

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



**00989/08/FR
WP150**

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»)

Adopté le 15 mai 2008

Le 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.

Son secrétariat est assuré par la direction C (Justice civile, droits fondamentaux et citoyenneté) de la direction générale «Justice, liberté et sécurité» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau LX-46 06/80.

Site web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL,

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995¹,

vu l'article 29 et l'article 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 l'article 255 du traité CE et le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001, relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

A ADOPTÉ LE PRESENT AVIS:

1. CONTEXTE

Le 13 novembre 2007, la Commission a adopté une proposition de directive modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après «la proposition»).

Le principal objectif de la proposition est d'améliorer la protection des données à caractère personnel et de la vie privée des individus dans le secteur des communications électroniques, notamment en renforçant les dispositions liées à la sécurité et les mécanismes coercitifs.

Le groupe de travail «article 29» tient à commenter la proposition et à aborder certaines questions supplémentaires.

2. COMMENTAIRES SPÉCIFIQUES

Notification des violations de la sécurité

Article 4

Le groupe de travail «article 29» soutient pleinement la proposition visant à renforcer l'article 4 «Sécurité» en exigeant que les fournisseurs de services de communications électroniques accessibles au public notifient les violations de la sécurité. Le groupe de travail souligne également l'importance d'informer toutes les personnes concernées, lorsque leurs données à caractère personnel sont compromises ou risquent de l'être. Le groupe de travail «article 29» n'estime cependant pas que cet article traite complètement certaines questions évoquées ci-après.

¹ JO L 281 du 23.11.1995, p. 31,
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

a) La nécessité d'étendre aux fournisseurs de services de la société de l'information la portée de l'obligation de notifier les violations de la sécurité

Le groupe de travail «article 29» approuve totalement l'avis du contrôleur européen de la protection des données (CEPD)², selon lequel l'introduction d'un système de notification des violations de la sécurité, tel que décrit à l'article 4, paragraphes 3 et 4, devrait également concerner les fournisseurs de services de la société de l'information, comme les banques en ligne, les activités en ligne des entreprises, les prestataires en ligne de services de soins de santé, etc.

Élargir la portée de l'obligation aux prestataires de services de la société de l'information en général augmenterait leur responsabilité et contribuerait à sensibiliser le public. Cela permettrait incontestablement de réduire les risques en matière de sécurité.

b) Destinataires des notifications de violations de la sécurité

Le groupe de travail estime qu'il faudrait élargir le groupe des destinataires de notifications de violations de la sécurité, afin d'englober toutes les personnes concernées et pas uniquement les «abonnés», en remplaçant à l'article 4 le terme «abonnés» par «personnes concernées».

Le terme «personnes concernées» inclurait toutes les personnes dont les données ont effectivement été compromises par la violation de la sécurité (par exemple les abonnés, mais également les anciens abonnés et certains tiers).

Cela peut être particulièrement important, par exemple pour les personnes qui se sont récemment désabonnées d'un service et qui ne sont plus des «abonnés», mais dont les données à caractère personnel sont encore conservées par le responsable du traitement des données (c'est-à-dire le fournisseur d'un service de communications électroniques accessible au public). Le cas où des fournisseurs de services de communications électroniques accessibles au public détiennent des informations sur une personne, A, qui ne s'est pas abonnée à leurs services constitue une autre situation hypothétique soulignant la nécessité d'élargir le groupe des personnes visées par l'obligation de notification. Ce cas peut se produire si l'information a été transmise par un abonné du service ayant invité A à devenir utilisateur de ce service. Si des informations concernant A sont divulguées par suite d'une violation de la sécurité, A devrait naturellement être averti de ladite violation.

Cela pourrait également être utile lorsque les notifications de violations concernent des services de la société de l'information. En effet, les utilisateurs peuvent interagir avec certains de ces services sans y être abonnés.

2

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf

c) Divulgateion au public

Le groupe de travail suggère que, dans certaines circonstances, l'autorité réglementaire nationale (ARN) soit autorisée, dans l'intérêt du public, à informer celui-ci d'une violation ou à obliger les entreprises concernées à le faire. L'ARN devrait évaluer si le cas doit être rendu public, en comparant les intérêts des fournisseurs et les droits des personnes concernées.

Article 4, paragraphe 4

Conformément à l'article 4, paragraphe 4, la Commission peut, après consultation de l'Autorité européenne du marché des communications électroniques et du contrôleur européen de la protection des données, adopter des mises en œuvre techniques concernant les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification visées à l'article 4.

a) Le choix de la procédure de «comitologie»

Le groupe de travail «article 29» approuve l'approche de la proposition consistant à régler de nombreuses questions importantes concernant la fourniture d'informations aux individus et aux autorités chargées de la protection des données par l'intermédiaire des dispositions de mise en œuvre plutôt que dans le contexte de la directive «vie privée et communications électroniques».

b) Nécessité de consulter le groupe de travail «article 29»

Outre l'Autorité européenne du marché des communications électroniques et le contrôleur européen de la protection des données, le groupe de travail «article 29» devrait également être consulté, car toute mesure introduite aura un impact direct sur les informations à fournir aux personnes concernées.

La notion de «données à caractère personnel»

Le groupe de travail se félicite de la pleine compatibilité de la définition et de la portée du terme «*données à caractère personnel*» retenues dans la proposition avec la définition correspondante figurant dans la directive relative à la protection des données. Il souligne également que tout resserrement de la définition des «*données à caractère personnel*» dans la directive «vie privée et communications électroniques» créerait une faille dans la protection des individus dans un domaine qui est au cœur des communications électroniques – et par conséquent aussi de la société de l'information et des services d'administration en ligne fondés sur les services électroniques –, ce qui serait tout à fait inacceptable du point de vue de la protection de la vie privée.

Les notions de «réseau public de communications» et de «services de communications électroniques»

La directive «vie privée et communications électroniques» s'applique à la fourniture de services de communications électroniques accessibles au public dans le cadre de réseaux publics. Dans la pratique cependant, les notions de «*réseau public de communications*» et de «*services de communications électroniques*» sont très souvent confuses. Les services

sont de plus en plus constitués d'une association d'éléments privés et publics et il est souvent très difficile, à la fois pour les régulateurs et pour les parties prenantes, de déterminer si la directive «vie privée et communications électroniques» s'applique dans une situation donnée. Par exemple, la fourniture d'un accès à l'internet à 30 000 étudiants relève-t-elle d'un système de communications électroniques public ou privé? Qu'en est-il si ce même accès est fourni par une entreprise multinationale à 300 000 employés? Et s'il l'est dans un cybercafé?

Le groupe de travail «article 29» renvoie à ses précédents avis (WP 36³ et WP 126⁴) et réitère son appel à la clarification de la définition des termes «*services de communications électroniques*» et «*réseaux publics de communications*», car le développement de réseaux hybrides public/privé doit être pris en compte.

Le groupe de travail «article 29» invite la Commission à le consulter sur cette question, au moyen d'une communication de la Commission ou d'un autre instrument approprié.

ARN

Dans la proposition, l'ARN (autorité réglementaire nationale) semble désigner parfois l'autorité nationale de régulation compétente en matière de télécommunications et parfois l'autorité chargée de la protection des données.

Le groupe de travail «article 29» suggère d'introduire un libellé similaire à celui de l'article 3, paragraphe 5, de la directive-cadre 2002/21/CE, afin d'assurer une coopération efficace entre les autorités réglementaires nationales et les autorités chargées de la protection des données.

En outre, l'article 15 bis, paragraphe 4, «*Mise en œuvre et contrôle de l'application*» propose de consulter l'Autorité européenne du marché des communications électroniques. Le groupe de travail «article 29» insiste pour être également consulté et pour qu'une référence explicite à un processus de consultation obligatoire soit ajoutée à cette fin.

Enfin, le groupe de travail estime nécessaire de veiller à ce que le mécanisme d'harmonisation proposé n'empêche pas les États membres de fixer des exigences supplémentaires en matière de sécurité afin de poursuivre les objectifs définis dans la directive «vie privée et communications électroniques».

Article 3

Le groupe de travail «article 29» approuve l'avis susmentionné du contrôleur européen de la protection des données et estime cette disposition positive, car elle précise qu'un certain nombre d'applications d'identification par radiofréquence (RFID) relèvent du champ d'application de la directive «vie privée et communications électroniques».

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36fr.pdf

⁴ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_fr.pdf

Article 13 Communications non sollicitées

Le groupe de travail «article 29» observe des tendances dans les technologies de la communication qui s'écartent du modèle traditionnel d'abonné⁵ et suggère que le terme «*abonné*» soit remplacé par «*utilisateur*» dans l'ensemble de l'article 13 et qu'un nouveau considérant soit ajouté pour clarifier la relation et le rôle des abonnés par rapport à ceux des utilisateurs.

La directive «vie privée et communications électroniques» modifiée devrait protéger les utilisateurs de médias sans fil à courte portée contre les communications non sollicitées, définies à l'article 13. Un nouveau considérant pourrait apporter des éclaircissements plus détaillés.

Article 13, paragraphe 1

Afin de couvrir les évolutions et les progrès permanents des technologies, le paragraphe 1 ne devrait pas mentionner les «*systèmes automatisés d'appel*», mais bien les «*systèmes automatisés d'appel et de communication*» pour conserver une approche neutre sur le plan technologique, tout en tenant compte des changements technologiques en cours.

Article 13, paragraphe 6

Dans le nouvel article 13, paragraphe 6, la Commission propose de confirmer le droit de toute personne physique ou morale d'engager des actions en justice contre les auteurs d'infractions aux dispositions nationales adoptées en application de l'article 13 de la directive «vie privée et communications électroniques». Le groupe de travail recommande d'étendre ce droit à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», afin qu'il soit permis d'engager des poursuites en cas d'infraction aux dispositions nationales interdisant l'utilisation de logiciels espions.

3. AUTRES QUESTIONS À PRENDRE EN CONSIDÉRATION

a) Prise en compte du respect de la vie privée dès la conception («Privacy by design»)

Le groupe de travail «article 29» préconise l'application du principe de minimisation des données et l'utilisation des technologies renforçant la protection de la vie privée⁶ par les responsables du traitement des données.

Le groupe de travail appelle les législateurs européens à prévoir un renforcement dudit principe, en reproduisant les considérants 9 et 30 de la directive «vie privée et communications électroniques» dans un nouveau paragraphe à l'article 1^{er} de ladite directive.

b) Adresses IP

Le groupe de travail «article 29» constate que, dans le contexte du débat sur la directive «vie privée et communications électroniques», la question a été soulevée de savoir si les adresses IP étaient des données à caractère personnel. Le groupe de travail «article 29»

⁵ Par exemple, par l'utilisation croissante de technologies comme le Bluetooth qui permettent une certaine forme de publicité devenue tout aussi intrusive que les spams, même si la base technologique est différente.

⁶ COM(2007) 228 final.

rappelle que, dans la plupart des cas, y compris dans les cas d'attribution dynamique d'adresses IP, les données nécessaires sont disponibles pour identifier le ou les utilisateur(s) de l'adresse IP.

Le groupe de travail avait précisé dans son avis WP 136⁷ que «[...] à moins que les fournisseurs d'accès internet soient en mesure de déterminer avec une certitude absolue que les données correspondent à des utilisateurs non identifiables, par mesure de sécurité, ils devront traiter toutes les informations IP comme des données à caractère personnel». Ces considérations s'appliqueront également aux moteurs de recherche (WP 148⁸).

c) Article 5, paragraphe 1

Le groupe de travail «article 29» rappelle que cet article impose une obligation de garantir la confidentialité des communications, indépendamment de la nature du réseau et du fait que les communications traversent les frontières de pays tiers.

Les fournisseurs de services de communications électroniques devraient renforcer les mesures afin de mieux protéger tous les individus concernés par des communications électroniques impliquant des parties situées dans des pays tiers. La révision de la directive «vie privée et communications électroniques» est le cadre approprié pour affirmer les droits civils à cet égard, afin notamment de garantir la transparence dans les mécanismes utilisés pour la transmission des communications.

4. REMARQUES FINALES, CONCLUSION

Le groupe de travail «article 29» appelle les législateurs européens à prendre en compte les questions mises en évidence dans le présent avis.

Fait à Bruxelles, le 15 mai 2008
Pour le groupe de travail
Le président
Alex Türk

⁷ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf

⁸ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf