LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

PETER HUSTINX
CONTROLEUR

M. Bernd LANGEHEINE
Directeur B – Chef d'unité (faisant fonction) B.1
DG INFSO
Commission européenne
B - 1049 Bruxelles

Bruxelles, le 6 octobre 2010
PH/RB/et/D(2010)1516 **C 2010-0645**

Monsieur Langeheine,

Je vous écris afin de participer à la consultation publique organisée par la DG INFSO au sujet de l'internet libre et de la neutralité du web en Europe. Nous avons appris de vos services que cette contribution sera tout de même prise en considération, malgré le fait que le délai pour les contributions a expiré la semaine dernière.

La neutralité de l'internet pose des problèmes au niveau de la protection et de la confidentialité des données. Comme vous le savez peut-être, au titre du règlement (CE) n° 45/2001[1], le Contrôleur européen de la protection des données («CEPD») est compétent pour conseiller les institutions et organes de l'UE au sujet des questions relatives à la protection et à la confidentialité des données dans une série de domaines politiques. Ces observations doivent être envisagées en tenant compte de ce rôle et ciblent la consultation publique actuellement organisée par la DG INFSO, susceptible d'entraîner l'adoption ultérieure de mesures politiques dans le domaine de la neutralité du web.

Les services du CEPD sont à votre disposition pour toute explication relative à ces observations.

Cordialement,

(**signé**)

Peter Hustinx

[1] Règlement (CE) n° 45/2001 du 18 décembre 2010 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

En copie: M. Ivan Brincat, M^{me} Anna Buchta, M. Achim Klabunde, M^{me} M.H. Boulanger, M. P. Renaudière

Personne de contact: M^{me} Rosa Barcelo (02-2831927)

OBSERVATIONS DU CEPD CONCERNANT LA NEUTRALITÉ DE L'INTERNET ET LA GESTION DU TRAFIC

Contribution à la consultation publique de la DG INFSO sur l'internet libre et la neutralité du web en Europe

I. Contexte

1. Il peut arriver que les fournisseurs de services de communication électronique, comme par exemple les FAI, participent à la «gestion du trafic». En fonction des mécanismes de gestion du trafic utilisés, ils peuvent examiner le contenu des communications, notamment les adresses URL consultées, les informations téléchargées (films, musique), les communications par courrier électronique, etc., dans le but éventuel de traiter différemment chaque communication, généralement en attribuant différents niveaux de qualité ou de vitesse.

2. Ces activités sont exécutées en utilisant des technologies permettant l'examen des paquets numériques formant les messages ou les transmissions par réseau. L'examen initial permet au fournisseur, en fonction du contenu en question, d'attribuer un niveau de priorité donné à chaque type de paquet numérique, ou tout simplement de le bloquer. Les paquets numériques composant un message ou une transmission sont évidemment reliés à un utilisateur donné, étant donné que chacun d'entre eux porte l'adresse IP de l'expéditeur et du destinataire.

3. Les raisons de gérer le trafic en traitant chaque paquet différemment peuvent être multiples. Par exemple, il peut arriver que la demande de bande passante soit supérieure à la capacité du réseau, ce qui peut entraîner une dégradation du service. Pour résoudre ce problème, on peut privilégier certains flux ou en retarder d'autres, afin de garantir une certaine qualité de service, particulièrement lorsqu'il s'agit de données variant avec le temps. La gestion du trafic peut également servir à assurer la qualité ou fiabilité particulièrement élevée nécessaire pour certains services. Une différentiation peut également être effectuée à des fins de sécurité, p.ex. afin de rechercher des virus, des codes ou courriers indésirables dangereux, ou encore pour filtrer certains contenus illégaux. La gestion du trafic peut aussi éventuellement servir à privilégier les fournisseurs de contenu disposés à payer des tarifs plus élevés (afin de conserver une vitesse élevée).

4. Le CEPD note que la mise en œuvre des politiques de gestion du trafic peut impliquer le contrôle des informations personnelles des utilisateurs et notamment des données de trafic et de contenu, ce qui pose de sérieux problèmes au niveau de la protection et de la confidentialité des données. Malheureusement, le questionnaire servant de référence à la consultation publique sur l'internet libre et la neutralité du web ne fait aucune référence à la protection et à la confidentialité des données, ce qui, comme expliqué ci-dessous, devra être pris dûment en considération par la Commission au moment d'élaborer des politiques à ce sujet.

II. Mécanismes de gestion du trafic: répercussions sur la protection et la confidentialité des données

5. En ce qui concerne la protection et la confidentialité des données, il convient de tenir particulièrement compte de deux aspects liés à l'application des mécanismes de gestion du trafic: **premièrement**, la capacité des fournisseurs à examiner le contenu des messages ou des transmissions et, **deuxièmement**, la possibilité d'attribuer ces informations à un

utilisateur particulier. Les mécanismes de gestion du trafic permettent de collecter les informations relatives au contenu et au trafic appartenant aux utilisateurs. Globalement, comme expliqué plus en détail ci-dessous, l'impact potentiel de cette activité sur la protection des données à caractère personnel et de la vie privée des personnes pourrait être considérable.

6. En interceptant les données relatives au trafic, les mécanismes de gestion du trafic peuvent violer la confidentialité des communications, qui constitue un droit fondamental garanti par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (la «CEDH») et par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (la «Charte»). La confidentialité est également protégée par le droit dérivé de l'UE, à savoir par l'article 5 de la directive relative à la vie privée et aux communications électroniques[2]. Cet article dispose que «[l]*es 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, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité».*

7. Par ailleurs, la mise en œuvre de ces politiques permet aux fournisseurs de collecter de grandes quantités de données à caractère personnel pouvant concerner des millions d'utilisateurs; en outre, la collecte et le traitement de ces données sont particulièrement invasifs si l'on tient compte du fait qu'ils peuvent inclure les enregistrements des activités de tous les utilisateurs de l'internet: films téléchargés, courriers électroniques échangés, recherches, etc.

8. **Au vu de ce qui précède, le CEPD insiste sur le fait que la Commission doit prendre en considération les aspects relatifs à la confidentialité et à la protection des données lorsqu'elle envisage d'adopter des politiques sur la neutralité du web et la gestion du trafic. Une attention particulière doit être accordée au cadre juridique décrit ci-dessous.**

III. Cadre légal applicable en matière de gestion du trafic dans le domaine de la protection des données et du respect de la vie privée

a) Cadre juridique de l'UE en vigueur

9. Le droit de l'UE prévoit des garanties en matière de protection de la vie privée et des données dans le cadre de la confidentialité des communications. Il importe de rappeler ce cadre juridique de l'UE au moment d'examiner l'évolution des politiques de l'UE en matière de gestion du trafic, et en particulier l'article 5, paragraphe 1, de la directive relative à la vie privée et aux communications électroniques, portant sur la confidentialité des communications et interdisant *«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 de la personne concernée. Est également pertinent l'article 6, paragraphe 1, disposant que les données relatives au trafic doivent être effacées dès que leur stockage n'est plus nécessaire à des

[2] 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.

fins liées à la communication elle-même (y compris à des fins de facturation)[3]. Les dérogations à ces dispositions sont soumises à de strictes conditions.

10. Lorsqu'il aborde l'utilisation des mécanismes de gestion du trafic, le considérant 28 de la directive concernant le service universel et les droits des utilisateurs[4] fait explicitement référence à ce cadre juridique en indiquant qu'il s'applique aux mécanismes de gestion du trafic: *«Les utilisateurs devraient, en tout état de cause, être pleinement informés de* ***toute limitation imposée par le fournisseur de service et/ou de réseau quant à l'utilisation de services de communications électroniques****. Ces informations devraient préciser, au choix du fournisseur, soit le type de contenu, d'application ou de service concerné, soit des applications ou services déterminés, soit les deux».* Le considérant indique ensuite ce qui suit: *«Selon la technologie utilisée et le type de limitation, ces limitations peuvent être subordonnées à un accord de l'utilisateur en vertu de la directive 2002/58/CE (directive Vie privée et communications électroniques)»*[5].

b) Application du cadre aux mécanismes de gestion du trafic

11. Au vu de ce qui précède, si les fournisseurs de services de communication électronique mettent en place des politiques de gestion du trafic impliquant l'interception ou la surveillance des communications, l'article 5 de la directive Vie privée et communications électroniques s'applique et exige le consentement éclairé des utilisateurs concernés, c'est-à-dire de toutes les personnes impliquées dans la communication en question. Si la transparence (et l'information des personnes) est un élément essentiel de la protection des données à caractère personnel et de la vie privée des personnes, elle n'est pas à elle seule suffisante. Comme expliqué plus en détail ci-dessous, une fois informées, les personnes doivent accepter, c'est-à-dire consentir à ce que leurs contenus et données de trafic soient traités au regard des finalités des politiques de gestion du trafic mises en œuvre par le fournisseur.

12. Le consentement à l'interception des communications et donc au traitement des données à caractère personnel doit être interprété au sens de l'article 2, point h), de la directive sur la protection des données[6]. Aux termes de cet article, pour que le consentement soit valable, il doit être donné de manière à permettre à l'utilisateur d'indiquer librement, de manière spécifique et informée qu'il accepte que des données à caractère personnel le concernant soient traitées. Le considérant 17 de la directive Vie privée et communications électroniques confirme ce principe: «[l]*e consentement peut être donné selon toute modalité*

---

[3] Comparer également la récente proposition de la Commission en vue d'une directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil, COM(2010) 517 final. L'article 6 de la proposition vise à faire de l'interception des transmissions de données une infraction pénale.

[4] Directive 2009/136/CE du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

[5] Dans certains cas précis, le consentement n'est pas toujours nécessaire. Ce principe est tiré de l'article 4 de la directive Vie privée et communications électroniques, qui dispose que *«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».* En interprétant cette disposition, le groupe de protection des données établi par l'article 29 de la directive a indiqué que la mise en place et l'utilisation de systèmes de filtrage par les fournisseurs de messageries électroniques dans le but de détecter les virus pouvaient se justifier par l'obligation d'adopter les mesures techniques et organisationnelles nécessaires pour assurer la sécurité de leurs services, conformément à l'article 4 de la directive Vie privée et communications électroniques. Voir l'avis 2/2006 du groupe de travail sur les problèmes de protection de la vie privée liés à la fourniture de services de filtrage du courrier électronique, adopté le 21 février 2006.

[6] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet».

13. Le consentement exprimé dans le cadre de l'acceptation générale des conditions régissant l'éventuel contrat principal (p.ex. un contrat d'abonnement, pour lequel le consentement est également demandé afin de permettre la gestion du trafic et, par là-même, la violation de la confidentialité des communications) doit satisfaire aux dispositions de la directive sur la protection des données, c'est-à-dire être donné librement, de manière spécifique et informée.

14. Concrètement, les exigences minimales sont les suivantes:

    a) fournir suffisamment d'informations aux utilisateurs;
    b) utiliser le langage adéquat afin de veiller à ce que les utilisateurs comprennent ce à quoi ils consentent et à quelles fins. L'utilisation d'un jargon juridique ou technique trop compliqué serait contraire aux dispositions de la loi;
    c) les informations fournies aux utilisateurs doivent être claires et suffisamment visibles pour ne pas passer inaperçues. Il convient pour cela d'utiliser des méthodes ciblées, comme par exemple des formulaires de consentement spécifiques (plutôt que d'insérer les informations dans les conditions générales du contrat et demander une signature globale du contrat);
    d) les finalités du mécanisme et des politiques de gestion du trafic doivent être suffisamment précisées. Si les finalités de la gestion du trafic ne sont pas suffisamment précisées, dans le but, par exemple, de permettre au fournisseur de continuer à utiliser les données à diverses fins, les dispositions légales ne sont pas non plus respectées;
    e) enfin, le consentement exprimé aux termes du cadre juridique applicable exige également une action explicite de la part de l'utilisateur afin que celui-ci signifie clairement son accord. Un consentement implicite ne suffirait pas à satisfaire à cette norme.

15. Outre ce qui précède, il importe également de souligner que pour qu'un consentement soit librement exprimé, l'utilisateur doit avoir la possibilité de choisir réellement de consentir ou de ne pas consentir. Les utilisateurs pourraient éprouver des difficultés à faire un tel choix si *tous* les fournisseurs d'un marché donné effectuaient des activités de gestion du trafic. Dans un tel cas de figure, les utilisateurs refusant que leurs données soient contrôlées n'auraient pas d'autre choix et ne pourraient pas trouver d'autre service disponible sur le marché. La seule possibilité qu'il leur resterait serait de ne pas s'abonner du tout à un service internet. L'internet joue un rôle de plus en plus important dans la vie courante. Étant donné qu'il est devenu un outil essentiel, tant pour la vie professionnelle que pour la vie privée, ne pas s'abonner à un service internet n'est pas une possibilité envisageable. Par conséquent, les personnes n'auraient pas de véritable choix: elles ne pourraient pas donner librement leur consentement. Le CEPD demande à la Commission de prendre ce fait en considération, particulièrement si ce scénario est crédible (c'est-à-dire s'il est possible que tous les fournisseurs exercent des activités de gestion du trafic). Un éventuel moyen de résoudre ce problème serait de contraindre les fournisseurs à proposer un autre service, comme par exemple un abonnement internet qui ne ferait pas l'objet d'un contrôle du trafic[7].

[7] Un autre problème non mentionné ici concerne la faisabilité de l'obtention du consentement de ***tous*** les utilisateurs participant à une communication, comme l'exige l'article 5, paragraphe 1. En effet, pour obtenir le consentement de tous les utilisateurs, il faudrait non seulement obtenir le consentement de l'abonné, mais aussi celui de l'expéditeur (qui n'est pas forcément abonné). Les modalités d'application concrète de cette disposition ne sont pas claires.

16. Dernier point, mais non des moindres: la conservation de données à caractère personnel dans le cadre de l'utilisation de technologies de gestion du trafic doit également respecter d'autres principes dérivés de la directive sur la protection des données et de la directive Vie privée et communications électroniques. Ces principes peuvent être particulièrement pertinents, selon la politique envisagée, mais il n'est pas utile de les aborder à ce stade.

17. En résumé, la législation de l'UE en matière de protection des données prévoit des garanties en matière de confidentialité et de protection des données en vertu du principe de confidentialité des communications, qui doivent être conservées dans les prochaines politiques élaborées au sujet de la neutralité du web et de la gestion du trafic.

IV. Recommandations

18. Au vu de ce qui précède, le CEPD recommande que lors de la présentation de politiques sur la neutralité du net et plus particulièrement sur la gestion du trafic, la Commission:

    a) prenne en considération les questions relatives à la confidentialité et à la protection des données, en plus des autres droits et valeurs établis;

    b) préserve le cadre juridique existant en matière de confidentialité et de protection des données, à savoir la disposition prévoyant que les mécanismes de gestion du trafic permettant d'examiner les communications (contenu et trafic) ne peuvent être autorisés qu'à condition que les utilisateurs concernés aient librement exprimé leur consentement, de manière spécifique et informée.

Bruxelles, le 6 octobre 2010