B-1049 Bruxelles, Belgique, Bureau N° LX-46 01/43.

Site internet: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

créé par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de ladite directive et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002,

vu le règlement intérieur du groupe de travail, et notamment ses articles 12 et 14,

adopte le présent avis:

1. Cadre général

La Commission européenne a adopté une communication sur le réexamen du cadre réglementaire européen pour les réseaux et services de communications électroniques [SEC (2006) 816] [SEC (2006) 817] le 29 juin 2006. Cette communication décrit le fonctionnement des cinq directives qui constituent le cadre réglementaire pour les réseaux et services de communications électroniques[1], explique comment le cadre réglementaire a atteint ses objectifs et identifie les domaines auxquels des changements pourraient être apportés.

Cette communication est complétée par un document de travail des services de la Commission [COM (2006) 334 final] mettant en œuvre les propositions de changements. Préalablement aux conclusions établies dans la communication, l'analyse d'impact associée reproduit l'éventail plus large des options considérées. Les documents susmentionnés ont initié le lancement d'une consultation publique sur l'avenir du cadre réglementaire pour les communications électroniques. Les commentaires à ce sujet doivent être communiqués pour le 27 octobre 2006 au plus tard.

L'étape suivante consistera, pour la Commission, à formuler des propositions législatives afin de modifier le cadre réglementaire, tout en prenant en compte les commentaires reçus. Ces propositions législatives seront ensuite présentées au Parlement et au Conseil.

Le réexamen couvre notamment la directive sur la protection de la vie privée, qui fait partie du paquet sur les communications électroniques. "L'Article 29" (le groupe de travail) souhaite contribuer comme suit à la consultation publique, en mettant l'accent en particulier sur la directive sur la protection de la vie privée.

2. Commentaires généraux

Les principales préoccupations du groupe de travail concernent le traitement des données à caractère personnel sur et via les communications électroniques, ainsi que leur sécurité, car ce traitement soulève un certain nombre de problèmes en matière de protection des données, que le groupe de travail tient à aborder dans le présent avis.

[1] Directives 19/2002/CE, JO L 108 du 24.4.2002, p.7, 20/2002/CE, JO L 108 du 24.4.2002 p. 21, 21/2002/CE, JO L 108 du 24.4.2002, p. 33, 22/2002/CE, JO L 108 du 24.4.2002, p. 51, et 58/2002/CE, JO L 201 du 31.7.2002, p. 37

Tout en évaluant la communication, et en particulier la directive sur la protection de la vie privée et les modifications susceptibles d'y être apportées, le groupe de travail tient à se référer à son avis 7/2000 sur la proposition, présentée par la Commission, de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[2]. Diverses propositions émises dans cet avis n'ont cependant pas été reprises et le groupe de travail souhaite par conséquent les énumérer à nouveau:

(1) Dans l'avis précité, le groupe de travail a mis l'accent sur le fait que les dispositions de la directive sur la protection de la vie privée ne s'appliquent qu'à la fourniture de services de communications électroniques accessibles au public au sein de réseaux de communication publics, ce qu'il trouve regrettable, car les réseaux privés revêtent une importance croissante dans la vie de tous les jours, avec des risques qui augmentent en conséquence, notamment parce que ces réseaux deviennent plus spécifiques (par exemple, surveillance du comportement des salariés au moyen de données relatives au trafic). Une autre évolution qui incite à revoir la portée de la directive est la tendance de plus en plus marquée des services à devenir à la fois privés et publics.

(2) Le groupe de travail remarque que les définitions des expressions «services de communications électroniques» et «fournir un réseau de communications électroniques» ne sont toujours pas claires et que ces deux expressions devraient être expliquées plus amplement, afin que les responsables du traitement des données, ainsi que les utilisateurs puissent disposer d'une interprétation claire et sans ambiguïté. L'absence de définitions claires de ces expressions soulève plusieurs questions, par exemple: «Un cybercafé peut-il être considéré comme un fournisseur de réseau de communications électroniques?» Il devrait être facile de répondre à ce type de questions, mais cela n'est pas toujours le cas.

(3) De plus, le groupe de travail s'est référé, dans son avis précédent 7/2000, au considérant 25 de la directive sur la protection de la vie privée, concernant l'utilisation des témoins de connexion (cookies). Celui-ci indique que les utilisateurs devraient avoir la possibilité de refuser qu'un témoin de connexion soit placé sur leur ordinateur personnel. Le groupe de travail a soutenu pleinement ce point de vue. Cependant, il est stipulé au dernier alinéa du considérant 25 que l'accès au contenu d'un site spécifique peut être subordonné au fait d'accepter l'installation d'un témoin de connexion, ce qui peut néanmoins être contradictoire avec la position selon laquelle les utilisateurs devraient pouvoir refuser qu'un témoin de connexion soit placé sur leur ordinateur personnel. Cet alinéa pourrait donc nécessiter une clarification ou une modification.

3. Commentaires particuliers concernant divers points

Document de travail, point 5.8 - Amélioration des mécanismes d'application dans le cadre existant

Ce point concerne la nécessité d'ajuster les mécanismes et les prérogatives de contrôle dont disposent les autorités qui mettent en œuvre la directive sur la protection de la vie privée.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36fr.pdf

Le document indique que les sanctions appliquées en cas d'infraction aux dispositions réglementaires se sont révélées inadaptées: *«les amendes pour infraction à la directive sur la protection de la vie privée sont trop légères et leur application est inégale.»*

Il est possible que les variations perçues dans les niveaux d'application ne soient pas dues aux dispositions de la directive sur la protection de la vie privée, mais aux différences de transposition dans les législations nationales. Par exemple, les États membres ont adopté différentes interprétations de l'article 13, paragraphe 2, ainsi que différentes sanctions maximales en cas d'infraction à cette directive.

À cet égard, même si des sanctions plus importantes et harmonisées pourraient se révéler plus dissuasives, elles ne suffisent pas pour remédier aux inégalités d'application perçues. De plus, ce ne sont pas forcément les sanctions disponibles qui déterminent la fréquence avec laquelle les contrôles sont exercés. La nature de ces prérogatives et les mécanismes par lesquels elles sont exercées pourraient constituer un facteur plus important.

Dans certains États membres, les autorités chargées de la protection des données ont des pouvoirs d'investigation limités, qui peuvent par exemple ne pas leur donner un droit d'accès aux données de communication permettant d'établir des preuves d'infractions à la directive.

Si, dans plusieurs États membres, les prérogatives de contrôle actuelles ne permettent pas aux régulateurs d'agir rapidement, il convient de remédier à ce problème. Le fait que de nombreux «spammeurs» soient exclus de la juridiction des autorités de l'Union européenne représente une difficulté supplémentaire pour le contrôle de l'application. Cette question devrait cependant être réglée grâce à une coopération étroite avec les régulateurs dans d'autres pays.

En ce qui concerne le droit de recours explicite contre les «spammeurs» mentionné dans le document de travail, il est difficile de comprendre en quoi cela diffère de la situation actuelle, où l'autorité concernée peut prendre des mesures répressives en cas d'infraction à la directive en vigueur.

Document de travail, point 7 - Sécurité

Ce point contient une proposition clé visant à étendre et à renforcer les dispositions en matière de sécurité. Les dispositions de la directive sur la protection de la vie privée et celles de la directive «service universel» seront rassemblées en un seul chapitre de la directive-cadre consacrée aux dispositions en matière de sécurité.

Si le renforcement des dispositions en matière de sécurité peut être avantageux pour les intérêts privés des consommateurs, il est difficile de voir quels seraient les effets positifs liés à la rédaction d'un chapitre spécifique hybride. On pourrait en effet alléguer que, comme le dit le document de travail, la suppression des dispositions en matière de sécurité de la directive sur la protection de la vie privée, loin de mettre en exergue l'importance de cette question, reviendrait à dire que la sécurité concerne simplement les réseaux, la concurrence et les fournisseurs de réseaux, alors qu'en réalité, elle couvre également la protection du droit fondamental à la protection de la vie privée, tel qu'exprimé dans la directive sur la protection de la vie privée.

Le groupe de travail souhaite ajouter que, au lieu de traiter la «sécurité» dans son sens le plus large, l'attention devrait être portée sur certains aspects spécifiques de la sécurité; non seulement la «continuité» et la «confidentialité», mais également l'«intégrité» des données, notamment en ce qui concerne les questions relatives au conflit entre authentification et anonymat. Etant donné qu'un manque de procédures d'authentification appropriées pourrait mener à la création de systèmes de fraude et réduire la confiance des utilisateurs à l'égard des communications électroniques, une sous-section («Fraude sur l'identité») pourrait être ajoutée à l'introduction du chapitre 7. Cette sous-section pourrait faire valoir que, tant la confidentialité que l'effacement rapide des données personnelles devenues inutiles, contribuent à la prévention de l'usurpation d'identité.

Cependant, lorsqu'il s'agit de résoudre ces questions d'authentification, il faut garder à l'esprit que, en principe, les particuliers doivent pouvoir faire usage des services publics en ligne de manière anonyme. C'est pourquoi il est nécessaire d'analyser de manière exhaustive l'accessibilité des services en ligne, avant de mettre en œuvre toute proposition ou toute modification relative à l'authentification, étant donné que la communication gratuite est essentielle. Cette analyse pourrait montrer que différents types de fraudes seront neutralisés grâce à la demande d'authentification auprès des fournisseurs de services. Des recherches dans ce secteur seraient les bienvenues.

Document de travail, point 7.1 - Obligations de prendre des mesures de sécurité, et de définir les prérogatives des ARN pour déterminer et contrôler la mise en œuvre technique

Ce point met en avant l'idée que le cadre actuel laisse trop d'espace aux fournisseurs de services pour évaluer le caractère approprié de leurs propres mesures de sécurité. Compte tenu des menaces accrues qui pèsent sur la sécurité, le document propose d'éclaircir les termes utilisés à l'article 4 de la directive sur la protection de la vie privée, en vue d'accroître l'efficacité des mesures de sécurité.

Cet éclaircissement prendrait la forme d'obligations nouvelles, telles que, des mesures permettant de résoudre les incidents liés à la sécurité, la nécessité de respecter les orientations établies par les régulateurs, des dispositions contractuelles informant les consommateurs des mesures à prendre en cas d'infraction aux règles de sécurité.

Premièrement, il est difficile de voir en quoi les propositions susmentionnées compléteraient en quelque point que ce soit le cadre existant, autrement qu'en codifiant ce que la plupart des régulateurs considèrent comme déjà en place. Il est peu probable, par exemple, qu'un régulateur continue de penser qu'un fournisseur de service dont les mesures de sécurité ne comprennent aucune procédure permettant de gérer les incidents de sécurité et de minimiser l'impact sur les consommateurs respecte la directive sur la protection de la vie privée.

Deuxièmement, le fait qu'un fournisseur de services ignore les orientations du régulateur devrait déjà permettre de déterminer dans une certaine mesure si ce fournisseur a enfreint l'article 4 de la directive sur la protection de la vie privée. Il est de ce fait difficile de voir comment le fait d'obliger les fournisseurs à suivre ces orientations irait au-delà d'une approche réglementaire responsable à l'égard des dispositions en vigueur.

Troisièmement, il est difficile de comprendre comment des dispositions contractuelles informant les clients des actions qu'ils peuvent entreprendre dans le cas d'une infraction à la sécurité représenteraient davantage qu'un simple exercice cosmétique.

En ordonnant de telles dispositions, les propositions risquent également d'alourdir le poids de la réglementation, non seulement pour le secteur mais aussi pour le régulateur. En raison de la nature du secteur, les autorités chargées de la protection des données ne peuvent énoncer les dispositions en matière de sécurité sous forme d'instructions contraignantes. Les mesures doivent être spécifiques au secteur en cause, car elles changent trop souvent pour permettre à une autorité de contrôler entièrement le secteur. Il existe bien sûr aussi de très nombreux experts spécialisés en matière de sécurité, qui sont mieux à même de donner des avis et d'effectuer des audits.

Des instructions plus claires et contraignantes devraient provenir d'une autorité spécifique au secteur plutôt que de spécialistes de la protection des données. Comme l'indique le document de travail lui-même (note de bas de page n° 30), il est également important d'éviter toute règlementation assez lourde: *«la gestion de la sécurité demande de voir au-delà des règlementations.»*

Document de travail, point 7.2 - Notification des infractions à la sécurité par les opérateurs de réseaux et les fournisseurs de services Internet

Eu égard aux commentaires qui précèdent, le groupe de travail approuve la proposition consistant à exiger une notification des infractions en matière de sécurité; cependant, il est important de souligner que la communication n'envisage aucune sanction dans le cas où un opérateur de réseau ou un fournisseur d'accès à Internet omet d'informer l'autorité chargée de la protection des données.

Le groupe de travail prévoit également que le secteur pourrait craindre que cela ressemble à un «traitement spécial» destiné à un secteur spécifique, tandis que d'autres n'ont aucune obligation de notification. Néanmoins, le groupe reconnaît que de telles obligations sont un sujet «brûlant» actuellement et, plus important encore, qu'elles représentent une règlementation sommaire avec peu d'obligations supplémentaires pour les fournisseurs de services qui mettent en œuvre des mesures appropriées, et un réel élément de dissuasion tourné vers les besoins du marché pour ceux qui désireraient faire des économies.

Par ailleurs, il faut souligner qu'aucune des infractions ayant récemment fait la une aux États-Unis (Choicepoint, LexisNexis, Bank of America, Time Warner, etc.) n'impliquait de fournisseurs d'accès à Internet. Le groupe de travail tient à suggérer qu'une obligation de notification soit également envisagée pour les «courtiers de données» (data brokers), les banques ou d'autres fournisseurs de services en ligne. Même s'ils ne sont pas, par définition, des fournisseurs d'accès à Internet, ils sont les plus concernés par toute infraction à la sécurité.

La proposition stipule que les FAI devront informer uniquement ceux qui, parmi leurs clients, sont victimes d'une quelconque infraction à la sécurité. Cependant, en cas d'infraction grave (la communication ne vise pas à définir les différents niveaux d'infraction ni le moment où une infraction fait l'objet d'une notification), tous les clients de ce fournisseur, et pas seulement les «victimes», devront être informés. La proposition législative devrait fixer des règles de classification des différents niveaux d'infraction.

Fournisseurs d'accès et fournisseurs de services

La communication distingue les fournisseurs d'accès des fournisseurs de services. L'article 3 de la directive en vigueur sur la protection de la vie privée définit le traitement des données auxquelles les réglementations s'appliquent. Il était aisé, auparavant, de savoir qui était considéré comme un fournisseur de services de communications électroniques accessibles au public. Cependant, les développements dans le domaine des communications en ligne pourraient rendre plus opaques les informations sur les fournisseurs de service pour les consommateurs. En effet, ils peuvent accéder à un service via un portail, et ce service peut impliquer plusieurs intervenants.

Lorsqu'il s'agit de fournir des informations et de donner son accord, il n'est pas toujours évident de savoir qui est chargé d'informer les utilisateurs ou à qui l'on doit donner son accord. Dans le même temps, il peut y avoir un risque que les fournisseurs de services redirigent par erreur des utilisateurs vers un fournisseur d'accès ou de réseau, s'il s'agit du fournisseur qui s'occupe d'aspects spécifiques du service d'un point de vue technique.

Si l'on prévoit les rôles spécifiques que les fournisseurs d'accès et les fournisseurs de services pourraient jouer, il peut être utile de chercher à savoir si les règlementations sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques nécessitent d'être approfondies afin d'empêcher tout malentendu en ce qui concerne les destinataires de ces règlementations. C'est pourquoi la proposition législative devrait mener à des éclaircissements et ne pas accroître la confusion.

4. Conclusion

Le groupe de travail s'est félicité de l'opportunité de présenter ses commentaires sur le réexamen du paquet relatif aux communications électroniques, en se concentrant sur la directive sur la protection de la vie privée. Avant toute chose, le groupe de travail tient à recommander l'amélioration des mesures de sécurité et à souligner que la protection des utilisateurs et le développement de leur confiance dans les communications en ligne devraient être sérieusement pris en compte, parallèlement à une amélioration de la sécurité des infrastructures.

Le groupe de travail propose également de remédier aux problèmes relatifs aux applications en ligne. Ceux-ci comprennent notamment les questions de sécurité, la responsabilité des opérateurs, ainsi que la clarification des statuts légaux et du rôle du contrôleur des données.

Le groupe de travail tient à souligner qu'il soutient l'amélioration des mesures de sécurité, mais n'approuve aucune mesure qui mène ou risquerait de mener à davantage de surveillance ou de blocage des contenus.

Le groupe de travail se réserve la possibilité de présenter ses commentaires sur la directive tout au long de son évolution.

Fait à Bruxelles, le 26 septembre 2006

Par le groupe de travail

Le vice-président
José Luis Piñar Mañas