GROUPE «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00350/09/FR
WP 159

Avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»)

Adopté le 10 février 2009

Table des matières

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

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 PRÉSENT AVIS:

1. CONTEXTE

Le 13 novembre 2007, la Commission a adopté une proposition de directive (ci-après «la proposition») modifiant la directive 2002/58/CE concernant le traitement des données à caractère personnel dans le secteur des communications électroniques (directive «vie privée et communications électroniques») et la directive 2002/21/CE (directive-cadre).

Le 24 septembre 2008, le Parlement européen a adopté en première lecture des amendements à la proposition («les amendements du Parlement») qui ont été commentés par la Commission européenne dans sa communication COM(2008) 723 final du 6 novembre 2008 («les observations de la Commission»).

Le 27 novembre 2008, le Conseil de l'Union européenne est parvenu à un accord politique («l'accord du Conseil»).

Le groupe «Article 29» tient à commenter les amendements du Parlement, les observations de la Commission et l'accord du Conseil.

Le groupe rappelle qu'il a déjà adopté deux avis sur les propositions modifiant le cadre réglementaire européen pour les réseaux et services de communications électroniques (l'avis 8/2006 adopté le 26 septembre 2006[2] et l'avis 2/2008 adopté le 15 mai 2008[3]).

Tout en se réjouissant qu'il ait été tenu compte de certaines de ses recommandations précédentes, le groupe tient à souligner certains aspects essentiels des questions soulevées à la suite de la première lecture au Parlement et au Conseil; il ne reprend pas l'ensemble des observations formulées dans ses avis précédents, qui toutefois demeurent valables.

---

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

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

3 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_fr.pdf .

2. NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

2.1. Observations

Le groupe soutient pleinement la proposition visant à renforcer l'article 4 de la directive «vie privée et communications électroniques» en exigeant que les fournisseurs de services de communications accessibles au public notifient les violations de la sécurité. Les notifications de violations peuvent devenir un instrument important pour permettre aux autorités chargées de la protection des données de mieux cibler leur action et d'en accroître l'efficacité s'agissant d'assurer le respect de l'obligation qui incombe aux fournisseurs de service de prendre les mesures de sécurité appropriées.

D'une manière générale, le groupe recommande l'approche suivante en ce qui concerne les notifications des violations de données à caractère personnel:

- l'autorité réglementaire nationale compétente est avertie en cas de risque de conséquences négatives[4] pour la protection de la vie privée et des données à caractère personnel;

- il est essentiel que le fournisseur de services avertisse sans délai les utilisateurs affectés dans les cas où la violation de la sécurité peut entraîner des conséquences négatives[5] pour la protection de la vie privée et des données à caractère personnel, sans préjudice de la possibilité pour l'autorité réglementaire nationale compétente d'informer le public de la violation en question ou d'obliger le fournisseur de services à le faire;

- chaque fournisseur de services devrait enregistrer[6] toutes les violations des données à caractère personnel.

Par ailleurs, le groupe observe que les trois propositions (du Parlement, de la Commission et du Conseil) adoptent des approches substantiellement différentes en ce qui concerne les violations de la sécurité et des données à caractère personnel, notamment lorsqu'elles considèrent:

- la portée de l'obligation (qui s'étend aux services de la société de l'information dans les amendements du Parlement et est limitée aux services de communications électroniques accessibles au public pour le Conseil et la Commission); le groupe soutient fermement une extension de l'obligation aux services de la société de l'information;

- l'entité qui doit décider d'avertir les particuliers (pour le Parlement et la Commission, il s'agit de l'autorité compétente et pour le Conseil du fournisseur de services);

---

4 Le risque de conséquences négatives doit être évalué en tenant compte d'éléments tels que le volume et la nature des données affectées par la violation, les conséquences qu'un particulier peut subir en raison de la violation, notamment le vol d'identité, les pertes financières, la perte d'activités économiques ou de possibilités d'emploi, ou une combinaison de ces conséquences ou toute autre circonstance similaire. Les critères qualitatifs et quantitatifs permettant d'évaluer l'incidence des conséquences négatives devront être définis avec précision au cours de la comitologie en gardant à l'esprit l'importance de ne pas submerger les autorités de cas mineurs et de ne pas alarmer inutilement les particuliers.

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

6 Le format de ces enregistrements devrait être harmonisé afin que l'autorité réglementaire nationale compétente puisse en assurer le contrôle.

- la nature des violations à notifier (toutes les violations dans la proposition du Parlement et dans les observations de la Commission et seules les graves violations dans l'accord du Conseil);

- et les destinataires de la notification (les abonnés ou les particuliers pour le Parlement et la Commission, mais uniquement les abonnés pour le Conseil).

La portée de l'obligation de notification: les services de la société de l'information

Le groupe soutient fermement les amendements 187/rev et 184 du Parlement. **Une extension de l'obligation de notification des violations de données à caractère personnel aux services de la société de l'information s'impose compte tenu du rôle toujours plus important que jouent ces services dans la vie quotidienne des citoyens européens** et du volume croissant de données à caractère personnel qu'ils traitent. Les transactions électroniques telles que l'accès aux services bancaires en ligne, aux dossiers médicaux du secteur privé et les achats en ligne ne sont que quelques exemples des services exposés à des violations de données à caractère personnel qui présentent un risque élevé pour un grand nombre de citoyens européens. À supposer que cette obligation soit limitée aux services de communications électroniques accessibles au public, elle ne toucherait qu'un nombre restreint de parties prenantes et cela réduirait dès lors considérablement l'effet des notifications de violations de données à caractère personnel en tant qu'instrument de protection des particuliers contre des risques tels que le vol d'identité, les pertes financières, la perte d'activité économique ou de possibilités d'emploi et l'atteinte à l'intégrité physique.

Le groupe déplore donc vivement que la Commission et le Conseil n'aient pas soutenu cette proposition et il rappelle que certaines dispositions de la directive «vie privée et communications électroniques» s'appliquent déjà en dehors du cadre strict des services de communications électroniques[7].

La responsabilité et les critères de notification

Les fournisseurs de services concernés devraient assurer l'évaluation des risques que comportent les violations des données à caractère personnel; ils sont les mieux placés pour déterminer rapidement, sur la base des règles d'évaluation établies par les autorités, s'il y a lieu d'avertir les personnes concernées. **Nonobstant leur obligation de notifier aux autorités réglementaires nationales compétentes toute violation risquant de produire des effets négatifs, les fournisseurs de services devraient déterminer s'il y a lieu d'avertir les abonnés ou les particuliers. Dans un souci de garantir une information précise et appropriée du public, les autorités réglementaires nationales compétentes pourront décider de rendre publique la violation lorsqu'elles l'estimeront nécessaire, ou obliger le fournisseur de services à le faire.**

---

[7] Certaines dispositions de la directive «vie privée et communications électroniques» telles que l'article 5, paragraphe 3 («cookies» et logiciels espions) et l'article 13 (communications non sollicitées) constituent d'ores et déjà des dispositions à caractère général qui ne s'appliquent pas qu'aux seuls services de communications électroniques.
La possibilité de dépasser le cadre strict des services de communications électroniques accessibles au public est déjà envisagée dans d'autres situations, la Commission ayant proposé d'élargir le champ d'application de l'article 5, paragraphe 3, de manière à couvrir les cas de diffusion de «cookies» et de logiciels espions sur des médias tels que les CD-ROM ou les clés USB, qui ne sont pas des services de communications électroniques accessibles au public.

La notification devant être effectuée par le fournisseur de services, **il est essentiel que la directive prévoie des dispositions permettant de garantir que celui-ci n'a pas dissimulé de violations**, qu'il a procédé correctement à l'évaluation de la violation et qu'il a, au besoin, averti les particuliers.

Les autorités seront informées dans un plus grand nombre de cas, de sorte qu'elles pourront exercer une surveillance sur le processus de notification aux particuliers mis en œuvre par les fournisseurs de service. Le modèle de notification devrait être harmonisé à l'échelle européenne et contenir des critères clairs et objectifs pour faciliter l'évaluation des répercussions négatives de la violation. En outre, l'autorité réglementaire nationale compétente devrait vérifier si le fournisseur de services a procédé correctement à l'évaluation de la violation des données à caractère personnel et s'il y a donné les suites appropriées. Enfin, **afin de prévenir la dissimulation d'infractions, il est essentiel que la directive confère à l'autorité réglementaire nationale compétente le pouvoir d'infliger des sanctions financières (amendes)**[8] **à tout fournisseur de services qui omet de signaler ou ne signale pas correctement au particulier ou à l'autorité réglementaire nationale une violation de données à caractère personnel.**

Les types de violations à notifier aux particuliers: la notion de conséquences négatives

Le groupe se félicite de l'introduction à l'article 2[9] d'une nouvelle définition de la «violation des données à caractère personnel», telle que proposée par la Commission dans ses observations[10] .

Le groupe relève néanmoins des différences de libellé dans les trois propositions en ce qui concerne les circonstances dans lesquelles une violation doit être notifiée aux personnes concernées. **Il recommande dès lors de notifier aux personnes concernées les violations de la sécurité lorsqu'elles peuvent entraîner des conséquences négatives pour la protection de la vie privée et des données à caractère personnel.** L'accord du Conseil fournit à cet égard des exemples utiles au considérant 29.

Les destinataires des notifications

Le groupe se félicite qu'il soit fait référence aux «abonnés et particuliers», aux «utilisateurs concernés/touchés» et à l'«autorité nationale compétente» au considérant 29 des amendements du Parlement[11]. L'accord du Conseil limitant les notifications aux «abonnés», certaines violations de données à caractère personnel qui avaient été décrites dans l'avis 2/2008 ne seront pas notifiées aux personnes concernées.

2.2. Exemptions de notification

Le groupe reconnaît que les notifications de violations devraient préciser les circonstances dans lesquelles la violation a eu lieu, et indiquer notamment si les données personnelles avaient été protégées par cryptage; il est essentiel que l'autorité réglementaire nationale compétente dispose de ces informations en cas d'infraction, afin de pouvoir décider des mesures à prendre, le cas échéant, à l'égard du fournisseur de services.

---

8 Le groupe note que de telles dispositions ont été proposées par le Parlement, la Commission et le Conseil dans un nouvel article 15 bis, paragraphe 1.

9 Voir les observations de la Commission sur les amendements 187/rev et 184 du Parlement.

10 Néanmoins, cette notion de «violation des données à caractère personnel» revêt un caractère général et ne devrait pas être limitée aux données traitées dans le cadre de services de communications électroniques accessibles au public; elle devrait également couvrir au moins les services de la société de l'information.

11 Voir l'amendement 183.

Néanmoins, **le groupe s'oppose à ce que le fournisseur de services soit exonéré de l'obligation de notification[12] lorsqu'il a mis en œuvre «les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation». Une telle disposition réduirait considérablement la qualité et l'utilité des informations fournies aux personnes concernées.** Les utilisateurs touchés ne pourront faire le nécessaire pour réduire les risques auxquels ils sont confrontés que s'ils ont été correctement informés. Par conséquent, **le groupe insiste sur l'importance du format de la notification et de l'évaluation des risques pour déterminer si les particuliers doivent être avertis, indépendamment des mesures techniques prises pour protéger leurs données.**

3. DONNÉES RELATIVES AU TRAFIC

3.1. Traitement des données relatives au trafic pour des raisons de sécurité

Dans un nouvel article 6, paragraphe 6 bis, le Parlement, le Conseil et la Commission proposent l'introduction, dans la directive «vie privée et communications électroniques», d'une nouvelle exemption permettant de traiter les données relatives au trafic pour des raisons de sécurité.

Le groupe a conscience que les «prestataires de services de sécurité» déploient des solutions de sécurité[13] (logiciels anti-virus et anti-spam, pare-feu, ou systèmes de détection d'intrusion) qui exigent le traitement des données relatives au trafic en vue de sécuriser les données personnelles des utilisateurs ou de protéger le service lui-même. Néanmoins, il redoute que le libellé actuel puisse légitimer le déploiement à grande échelle de l'analyse par paquets approfondie[14], tant sur le réseau que sur les équipements des utilisateurs tels que les boîtes ADSL, alors que le dispositif réglementaire actuel précise d'ores et déjà les cas dans lesquels les données relatives au trafic peuvent être traitées pour des raisons de sécurité.

En effet, les motifs juridiques justifiant le traitement des données relatives au trafic par les services de communications électroniques accessibles au public ainsi que le traitement des données à caractère personnel par les responsables du traitement des données sont exposés à l'article 6 de la directive «vie privée et communications électroniques» ainsi qu'aux articles 7 et 17 de la directive sur la protection des données. Les conditions dans lesquelles les données à caractère personnel peuvent être traitées compte tenu de l'intérêt légitime poursuivi par le responsable du traitement sont précisées à l'article 7, point f), de la directive sur la protection des données; cet intérêt ne peut l'emporter sur l'intérêt ou les droits et libertés fondamentaux de la personne concernée. L'article 17 de la directive sur la protection des données impose en outre au responsable du traitement l'obligation de *«mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés [...] ainsi que contre toute autre forme de traitement illicite»*. Par ailleurs, les mesures adoptées doivent être proportionnées aux risques présentés par le traitement et à la nature des données à protéger.

---

12 Voir le considérant 29 dans les amendements du Parlement (amendement 122) et les considérants 29 et 32 dans l'accord du Conseil.

13 Sur l'équipement terminal de l'utilisateur ou sur le réseau.

14 L'analyse par paquets est une technique très envahissante de repérage et de traçage du comportement de l'utilisateur.

Le groupe fait en outre observer que le champ d'application de l'amendement 180 du Parlement a été précisé dans les observations de la Commission. **Le groupe note que le libellé proposé par la Commission établit sans équivoque que le traitement des données relatives au trafic relève du champ d'application de la directive sur la protection des données.** Par conséquent, les prestataires de services de sécurité doivent avertir en tant que de besoin les autorités chargées de la protection des données et garantir aux utilisateurs l'exercice de leurs droits.

Enfin, le groupe rappelle que le traitement des données relatives au trafic pour des raisons de sécurité est d'ores et déjà mis en œuvre dans les États membres qui ont adopté des mesures spécifiques conformément à l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques», en vertu duquel les États membres peuvent adopter des mesures législatives dérogeant au principe de l'anonymisation ou de l'effacement des données relatives au trafic[15] lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, afin de protéger le système de communications électroniques contre les utilisations non autorisées.

Pour les raisons invoquées ci-dessus, **il est inutile de proposer un nouvel article 6, paragraphe 6 bis.**

4. ADRESSES IP

Le Parlement et la Commission proposent l'introduction d'un nouveau considérant (27 bis) relatif aux adresses IP[16].

Le groupe apprécie la formulation proposée par la Commission dans ses observations en ce qui concerne la référence spécifique à ses travaux, mais il n'est pas en faveur d'une mention explicite de cette question, dans une directive.

À cet égard, **il renvoie à son précédent avis[17] dans lequel il précisait qu'à moins que les fournisseurs de services «***soient en mesure de préciser 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»*.

Les adresses IP correspondent le plus souvent à des personnes identifiables, c'est-à-dire qui peuvent être identifiées par le fournisseur d'accès internet ou par d'autres moyens, à l'aide d'identifiants supplémentaires tels que les «cookies» ou dans des interactions avec d'autres services internet apportant, explicitement ou implicitement, des éléments d'identification sur la personne concernée.

Le considérant 26 de la directive sur la protection des données indique clairement que pour déterminer si une personne est identifiable, *«il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne»*.

---

15 Établi à l'article 6, paragraphe 1.

16 Amendement 185 du Parlement.

17 Avis 4/2007 sur le concept des données à caractère personnel et avis sur les aspects de la protection des données liés aux moteurs de recherche.

La définition des données à caractère personnel établie dans la directive sur la protection des données se réfère aux données «concernant» une personne physique, et les adresses IP sont couramment utilisées pour catégoriser les utilisateurs dans le cadre, par exemple, de la transmission de publicité ciblée ou de la création de profils.

Tout en étant prêt à assister la Commission dans la réalisation des travaux en matière d'adresses IP suggérés par le Parlement[18], le groupe reconnaît avec la Commission que l'introduction d'une disposition matérielle dans une directive n'est pas le meilleur moyen d'aborder cette question et qu'une obligation de couvrir dans le rapport des «fins qui ne sont pas couvertes par la présente directive» n'apparaît pas appropriée.

5. INFORMATION DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES

Le Parlement a adopté en première lecture l'amendement 136 relatif à l'article 15 de la directive «vie privée et communications électroniques», qui a été modifié par la suite par la Commission dans ses observations. Cette proposition instaurerait, pour tous les fournisseurs de services et de réseaux de télécommunications et les fournisseurs de services de la société de l'information, l'obligation d'informer l'autorité compétente en matière de protection des données de toute demande «reçue conformément au paragraphe 1[19]» et, pour ladite autorité, l'obligation d'examiner chaque demande et d'informer les autorités judiciaires compétentes des cas dans lesquels elle estime que les dispositions pertinentes de la législation nationale n'ont pas été respectées.

L'obligation d'information proposée est un ajout utile dans l'intérêt d'une plus grande transparence et d'une amélioration des contrôles exercés par les autorités réglementaires. Cette disposition renforcerait sans doute considérablement les moyens de surveillance et de répression des autorités chargées de la protection des données et contribuerait dès lors à améliorer la mise en œuvre de l'accès licite à l'information, mais elle alourdirait la charge administrative, tant pour les entreprises concernées que pour les autorités chargées de la protection des données. À cet égard, le groupe est préoccupé par le nombre croissant de demandes[20] que les autorités judiciaires auraient à contrôler et du suivi que les autorités chargées de la protection des données seraient tenues d'exercer sur la moindre enquête judiciaire, ce qui nécessiterait une augmentation substantielle de leurs ressources financières et humaines.

Par conséquent, **le groupe suggère de limiter à une fois par an l'établissement de ce rapport. Celui-ci pourrait décrire en détail les procédures internes suivies pour répondre aux demandes d'accès aux données personnelles des utilisateurs et indiquer le nombre de demandes reçues, la justification légale invoquée et les problèmes rencontrés, le cas échéant.** Par ailleurs, il y a lieu d'harmoniser et de détailler au niveau européen cette obligation d'information.

---

[18] Dans les amendements 139 et 186/rev.

[19] Ce paragraphe décrit les obligations en matière de conservation des données énoncées formellement dans la directive sur la conservation des données (2006/24/CE).

[20] De nombreux opérateurs de télécommunications reçoivent plusieurs centaines de demandes par jour.

6. COMMUNICATIONS NON SOLLICITÉES

L'amendement 131 du Parlement précise que la définition du «courrier électronique», à l'article 2, point h), couvre les MMS et les technologies du même type.

En premier lieu, le groupe fait observer que le considérant 40 de la directive «vie privée et communications électroniques» précise déjà que les SMS relèvent de la définition du courrier électronique[21].

En deuxième lieu, il convient, en application du principe énoncé au considérant 4[22], d'adapter l'article 13, paragraphe 1, aux technologies émergentes. Dans sa formulation actuelle, l'article 13, paragraphe 1, part de l'hypothèse que la personne est déjà connectée au réseau qui achemine la communication (notamment un appel téléphonique ou un courriel). Il ne couvre pas les cas où des messages demandent à l'utilisateur de se connecter à un réseau diffusant des annonces publicitaires. Cela est précisément le cas des systèmes de prospection commerciale par Bluetooth.

Le groupe se félicite donc des éclaircissements apportés par les observations de la Commission sur le champ d'application de l'article 13, en ce qui concerne principalement l'utilisation du terme «communication» et le nouveau considérant qui évoque des «technologies de nature semblable». Ce libellé garantit que l'accord préalable de l'utilisateur est requis en cas de prospection commerciale par Bluetooth et tient compte par conséquent des observations formulées par le groupe dans son avis 2/2008 concernant la nécessité de «protéger les utilisateurs de médias sans fil à courte portée contre les communications non sollicitées, définies à l'article 13». La technologie Bluetooth pourrait également être explicitement mentionnée au considérant 40.

En troisième lieu, le groupe rappelle l'observation formulée dans son avis 2/2008 au sujet de l'utilisation du terme «abonné» à l'article 13, et prend note avec satisfaction du libellé proposé dans l'accord du Conseil.

Enfin, la proposition du Conseil visant à modifier l'article 13, paragraphe 2, en y ajoutant l'expression «au moment où elles sont recueillies» est également d'une grande utilité dans la mesure où elle précise clairement à quel moment les utilisateurs peuvent s'opposer à l'exploitation de leurs coordonnées électroniques à des fins de prospection directe.

7. PARAMETRES DU NAVIGATEUR

Le groupe conteste fermement l'amendement 128 adopté par le Parlement, selon lequel la fixation par défaut de paramètres du navigateur constituerait un consentement préalable. Le groupe tient à commenter cet amendement même s'il n'a pas été repris dans les observations de la Commission et dans l'accord du Conseil.

Au-delà du problème formel que pose l'introduction dans la directive d'une terminologie propre à une technologie, le groupe est préoccupé par l'érosion de la définition de «consentement» et par le manque de transparence qui en découle.

---

[21] Défini à l'article 2, point h), de la directive «vie privée et communications électroniques».

[22] Ce considérant précise que la directive «vie privée et communications électroniques» «doit être adaptée à l'évolution des marchés et des technologies des services de communications électroniques afin de garantir un niveau égal de protection des données à caractère personnel et de la vie privée aux utilisateurs de services de communications électroniques accessibles au public, indépendamment des technologies utilisées».

La plupart des navigateurs fixent des paramètres par défaut qui ne permettent pas aux utilisateurs d'être informés du stockage provisoire d'informations dans leur équipement terminal ou de l'accès à celui-ci par des tiers. Les paramètres des navigateurs devraient donc être fixés de manière à respecter la confidentialité. Toujours est-il qu'ils ne peuvent pas être considérés comme un outil pour recueillir le consentement libre, spécifique et informé de l'utilisateur, tel que prévu à l'article 2, point h), de la directive sur la protection des données.

Pour ce qui concerne les «cookies», le groupe estime que l'entité qui contrôle ces fichiers témoins devrait, dans sa déclaration de confidentialité, informer les utilisateurs de leur existence et que celle-ci ne saurait exciper à cet égard du paramétrage du navigateur (par défaut). Par ailleurs, la formulation retenue ne couvre pas uniquement la question actuelle des «cookies», mais sous-entend toute nouvelle technologie pouvant servir à cerner le comportement de navigation des utilisateurs.

8. ACTIONS EN JUSTICE ENGAGEES PAR DES PERSONNES PHYSIQUES OU MORALES

Le groupe soutient la proposition du Parlement[23] visant à introduire à l'article 13, paragraphe 6, la possibilité pour toute personne physique ou morale lésée par suite d'une violation des dispositions nationales adoptées en application de la directive «vie privée et communications électroniques» d'engager une action en justice.

Cette disposition renforcera sans doute les droits des utilisateurs et contribuera au développement de meilleures pratiques de sécurité parmi les opérateurs du secteur.

9. AUTRES QUESTIONS

Pour finir, le groupe note avec satisfaction:

- que le législateur entend sanctionner les pratiques d'hameçonnage[24];
- que la Commission et le Conseil ont tenu compte[25] de la demande du groupe d'être consulté au cours de la procédure de comité établie à l'article 4, paragraphe 4;
- qu'il a été associé au processus de consultation prévu à l'article 15 bis, paragraphe 4;
- qu'il sera consulté dans le cadre de la préparation du rapport sur l'application de la directive révisée «vie privée et communications électroniques»[26];
- que la Commission, le Conseil et le Parlement tiennent à préciser que la directive «vie privée et communications électroniques» s'applique aux technologies émergentes telles que l'identification par radiofréquence (*radio frequency identification, RFID*)[27] ou la communication en champ proche (*near field communication, NFC*), qui reposent sur des dispositifs d'identification sans contact utilisant les fréquences radio.

---

23 À l'amendement 133.
24 Voir l'amendement 132 du Parlement.
25 Dans ses observations sur l'amendement 127 du Parlement.
26 Voir les amendements 139 et 186/rev du Parlement.
27 À l'article 3 et au considérant 28.

10. CONCLUSION

Le groupe «Article 29» invite les législateurs européens à examiner avant tout, parmi les questions soulevées dans le présent avis, l'extension de l'obligation de notification des violations de données à caractère personnel aux services de la société de l'information, étant donné son impact fondamental sur la protection des données personnelles de l'ensemble des citoyens européens.

Fait à Bruxelles, le 10 février 2009

Pour le groupe
Le président
Alex TÜRK