Groupe de travail "ARTICLE 29" sur la protection des données

00451/06/FR
WP 118

Avis 2/2006 du groupe 29 sur les problèmes de protection de la vie privée liés à la fourniture de services de vérification du contenu des courriers électroniques

Adopté le 21 février 2006

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A 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, l'article 30, paragraphe 1, point c), et l'article 30, paragraphe 3, de ladite directive,

vu son règlement intérieur, et notamment ses articles 12 et 14,

ADOPTE LE PRÉSENT AVIS:

I. INTRODUCTION

Le groupe 29 constate que divers services de communication en ligne sont en expansion, dont les messageries électroniques gratuites sur Internet et leurs services associés. Or le développement des services de communication électronique suscite des préoccupations quant à la protection de la confidentialité des communications, notamment en raison de pratiques consistant à les surveiller en vue d'éliminer le spam et les virus ainsi que de détecter des contenus prédéterminés.

Le groupe 29 sait que la plupart des fournisseurs d'accès Internet et des services de messagerie électronique («FAI» et «SME») recourent à des outils de filtrage pour protéger leurs réseaux et leurs machines ainsi que, dans des cas moins répandus, pour surveiller les communications à des fins commerciales. Or le groupe considère que, dans certains cas, ce filtrage peut être contraire à la législation protégeant les données, détaillée ci-après, notamment parce que l'application des textes à ces nouveaux types de prestations n'est pas toujours évidente.

Le présent avis vise avant tout à donner des orientations en matière de confidentialité des communications par courrier électronique et, plus particulièrement, de filtrage des communications en ligne. Il s'agit notamment de déterminer si la vérification des communications habituellement effectuée par les FAI et SME à différentes fins constitue une interception de communication, si cette dernière peut être justifiée et, dans l'affirmative, dans quelles conditions.

À cet effet, le présent document analyse, entre autres, les dispositions relatives à la confidentialité des communications électroniques, telle qu'elle est définie à l'article 5, paragraphe 1, de la directive 2002/58 sur la vie privée et les communications électroniques, ainsi que les autres dispositions pertinentes faisant partie de l'acquis communautaire et les lois nationales le mettant en œuvre.

II. LE CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE DANS LES COMMUNICATIONS PAR COURRIER ÉLECTRONIQUE

A) La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

La confidentialité des communications est garantie en conformité avec les instruments internationaux relatifs aux droits de l'homme, notamment la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ("CEDH") et les constitutions des États membres. Elle est également garantie par les deux directives européennes examinées ci-après.

---

[1] Journal officiel L 281 du 23.11.1995, p. 31, disponible sur: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

L'article 8 de la CEDH reconnaît à toute personne le droit au respect de sa vie privée et de sa correspondance et elle fixe les conditions dans lesquelles la restriction de ce droit est admissible. Une jurisprudence constante de la Cour européenne des droits de l'homme ("la Cour") applique l'article 8 aux communications par courrier ordinaire.

Ainsi l'interception, l'ouverture, la lecture de lettres et le retardement de leur réception , de même que la création d'obstacles à leur envoi, ont tous été considérés comme des violations de l'article 8 de la CEDH[2]. Au vu des décisions de la Commission des droits de l'homme et de la jurisprudence de la Cour, il est quasi certain que les communications par courrier électronique seront couvertes par l'article 8 de la CEDH, par la combinaison des notions de "vie privée" et de "correspondance"[3]. Les personnes échangeant des messages électroniques peuvent donc raisonnablement attendre que leurs communications ne soient pas surveillées par des tiers, qu'ils soient publics ou privés.

Le droit au respect de la "correspondance" comprend non seulement le secret mais également le droit d'envoyer et de recevoir cette correspondance[4]. On peut dès lors en conclure qu'une interdiction générale d'envoyer ou de recevoir du courrier électronique sera contraire à l'article 8 de la CEDH.

Toute personne résidant dans l'un des États signataires de la CEDH a droit au respect de sa vie privée et de sa correspondance. Cette protection s'étend à tous les correspondants d'une communication. Ainsi, dans l'affaire A. contre France (1993), la Cour a déclaré que l'enregistrement d'une conversation téléphonique avec le consentement d'une seule partie constituait une ingérence dans l'exercice du droit au respect de la correspondance de l'autre personne participant à la communication.

La CEDH autorise ses États signataires à procéder à des interceptions légitimes de correspondance, y compris de communications électroniques, ou à prendre d'autres mesures, si elles sont nécessaires à l'une des finalités de la convention et conformes à l'interprétation de la CEDH donnée dans les arrêts de la Cour. Une interception peut se définir comme l'accès par un tiers au contenu et/ou aux données de trafic de communications privées entre plusieurs correspondants, notamment aux données de trafic concernant l'utilisation de services de communication électroniques, qui constitue une violation du droit d'une personne physique au respect de sa vie privée et au secret de sa correspondance. Ces interceptions ne sont admissibles que si elles remplissent trois critères fondamentaux, conformément à l'article 8, paragraphe 2, de la CEDH et à son interprétation:

"… un fondement légal, la nécessité d'une telle mesure dans une société démocratique, et sa conformité avec l'une des finalités légitimes énumérées dans la convention…"

---

[2] Dans l'affaire Niemitz (1992), la Cour a déclaré que des lettres déjà remises à leur destinataire sont couvertes par l'article 8 de la CEDH. Elle y ajoutait que la protection s'étend aux communications non seulement privées mais également professionnelles. Par ailleurs, dans les affaires Klass (1978), Malone (1984) et Huvig (1990), la Cour a estimé que les conversations téléphoniques sont elles aussi couvertes par l'article 8. En ce qui concerne les autres moyens de communication, la décision de la Commission dans l'affaire Mersch (1985) est pertinente en ce qu'elle a considéré que l'interception de toute forme de communication constituerait une violation de l'article 8.

[3] Cette conclusion est corroborée par le fait que, dans la plupart des États membres, la surveillance des messages électroniques est interdite et que, tant au niveau national qu'international, l'interception des communications par courrier électronique relève de pouvoirs spéciaux.

[4] Golder (1975), considérant 43: «Un obstacle apporté à la possibilité même de correspondre représente la forme la plus radicale d' «ingérence» (paragraphe 2 de l'article 8) dans l'exercice du «droit au respect de la correspondance»; on n'imagine pas qu'il sorte du domaine de l'article 8 alors qu'un simple contrôle en relève sans contredit.» La rétention de courrier reçu constitue également une ingérence (Schöneberger & Durmaz, 1988).

Toutefois, dans le cadre des relations privées, le dispositif le plus propice à l'application des droits prévus par la convention est la doctrine des obligations positives des Parties contractantes, selon laquelle celles-ci, outre l'obligation de s'abstenir de toute ingérence, sont tenues de prendre des mesures concrètes garantissant la possibilité d'exercer ces droits non seulement à l'égard de la puissance publique mais également dans la sphère des relations individuelles. Elle comprend l'obligation de mettre en place un cadre juridique adapté permettant l'exercice de ces droits.

L'article 6, paragraphe 2, du traité sur l'Union européenne mentionne expressément que l'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire. Selon l'article 52, paragraphe 3, de la Charte des droits fondamentaux de l'UE, le sens et la portée des droits qu'elle contient sont les mêmes que ceux que leur confère la CEDH. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

B) Les textes spécifiques applicables à la confidentialité des communications par courrier électronique

Ainsi qu'il a été dit précédemment, la confidentialité des communications est en outre garantie par deux directives européennes. Lorsque l'on examine cette question, il convient d'interpréter leurs dispositions en tenant compte de la CEDH et de la jurisprudence de la Cour européenne des droits de l'homme, exposée plus haut.

La directive 95/46/CE du Parlement européen et du Conseil 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 (ci-après, la «directive sur la protection des données») instaure un régime juridique horizontal destiné à garantir le droit des personnes physiques à la protection des données les concernant. S'agissant du traitement des données à caractère personnel, la directive énonce le droit au respect de la vie privée tel qu'il est reconnu à l'article 8 de la CEDH[5]. La liberté de recevoir ou de communiquer des informations est également reconnue, et incluse dans la liberté d'expression telle que garantie à l'article 10 de la CEDH[6]. En outre, le considérant 47 énonce que la personne dont émane un message contenant des données à caractère personnel sera normalement considérée comme responsable du traitement de ces données, tandis que la personne offrant le service de transmission sera normalement considérée comme responsable du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service.

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 (ci-après, la «directive e-vie privée») est applicable au traitement des données à caractère personnel lié à la fourniture de réseaux de communications électroniques accessibles au public. Ses dispositions précisent et complètent la directive sur la protection des données. La confidentialité des communications est notamment protégée par l'article 5 de la directive e-vie privée, formulé comme suit:

---

5 Considérant 10: «considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire;»

6 Considérant 37: «considérant que le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire, notamment dans le domaine audiovisuel, doit bénéficier de dérogations ou de limitations de certaines dispositions de la présente directive dans la mesure où elles sont nécessaires à la conciliation des droits fondamentaux de la personne avec la liberté d'expression, et notamment la liberté de recevoir ou de communiquer des informations, telle que garantie notamment à l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales;»

«Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, …»

De plus, aux termes de son article 4, «*le prestataire d'un service de télécommunications accessible au public doit prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de télécommunications en ce qui concerne la sécurité du réseau*.»

On peut encore citer la directive sur le commerce électronique, notamment ses dispositions relatives à la responsabilité des fournisseurs d'accès Internet ou de services de courrier électronique, interdisant aux États membres de leur imposer une obligation générale de surveiller les informations car elle constituerait une atteinte à la liberté d'expression et au secret de la correspondance (article 15 de la directive sur le commerce électronique[7]).

III. LA VÉRIFICATION DU CONTENU DES COURRIERS ÉLECTRONIQUES

C'est sur cette toile de fond juridique que se pose la question de la compatibilité avec le droit communautaire de la vérification des communications habituellement effectuée par les FAI et SME à différentes fins.

Car la majorité de ces prestataires vérifient bel et bien les messages électroniques. Ils le font systématiquement à des fins telles que le filtrage des spams, la détection des virus, les recherches de texte et le contrôle orthographique, ainsi que la retransmission de messages, la réponse automatique, le signalement des messages urgents, la conversion des courriels en message texte pour téléphone mobile, la sauvegarde et le stockage automatiques dans des répertoires ou la conversion d'URL texte en liens à cliquer.

Nous étudierons donc le cadre juridique régissant la vérification des contenus réalisée aux fins suivantes: (A) la détection des virus, (B) le filtrage des spams (C) la détection de contenus prédéterminés.

A) La vérification des courriers électroniques visant à détecter les virus

La recherche de virus consiste à contrôler des fichiers pour voir s'ils contiennent des virus connus. Dans certains cas, elle est suivie de l'élimination des virus, procédé par lequel les virus détectés sont supprimés du fichier, de sorte qu'il puisse être utilisé en toute sécurité. En général, cette recherche a lieu à la première entrée du courriel sur les serveurs du service de messagerie électronique. Chez la plupart de ces prestataires, la recherche de virus fait partie intégrante de leur service, dans le souci de protéger leurs propres installations et celles des utilisateurs contre les virus dangereux. Les utilisateurs ne peuvent généralement pas désactiver la recherche automatique car elle est prévue par défaut dans la prestation.

---

[7] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

S'agissant des arguments juridiques légitimant cette pratique, le groupe 29 est d'avis que la mise en place et l'utilisation de dispositifs de filtrage par les services de messagerie électronique, en vue de détecter les virus, pourraient se justifier par l'obligation de prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de leurs services, imposée par l'article 4 de la directive e-vie privée précitée.

En effet, puisque la transmission de courriels contenant des virus risque de fermer le système des services de messagerie électronique (en plus d'endommager d'autres documents et logiciels stockés sur l'équipement terminal de l'utilisateur) et donc d'empêcher la transmission ultérieure des communications par courrier électronique, le groupe 29 considère que cette recherche de virus constitue une mesure de sécurité destinée à protéger le système du responsable du traitement des données (service de messagerie électronique), ce qui, ainsi qu'il a été exposé précédemment, est une obligation imposée par l'article 4 de la directive e-vie privée aux fournisseurs de services de communications électroniques.

Le groupe 29 estime par conséquent que le recours aux filtres, aux fins de l'article 4, peut être compatible avec l'article 5 de la directive e-vie privée.

Il tient à souligner en particulier que les mesures précédemment mentionnées doivent être conformes aux principes généraux du droit communautaire.

Il estime de surcroît que, lorsque les services de messagerie électronique mettent en place des dispositifs de filtrage, on peut en outre considérer qu'ils garantissent l'exécution du contrat de services conclu avec leurs clients, qui attendent un certain degré de sécurité des courriels qu'ils reçoivent et envoient. Par conséquent, le traitement de données qu'effectuent ces prestataires lorsqu'ils mettent en place les dispositifs de filtrage peut également être justifié par l'article 7, point b), de la directive sur la protection des données, qui prévoit le traitement de données «*nécessaire à l'exécution d'un contrat auquel la personne concernée est partie*».

Le filtrage visant à détecter les virus pouvant dès lors se justifier par l'obligation d'assurer la sécurité des services imposée par l'article 4 de la directive e-vie privée et/ou par la simple exécution du contrat conformément à l'article 7, point b), de la directive sur la protection des données, sans remettre en cause la confidentialité de la communication, le groupe 29 rappelle que les services de messagerie électronique sont tenus de respecter les règles suivantes:

a) le contenu des messages électroniques et de leurs annexes doit demeurer secret et n'être divulgué qu'à leur(s) destinataire(s);

b) si un virus est détecté, le logiciel installé doit offrir suffisamment de garanties de confidentialité;

c) s'il est effectué une recherche de virus par vérification du contenu, elle doit être lancée automatiquement et à cette seule fin, c'est-à-dire que le contenu ne peut être analysé dans un quelconque autre but.

Il convient de surcroît de communiquer des informations sur cette vérification (voir la partie consacrée à ce point ci-dessous).

B) La vérification des messages électroniques visant à filtrer les spams[8]

Les fournisseurs d'accès Internet et les services de messagerie électronique emploient diverses techniques pour empêcher les messages non désirés (qui ne sont pas uniquement de nature commerciale), c'est-à-dire les spams, de parvenir aux adresses désignées.

L'une d'elles consiste à mettre sur liste noire les adresses IP de certains serveurs et les plages d'adresses IP dynamiques attribuées à certains FAI[9]. La mise sur liste noire n'est toutefois pas examinée dans le présent document.

Force est de reconnaître que l'élimination des spams par filtrage est devenu une pratique nécessaire. En effet, si les services de messagerie électronique ne recouraient pas au filtrage des messages pour détecter les spams, ces derniers constitueraient une part croissante du flot de messages reçus et les systèmes deviendraient probablement très lents et inefficaces, rendant les services de messagerie pratiquement inutilisables par leurs utilisateurs. Cela susciterait sans nul doute le mécontentement des consommateurs et limiterait la possibilité d'offrir un service de messagerie fiable et sûr.

Bien que le spam ne nuise pas en soi à la sécurité des services des SME mais plutôt à l'efficacité du réseau en général, et du service de messagerie en particulier, il risque néanmoins de rendre le SME incapable de fournir ce service même. Le groupe 29 estime que l'article 4 de la directive e-vie privée, qui impose aux services de messagerie électronique de prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de leurs services, vise certes à assurer la sécurité des SME et des services en réseau proprement dits mais également l'efficacité générale des services de messagerie et de réseau. La sécurité des SME constitue un problème dans la mesure où elle affecte leurs prestations. C'est pourquoi le groupe 29 considère que l'article 4 pourrait également s'appliquer à cette situation. Autrement dit, les menaces planant sur l'efficacité générale des services de messagerie et de réseau peuvent justifier le filtrage effectué par les FAI et SME à des fins anti-spam. Les effets produits par le spam, quand bien même leur auteur ne diffuse qu'un nombre réduit d'informations par jour, mais à un nombre considérable de destinataires, confortent donc l'argument en faveur de l'application de l'article 4 de la directive e-vie privée car, même dans ces cas, l'envoi de ce nombre limité de messages risque de bloquer le trafic sur Internet et de nuire gravement à la fiabilité, à la sécurité et à l'efficacité des services de messagerie en général. Pour les mêmes raisons, le groupe 29 estime en outre que ce filtrage pourrait être légitimé par l'article 7, point b), de la directive sur la protection des données, au motif que sans le filtrage anti-spam, le service de messagerie électronique ne pourrait exécuter correctement le contrat de services auquel la personne concernée, à savoir le destinataire, est partie.

---

8 Le rapport de l'OCDE intitulé «Anti Spam Regulation», établi par la Spam Task Force en mars 2005 (DSTI/CP/ICCP/SPAM(2005)1, décrit la notion de spam dans les termes suivants: «*Le terme «spam» est largement employé dans les médias internationaux et dans les déclarations de politique faites par plusieurs pays, mais il n'en existe aucune définition généralement reconnue. Bien que faisant référence à un phénomène à peu près identique, ces pays définissent le spam d'une façon correspondant avant tout à leur environnement local. Pour élaborer une politique anti-spam, il est essentiel que la nature de ce phénomène soit bien comprise et clairement définie, et qu'il soit distingué des pratiques légitimes.*»

9 En recourant à cette technique, le service de messagerie électronique n'effectue pas de filtrage, il bloque simplement (c'est-à-dire qu'il refuse) les messages émanant des serveurs ou plages d'adresses IP figurant sur la liste noire, sans vérifier leur contenu. Si le recours à la liste noire est, en principe, moins attentatoire à la vie privée que le filtrage des contenus, il peut néanmoins soulever la question de la liberté de parole et d'expression, ainsi que celle du droit de correspondre librement et de recevoir cette correspondance, tel qu'il est reconnu à l'article 8 de la CEDH, dans son interprétation donnée par la Cour.

D'un autre côté, le groupe 29 s'inquiète de ce que le filtrage aboutisse parfois à de «faux positifs» c'est-à-dire que des messages légitimes «désirés» ne sont pas transmis à leur destinataire parce qu'ils sont considérés comme des spams. Il estime que le fait de filtrer et de retenir des messages supposément non désirés risque de conduire non seulement à une atteinte à la liberté d'expression mais également à une violation de l'article 10 de la CEDH, et de constituer une ingérence dans les communications privées[10].

C'est pourquoi, nonobstant l'application de l'article 4 de la directive e-vie privée, et afin de garantir le principe de liberté des communications tel qu'il est reconnu par l'article 10 de la CEDH, ainsi que leur confidentialité prévue à l'article 5 de la directive et reconnue par l'article 8 de la convention, le groupe 29 invite vivement les services de messagerie électronique à suivre les recommandations émises ci-après, dont l'objectif premier est de donner aux destinataires des messages électroniques un contrôle sur les communications qui leur sont en principe destinées:

a) le groupe 29 est partisan de la pratique consistant à permettre aux abonnés de choisir que leurs messages électroniques ne soient pas vérifiés pour détecter les spams, de contrôler les messages réputés spams pour s'assurer qu'il s'agit bien de spams, et de décider quelle «sorte» de spam doit être éliminée par filtrage. En outre, il est favorable à la possibilité offerte par certains SME à leurs abonnés de pouvoir facilement réintégrer la vérification de leurs messages visant à détecter les spams;

b) le groupe 29 encourage également la mise au point d'outils de filtrage pouvant être installés ou configurés par les utilisateurs, soit sur l'équipement terminal soit sur des serveurs tiers ou le serveur email du prestataire, et leur permettant de décider ce qu'ils souhaitent et ne souhaitent pas recevoir, ce qui contribuera à réduire les coûts engendrés par le téléchargement de messages électroniques non sollicités, ainsi que le rappelle le considérant 44 de la directive 2002/58. Il est en outre favorable à la recherche d'autres outils de lutte contre le spam qui soient moins attentatoires à la vie privée.

Par ailleurs, le groupe 29 rappelle aux services de messagerie électronique procédant à la vérification des messages en vue de détecter les spams leur obligation, mentionnée à l'article 10 de la directive sur la protection des données, d'informer les abonnés de leur politique en matière de spam, d'une manière claire et précise, ainsi que l'explique la partie IV du présent avis. Le prestataire doit en outre garantir la confidentialité des messages filtrés, qui ne sauraient servir à une quelconque autre fin.

[10] Ainsi que la Cour l'a admis dans l'affaire Schöneberger & Durmaz, en 1988.

C) La vérification des messages électroniques visant à détecter des contenus prédéterminés

Le groupe 29 observe que certains services de messagerie électronique se réservent le droit de vérifier et même de supprimer des contenus prédéterminés[11], par exemple s'ils contiennent des éléments jugés illicites ou dont le destinataire, utilisateur de ce service, ne veut pas. Les moyens techniques utilisés pour ce type de vérification sont très proches de ceux servant à détecter les virus et les spams.

Or, contrairement à la recherche de virus, la vérification des messages visant à détecter des contenus prédéterminés, même considérés comme des éléments supposés illicites, ne peut être assimilée à une mesure d'ordre technique et organisationnel appropriée afin de garantir la sécurité des services de messagerie, tel que le prévoit l'article 4 de la directive e-vie privée. En effet, le service de messagerie électronique ne court pas le risque d'être atteint, ni les communications d'être interrompues, par les éléments figurant dans les messages. C'est pourquoi la vérification visant à détecter ces éléments n'est pas justifiée par le besoin du service de messagerie de garantir la sécurité du service. Le groupe 29 est également préoccupé de ce qu'en procédant à ce type de filtrage, les services de messagerie électronique s'érigent en censeurs des communications privées, par exemple en bloquant des communications dont le contenu peut être tout à fait licite, soulevant ainsi des questions fondamentales sur la liberté de parole, d'expression et de l'information. Le groupe tient à rappeler que les prestataires de services n'ont aucune obligation générale de surveiller les contenus prédéterminés ou jugés nuisibles mais que, ainsi qu'il sera développé ci-après, ce type de service peut être proposé par un prestataire à titre de valeur ajoutée.

Par conséquent, le groupe 29 est d'avis que, conformément à l'article 5, paragraphe 1, de la directive e-vie privée, il est interdit aux services de messagerie électronique de filtrer et de stocker les communications et les données de trafic y afférentes ou de les soumettre à tout autre moyen d'interception, en vue de détecter des contenus prédéterminés, sans le consentement des utilisateurs concernés, sauf à y être légalement autorisés conformément à l'article 15 de la directive e-vie privée telle que transposée dans les États membres.

IV. OBLIGATION D'INFORMER

Outre l'article 5 de la directive e-vie privée, le traitement de données à caractère personnel aux fins de connaître le contenu et/ou les données de trafic relatifs à des communications privées est soumis à diverses dispositions de la directive sur la protection des données.

---

[11] Voir les conditions d'utilisation de Yahoo!: «Vous reconnaissez que Yahoo! ne peut visionner le Contenu avant sa diffusion. Néanmoins Yahoo!, ou toute personne ou entité désignée par cette société, se réserve le droit, à sa seule discrétion, (sans que cela ne constitue une obligation) de visionner, de refuser ou de déplacer tout Contenu disponible via le Service. Par ailleurs, Yahoo!, ou toute personne ou entité désignée par cette société, sera en droit de supprimer ou de retirer tout Contenu qui violerait les termes des présentes ou serait répréhensible de toute autre façon. Vous reconnaissez également que vous devez faire preuve de discernement, et supporter tous les risques y afférant, dans l'utilisation que vous faites du Contenu et notamment lorsque vous vous fiez à l'opportunité *(sic)*, l'utilité ou le caractère complet de ce Contenu. En conséquence, vous reconnaissez que vous ne pouvez vous fier ni au Contenu créé par Yahoo! ni au Contenu soumis à Yahoo!, notamment disponible dans les Forums ou les Clubs Yahoo! ou dans toutes autres parties du Service. Vous reconnaissez et acceptez que Yahoo! consulte, conserve et divulgue les informations relatives à votre compte et le Contenu si Yahoo! y est obligé pour se conformer aux lois en vigueur ou si, de bonne foi, Yahoo! pense qu'une telle mesure est nécessaire : (i) dans le cadre d'une procédure judiciaire, (ii) pour faire respecter les Conditions d'Utilisation du Service, (iii) pour répondre à des plaintes arguant de la violation des droits de tiers, (iv) pour répondre à vos demandes adressées au service clients, ou (v) pour protéger les droits ou les intérêts de Yahoo!, ses utilisateurs ou le public.»

Cette dernière prévoit notamment une obligation d'informer les personnes physiques du traitement des données à caractère personnel les concernant. En particulier, son article 10 «*Informations à fournir à la personne concernée*» oblige les responsables du traitement à fournir certaines informations aux personnes auprès desquelles des données sont collectées, dont l'identité du responsable du traitement et les finalités du traitement auquel les données sont destinées. En outre, l'article 6, paragraphe 1, point a), de la directive sur la protection des données dispose que celles-ci doivent être traitées loyalement et licitement, ce qui renforce l'obligation des responsables du traitement d'assurer la totale transparence des conditions de traitement des données concernant ces personnes.

S'agissant du filtrage visant à détecter les virus et le spam, le groupe 29 estime que la pratique des SME consistant à informer les abonnés dans le cadre des conditions d'utilisation du service est appropriée.

Outre les dispositions qui précèdent, les SME doivent se conformer à l'article 4 de la directive e-vie privée, qui impose aux fournisseurs d'un service de communications électroniques accessible au public d'informer les abonnés de tout risque particulier de violation de la sécurité du réseau. Si les mesures que peut prendre le fournisseur du service ne permettent pas d'écarter ce risque, il doit informer ses utilisateurs et abonnés des mesures qu'il leur est possible d'appliquer pour assurer la sécurité de leurs communications.

V. AUTRES PRESTATIONS LIÉES AU COURRIER ÉLECTRONIQUE

Le groupe 29 observe le développement d'un nouveau type de logiciels et de services, comme le «DidTheyReadIt» («l'ont-ils lu?») qui permet de vérifier si un message a été ouvert.

Ce service met toute personne qui y est abonnée en mesure de savoir a) si les destinataires de ses messages électroniques les ont lus, b) à quel moment, c) combien de fois ils les ont lus (ou, au moins, ouverts), d) s'ils les ont transmis à d'autres personnes, et e) vers quel serveur de messagerie, y compris sa localisation. Enfin, il permet également de connaître le navigateur utilisé par le destinataire ainsi que son système d'exploitation.

Le traitement des données se déroule à l'insu des destinataires des messages électroniques, c'est-à-dire qu'ils ne reçoivent aucune information sur le traitement de données dont ils font l'objet. De plus, ils n'ont pas le choix d'accepter ou de refuser cette extraction d'informations. En résumé, à la différence des services «classiques» d'accusé de réception de messages, le destinataire n'a pas la possibilité d'accepter ou de refuser de retourner les informations à l'utilisateur du logiciel.

Le groupe 29 émet les plus vives réserves sur ce procédé car des données personnelles sur le «comportement» du destinataire sont ainsi enregistrées et transmises sans qu'il y ait eu consentement indubitable de sa part. Un tel traitement, effectué à l'insu des personnes concernées, est contraire aux règles de protection des données qui exigent loyauté et transparence dans la collecte des données à caractère personnel, conformément à l'article 10 de la directive sur la protection des données.

Pour pouvoir réaliser le traitement de données consistant à rechercher sur le terminal du destinataire d'un courriel s'il l'a lu, quand il l'a lu et s'il l'a transmis à des tiers, son consentement indubitable est nécessaire. Aucun autre argument juridique ne saurait justifier ce traitement. Par conséquent, un traitement de données effectué à l'insu des personnes concernées est contraire aux règles de protection des données qui exigent un consentement donné indubitablement, ainsi qu'en dispose l'article 7 de la directive sur la protection des données.

VI. CONCLUSION

Le groupe 29 a jugé utile de publier le présent avis afin de dissiper l'incertitude qui entoure la compatibilité du filtrage des communications électroniques et de répondre à la demande d'orientations des parties intéressées.

Il invite les services de messagerie électronique à suivre les indications et recommandations exposées dans l'avis lors de la prestation de leurs services. En outre, dans le souci de promouvoir les technologies intégrant la protection des données et les exigences de la protection de la vie privée dans la conception des infrastructures et des systèmes d'information, y compris les équipements terminaux, le groupe 29 souhaite encourager les développeurs de logiciels de courrier électronique à concevoir et à mettre au point des systèmes respectant la vie privée, de façon à réduire le traitement des données à caractère personnel au strict minimum, en le limitant à ce qui est absolument nécessaire et proportionné à ses finalités.

Fait à Bruxelles, le 21.02.06.

Pour le groupe de travail,

Le président
Peter Schaar