COMMENTAIRES DU CEPD SUR LA CONSULTATION PUBLIQUE DE LA DG CONNECT SUR «DES ASPECTS SPÉCIFIQUES DE LA TRANSPARENCE, DE LA GESTION DU TRAFIC ET DES CHANGEMENTS DE FOURNISSEURS, DANS LE CADRE DE L'INTERNET OUVERT»

La Commission européenne a lancé une consultation publique visant à obtenir des contributions sur des aspects spécifiques apparaissant comme des questions clés dans le débat sur la neutralité de l'internet qui a eu lieu en Europe ces dernières années. L'objectif principal de l'action de la Commission dans ce domaine est d'habiliter les consommateurs à faire des choix informés dans un marché compétitif régi par des règles claires, par le biais de mesures politiques visant à traiter les questions de la transparence, du changement de fournisseurs et de certains aspects de la gestion du trafic, dont l'inspection approfondie des paquets (IAP)[1].

Le CEPD accueille favorablement l'initiative de la Commission de consulter un large éventail de parties intéressées, comprenant les secteurs public et privé ainsi que la société civile, sur les questions relatives à la neutralité de l'internet. Le CEPD considère cette consultation comme une partie importante du débat, qui doit avoir lieu avant l'élaboration de toute recommandation politique ou mesure juridique.

Le CEPD prend note du fait que l'initiative de la Commission fait suite à une investigation sur la gestion du trafic menée par l'Organe des régulateurs européens des communications électroniques (ORECE)[2] entreprise à la demande de la Commission.

I. Pertinence de la protection des données à caractère personnel dans le contexte du débat sur la neutralité de l'internet

Les pratiques de gestion du trafic, plus particulièrement celles impliquant l'examen des communications des citoyens sur l'internet au moyen de techniques d'inspection approfondie des paquets, présentent un risque élevé pour la vie privée et la protection des données à caractère personnel des personnes. Il se peut qu'en inspectant les données de communication, les fournisseurs de service internet (FSI) s'immiscent dans la vie privée des personnes et violent la confidentialité des communications, droit fondamental garanti par l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après, la «CEDH») et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après,

[1] Les technologies d'inspection approfondie des paquets examinent différentes couches (en-tête et contenu) des paquets de données et, en fonction des résultats, traitent davantage ces paquets. Les actions en résultant comprennent l'acheminement, la priorisation, le verrouillage des paquets, etc., en fonction des politiques prédéfinies. Des exemples de telles actions sont la priorisation ou le filtrage du trafic VoIP ou P2P par des FSI, ou des mesures de sécurité spécifiques lorsqu'un virus est découvert dans les paquets.

[2] Cf. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf .

Adresse: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

la «Charte»). La confidentialité est en outre protégée par le droit dérivé de l'UE, à savoir l'article 5 de la directive «vie privée et communications électroniques»[3].

L'importance du respect de la vie privée et de la protection des données augmente avec la convergence de toutes les communications vers l'internet et le rôle de plus en plus central qu'il joue dans la vie de chacun. Les fournisseurs de service internet peuvent avoir un aperçu inégalé de la vie privée de chacun s'ils pouvaient librement accéder aux communications et les traiter à des fins qui leur sont propres.

Le CEPD a déjà contribué au débat à de multiples occasions, en particulier par le biais de commentaires transmis sur la consultation publique de la Commission sur «l'internet ouvert et la neutralité de l'internet en Europe»[4] et de l'avis du CEPD sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles[5].

Néanmoins, nous souhaitons saisir l'opportunité de cette consultation publique pour souligner certains points relevés par les questions de la consultation de sorte que la Commission puisse tenir compte des considérations du CEPD lors de l'élaboration de futures actions politiques dans ce domaine.

II. Problème général: la gestion du trafic internet et les données à caractère personnel (question 9)

Comme nous l'avons précisé dans notre avis sur la neutralité de l'internet, nous soutenons le concept d'un internet ouvert. Les FSI ont le droit d'élaborer des mesures de gestion du trafic, à condition qu'elles respectent entièrement les exigences relatives à la vie privée et à la protection des données.

L'utilisation de techniques d'inspection approfondie des paquets implique le traitement par les FSI d'un nombre considérable de données relatives aux utilisateurs internet, beaucoup d'entre elles étant considérées comme personnelles (par exemple, les adresses IP), confidentielles (par exemple, le contenu des communications)[6], ou même sensibles (par exemple, les informations concernant la santé). Conformément à l'article 7 de la directive 95/46/CE sur la protection des données et à l'article 5 de la directive «vie privée et communications électroniques», il convient de trouver une

[3] 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 (directive «vie privée et communications électroniques»), JO L 201 du 31 juillet 2002 page 37, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009.

[4] Observations du CEPD sur la consultation publique de la Commission sur «l'internet ouvert et la neutralité de l'internet en Europe», 6 octobre 2010, disponible sur le site: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_FR.pdf.

[5] Cf. avis du CEPD sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles, 7 octobre 2011, disponible sur le site http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_FR.pdf.

[6] Cf. avis du groupe de travail «Article 29» sur le concept de données à caractère personnel, 20 juin 2007, pages 16-17, disponible sur le site http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf.

base juridique appropriée pour justifier le traitement des données personnelles dans le contexte de la gestion du trafic internet.

La gestion du trafic est effectuée par les FSI à de nombreuses fins. Les finalités traditionnelles sont la sécurité du réseau et la gestion de la congestion. Les techniques d'inspection du trafic se fondent sur l'analyse des protocoles internet à différentes couches du paquet, principalement pour lire les adresses IP d'origine et de destination et les protocoles internet, ce qui est dans la plupart des cas suffisant pour des fins de gestion de congestion et de limitation du trafic. Comme le CEPD l'a expliqué en détail dans son avis sur la neutralité de l'internet[7], les FSI peuvent généralement, en vertu de la directive «vie privée et communications électroniques», réaliser ce type de traitement afin de transmettre les communications, garantir la sécurité du service des communications, ou minimiser la congestion.

Au fil des ans, de nouvelles finalités ont vu le jour, comme la spécialisation du service et la différenciation des niveaux de service, basées ou non sur des contrats avec le consommateur, menant à l'inspection et au filtrage du trafic internet selon l'application/le service spécifique. Des finalités plus récentes impliquant une inspection globale du trafic internet comprennent une analyse comportementale et un profilage, utilisés principalement pour des raisons de sécurité, mais également pour des utilisations commerciales, relatives à la protection des droits d'auteur et autres. Ces nouvelles finalités peuvent être bien plus intrusives que les finalités traditionnelles en ce qui concerne la vie privée et la protection des données, plus particulièrement lorsqu'elles peuvent entraîner le suivi du comportement en ligne des abonnés internet[8]. Comme le CEPD le décrit dans son avis sur la neutralité de l'internet[9], certaines de ces activités de traitement peuvent sortir du champ d'application autorisé par la loi. Plus particulièrement, lorsque ces opérations de traitement n'ont pas été prévues de manière explicite dans la directive «vie privée et communications électroniques» et/ou ne respectent pas pleinement d'autres obligations incombant aux FSI, telles que celles établies dans l'article 15 de la directive sur le commerce électronique, il convient d'évaluer à tout le moins soigneusement (i) si chacune de ces opérations de traitement est nécessaire et proportionnée à l'objectif poursuivi, et (ii) si elles se fondent sur une base juridique suffisante en vertu de l'article 7 de la directive 95/46/CE. En l'absence d'un tel fondement dans la législation, elles doivent se baser sur un autre fondement juridique, comme le consentement.

Dès lors, les politiques de gestion du trafic doivent être élaborées dans le plein respect des droits fondamentaux et conformément au cadre juridique existant en matière de communications électroniques, de commerce électronique et de protection des données.

[7] Pour plus de détails, cf. avis du CEPD sur la neutralité de l'internet, pages 10-12.
[8] Les mesures qui visent le suivi général de l'internet ne peuvent être réalisées que conformément à la loi (plus particulièrement l'article 15 de la directive sur le commerce électronique). Ce principe a été repris par la Cour de justice de l'Union européenne dans l'affaire C-70/10, Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), arrêt du 24 novembre 2011.
[9] Cf. avis du CEPD, pages 10-14.

III. Commentaires spécifiques

a) Techniques d'inspection et risques d'atteinte à la vie privée (question 10a)

Une description détaillée des problèmes soulevés par l'utilisation de l'inspection approfondie des paquets du point de vue de la vie privée et de la protection des données personnelles figure dans l'avis du CEPD sur la neutralité de l'internet[10]. Les risques d'atteinte à la vie privée, à la protection des données et à la confidentialité des communications sont très élevés en raison du caractère hautement intrusif de l'inspection approfondie des paquets, qui analyse l'entièreté du contenu des paquets IP afin de trouver des configurations spécifiques en le comparant à des critères prédéfinis établis dans les politiques d'inspection.

L'impact de ces mesures a encore augmenté en raison de la convergence croissante de tous types de communications vers l'internet, y compris celles contenant des données personnelles sensibles. En outre, les communications traditionnelles se déplacent vers l'internet. L'accès universel est stimulé par l'offre croissante de services pour les appareils mobiles «intelligents». En plus d'ajouter les données de localisation relatives au téléphone portable traditionnel aux informations habituellement traitées, l'utilisation d'appareils «intelligents» permet de rassembler davantage d'informations par les capteurs qu'ils comportent, comme des données de localisation plus détaillées grâce aux antennes GPS et aux appareils photo à haute résolution. Dans certains cas (utilisation de mêmes FSI, voire de mêmes passerelles physiques), tous les types de communication passent par le même point d'accès, augmentant ainsi la convergence physique des données personnelles relatives à la même personne et aux autres personnes avec qui celle-ci communique.

Dès lors, les FSI peuvent rassembler de larges quantités de données relatives à la même personne qui peuvent faciliter le rassemblement exhaustif de renseignements et le profilage. En outre, il pourrait être tentant d'utiliser des données personnelles rassemblées de manière illégale à des fins commerciales, plus particulièrement pour la publicité comportementale et la publicité ciblée. L'expérience a démontré que la disponibilité de nouvelles possibilités de collecte et de traitement des données suscite souvent un intérêt pour l'utilisation des données disponibles à de nouvelles fins, au-delà de ce qui était prévu à l'origine, communiquée aux individus concernés et qui ont indiqué leur consentement. La mise en place d'infrastructures globales pour l'inspection approfondie des paquets dans les réseaux de communication peut attiser un tel intérêt, par exemple pour des raisons économiques ou d'application de la loi. À moins que l'infrastructure ne soit équipée de moyens pour détecter l'utilisation non autorisée, il peut être difficile de détecter et de prouver les violations de la vie privée qui en résultent.

b) Gestion du trafic et alternatives à l'inspection approfondie des paquets (question 10b)

Les techniques traditionnelles de gestion des paquets utilisent les champs d'information de l'en-tête du paquet pour en traiter les flux. Certains nouveaux types d'application/service internet ne peuvent plus être identifiés par la simple inspection

[10] Cf. section V, paragraphe 4, page 17.

des champs relatifs au protocole, mais portent leur identité dans les données utiles du paquet[11]. Cela est parfois fait délibérément (changement des ports standards TCP/UDP, tunnellisation, etc.) pour entraver une identification aisée de l'application. Pour un contrôle plus détaillé, l'information est recherchée dans les données utiles.

Le CEPD estime que les recherches sur des alternatives à l'inspection approfondie des paquets favorables à la vie privée devraient être encouragées. Dans cette optique, il souhaite souligner des points spécifiques qui doivent être pris en compte pour aider au développement d'alternatives favorables à la vie privée:

- La limitation des finalités et les principes de proportionnalité devraient toujours guider l'exploration et l'adoption des techniques de gestion/traitement du trafic et des communications actuelles et futures. Le principe de proportionnalité, tel qu'il est exprimé dans l'article 6, paragraphe 1, point c), de la directive 95/46/CE, exige que les données personnelles traitées soient «non excessives au regard des finalités pour lesquelles elles sont collectées». Comme le CEPD l'a indiqué dans son avis, le principe de proportionnalité doit servir de principe directeur aux FSI; il doit promouvoir l'utilisation des méthodes les moins intrusives pour l'inspection des communications électroniques et l'application des garanties en matière de protection des données, comme la pseudo-anonymisation[12].

- Le processus de normalisation des protocoles de communication a toujours eu pour objectif de mettre les champs d'informations de l'application/du service au niveau du protocole (généralement, par définition, sur la couche d'application). Le CEPD estime que cette intention fondamentale doit être conservée à l'avenir et encourage les efforts fournis pour l'évaluation de l'adéquation actuelle des couches de la pile du protocole internet en ce qui concerne les derniers besoins du marché.

- Dans de nombreux cas, les services qui peuvent exiger des pratiques spécifiques de gestion du trafic peuvent être identifiés par les adresses IP qu'ils utilisent (par exemple, moteurs de recherche, portails vidéo). L'utilisation des adresses IP des services demandés comme indicateur du type de service doit être poursuivie pour l'identification du service. Cette information pourrait également être utile pour mieux acheminer les ressources demandées au client.

- Des recherches sur les méthodes permettant de déduire le type de service/application à partir de certaines caractéristiques statistiques des paquets et du flux du paquet doivent être stimulées.

- Une offre équitable de largeur de bande sur ce qui est défini dans le contrat entre le FSI et les abonnés limiterait le problème.

[11] Pour une initiation à la transmission des informations par le biais de l'internet et les techniques d'inspection, cf. les sections IV, paragraphe 1, et IV, paragraphe 2, de l'avis, op.cit.

[12] Cf. avis sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles, 7 octobre 2011, paragraphes 68-72, op.cit.

c) Inspection des communications, sécurité et mesures de responsabilité

Comme le CEPD l'explique dans son avis[13], l'article 4 de la directive «vie privée et communications électroniques» exige des FSI qu'ils prennent les mesures d'ordre technique et organisationnel afin de garantir un degré de sécurité adapté au risque existant[14].

Étant donné, comme décrit dans la section I.a) ci-dessus, que l'analyse des données utiles des paquets est une opération de traitement à haut risque en termes d'impact éventuel sur la vie privée et sur la protection des données, les garanties d'ordre technique et organisationnel à mettre en place doivent dès lors être aussi fortes et effectives que possible pour contrer ces risques, principalement en ce qui concerne l'éventuel mauvais usage des données.

L'obligatoire «mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel», conformément à l'article 4 de la directive «vie privée et communications électroniques», doit être le résultat d'une évaluation appropriée des risques pour les libertés fondamentales. Il convient de signaler que la proposition de la Commission d'un règlement général sur la protection des données (ci-après, le «règlement proposé»)[15], prévoit de manière explicite une «évaluation des risques»[16] en vue d'adopter les mesures les plus appropriées. L'article 33 du règlement proposé exige qu'une analyse de l'impact soit réalisée pour certaines opérations de traitement présentant des risques spécifiques d'atteinte à la vie privée et à la protection des données. Dans cette perspective, le CEPD encourage une analyse supplémentaire des pratiques d'inspection approfondie des paquets qui peuvent exiger une analyse obligatoire de l'impact sur la protection des données.

Le respect de la vie privée par défaut et de la vie privée dès la conception (comme prévu dans l'article 23 du projet de règlement) doit également guider les FSI dans l'élaboration de leur infrastructure et de leurs services. Le respect de la vie privée dès la conception et par défaut a des conséquences sur l'offre des services aux abonnés. Par exemple, les FSI doivent offrir des services dans lesquels le traitement/filtrage des données personnelles est minimisé. Les principes de respect de la vie privée par défaut et dès la conception doivent également être pris en compte par les entreprises fournissant des solutions pour la gestion générique et spécialisée du trafic.

---

[13] Cf. section V, paragraphe 4, page 17, op.cit.

[14] Au minimum, ces mesures garantiront *(i)* que seules des personnes autorisées peuvent avoir accès aux données personnelles à des fins légalement autorisées; *(ii)* les données à caractère personnel sont protégées contre le traitement accidentel ou illicite, et *(iii)* une politique de sécurité relative au traitement des données à caractère personnel est mise en œuvre. Cet article habilite en outre les autorités nationales compétentes en la matière à vérifier ces mesures et à émettre des recommandations sur les bonnes pratiques concernant le degré de sécurité que ces mesures doivent atteindre. Dans le cas de violation des données, les FSI doivent le notifier à l'autorité nationale de protection des données. Si les données personnelles ou la vie privée des abonnées sont atteintes, les FSI ont l'obligation de les informer sans délai de l'incident, à moins qu'ils ne puissent démontrer avoir mis en place des mesures pour protéger la confidentialité de ces données. À titre de mesure préventive, les FSI doivent également informer les abonnées des risques particuliers de violation de la sécurité du réseau.

[15] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du 25 janvier 2012, COM(2012)11 final, actuellement soumis au processus législatif par le Parlement européen et le Conseil.

[16] Cf. article 30, paragraphe 2, du projet de règlement.

En outre, l'utilisation par les FSI de systèmes et de sceaux de certification relative au respect de la vie privée pourrait augmenter le niveau d'assurance raisonnable de traitement favorable à la vie privée et stimuler le marché respectif.

Le CEPD estime que les FSI doivent faire preuve d'un degré de responsabilité élevé (comme prévu dans l'article 22 du projet de règlement), non seulement envers les autorités compétentes, mais également envers les personnes concernées.

Finalement, les autorités nationales pertinentes, par exemple les autorités chargées de la protection de données, devraient être habilitées à contrôler les mesures de sécurité, comme prévu dans l'article 4 de la directive «vie privée et communications électroniques».

d) Transparence et consentement de la personne concernée dans la gestion du trafic (questions 10 et 11)

Compte tenu des risques élevés entraînés par certaines techniques de gestion du trafic pour les personnes concernées, le CEPD n'a cessé de réclamer de la transparence de la part des FSI. Les abonnés aux services de communication ont droit à un degré approprié d'informations relatives aux pratiques commerciales appliquées par les FSI. Cette exigence de transparence s'étend en réalité à tous les utilisateurs concernés par la communication. Le choix informé des consommateurs n'est conditionnel et possible que si le fournisseur de services fait preuve de transparence quant à ses pratiques commerciales.

Le CEPD souhaite partager les considérations suivantes sur des éventuelles façons de présenter leurs politiques de gestion du trafic d'une manière transparente:

- En général, les FSI doivent fournir à leurs consommateurs les informations nécessaires relatives à leur politique de gestion du trafic. Du point de vue de la protection des données, les informations appropriées doivent inclure toutes les informations reprises dans les articles 10 et 11 de la directive 95/46/CE. De telles informations peuvent être fournies avec les termes du contrat: elles doivent cependant être claires et sortir des clauses contractuelles classiques.

- En outre, des informations spécifiques doivent être fournies en ce qui concerne les politiques de gestion du trafic qui impliquent un traitement plus intrusif pour lequel le consentement doit être recherché (tel que la lecture de certaines couches de contenu, le profilage, etc.). Par exemple, il conviendrait que de telles informations avertissent l'abonné du caractère intrusif d'un tel traitement du point de vue du respect de la vie privée et de la protection des données, et que ces informations indiquent la possibilité pour l'abonné de retirer son consentement à tout moment.

- Afin d'obtenir un consentement valable pour appliquer les politiques de gestion du trafic qui impliquent des activités de traitement plus intrusives, les FSI doivent s'assurer que le consentement est basé sur une action affirmative de la personne concernée et est libre, spécifique et informé. Dès lors, un tel consentement ne peut être obtenu par une simple signature de l'offre contractuelle, étant donné que ce consentement ne sera pas considéré comme

suffisamment spécifique. À cet égard, les FSI doivent soigneusement vérifier quelles activités de traitement nécessitent un consentement, et ils doivent s'assurer de pouvoir respecter tout choix futur de l'abonné de se soustraire à un tel traitement.

- Les FSI portent la responsabilité d'informer les consommateurs sur toutes mises à jour ou modifications apportées à leurs politiques de gestion du trafic. Lorsque le consentement est nécessaire pour de telles modifications ou mises à jour, les FSI doivent rechercher de nouveau une indication libre, spécifique et informée des souhaits de leurs abonnés. Les FSI doivent contacter leurs consommateurs de la manière la plus appropriée pour les informer des modifications, et rechercher leur consentement individuel si nécessaire. Une simple publication des modifications sur leur site web ne constitue pas une notification appropriée de ces modifications.

Bruxelles, le 15 octobre 2012