I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur la neutralité de l'internet, la gestion du trafic et la protection de la vie privée et des données personnelles

(2012/C 34/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la 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 ([1]),

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 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 ([2]), et notamment son article 41, paragraphe 2,

vu 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 ([3]),

A ADOPTÉ LE PRÉSENT AVIS:

I. **INTRODUCTION**

I.1. **Contexte**

1. Le 19 avril 2011, la Commission a adopté une communication intitulée «L'internet ouvert et la neutralité de l'internet en Europe» ([4]).

2. Le présent avis peut être considéré comme la réaction du CEPD à cette communication. Il vise à contribuer au débat politique sur la neutralité de l'internet qui a cours dans l'UE, plus particulièrement en ce qui concerne les aspects liés à la protection des données et à la vie privée.

([1]) JO L 281 du 23.11.95, p. 31, «directive relative à la protection des données».
([2]) JO L 8 du 12.1.2001, p. 1, le «règlement relatif à la protection des données».
([3]) JO L 201 du 31.7.2002, p. 37, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 (Cf. note 15), «directive "vie privée et communications électroniques"».
([4]) COM(2011) 222 final.

3. L'avis s'appuie sur la réponse ([5]) du CEPD à la consultation publique de la Commission au sujet de l'internet libre et de la neutralité du web en Europe, qui a précédé la communication de la Commission. Le CEPD a également pris note du récent projet de conclusions du Conseil sur la neutralité de l'internet ([6]).

I.2. **Le concept de neutralité de l'internet**

4. La neutralité de l'internet a trait à un débat d'actualité visant à déterminer si les fournisseurs de services internet (FSI) ([7]) peuvent être autorisés à limiter, filtrer ou verrouiller l'accès à l'internet ou affecter ses performances. Le concept de neutralité de l'internet repose sur l'idée que les informations sur l'internet doivent être transmises de manière impartiale, indépendamment de leur contenu, de leur destination ou de leur source, et que les utilisateurs doivent pouvoir décider d'utiliser les applications, les services et le matériel de leur choix. Cela implique que les FSI ne peuvent hiérarchiser ou ralentir arbitrairement l'accès à certains services ou applications tels que le poste à poste (P2P), etc. ([8]).

5. Le filtrage, le verrouillage et l'inspection du trafic du réseau soulèvent d'importantes questions, souvent méconnues ou passées sous silence, concernant la confidentialité des communications et le respect de la vie privée des individus et de leurs données à caractère personnel lorsqu'ils utilisent l'internet. Par exemple, certaines techniques d'inspection supposent de surveiller le contenu des communications, les sites web visités, les courriels envoyés et reçus, et à quel moment, etc., ce qui permet de filtrer les communications.

6. Il se peut qu'en inspectant les données de communication, les FSI 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, 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».

I.3. **Éléments fondamentaux et structure de l'avis**

7. Le CEPD considère qu'un débat politique sérieux sur la neutralité de l'internet doit aborder la question de la confidentialité des communications ainsi que d'autres implications pour la vie privée et la protection des données.

8. Le présent avis contribue à ce débat d'actualité dans l'UE. Son objectif est triple:

— Il met en évidence la pertinence de la vie privée et de la protection des données dans les discussions en cours sur la neutralité de l'internet. Il souligne plus particulièrement la nécessité de respecter les règles existantes relatives à la confidentialité des communications. Seules les pratiques respectueuses de ces règles doivent être autorisées.

— La neutralité de l'internet se rapporte à des possibilités — technologiques — assez récentes, or l'expérience relative à l'application du cadre juridique est limitée. Le présent avis donne dès lors des orientations quant à la manière dont les FSI doivent appliquer et respecter le cadre juridique en matière de protection des données lorsqu'ils filtrent, verrouillent ou inspectent le trafic du réseau. Ces orientations devraient leur être utiles, ainsi qu'aux autorités chargées de faire appliquer le cadre.

— Dans le cadre de la protection des données et de la vie privée, le présent avis met en exergue des domaines méritant une attention particulière et pouvant nécessiter l'adoption de mesures au niveau de l'UE. Cet élément revêt une importance particulière à la lumière du débat en cours dans l'UE et des mesures politiques que la Commission pourrait prendre dans ce contexte.

([5]) Le CEPD a répondu en soulignant qu'il était important de tenir compte des problèmes liés à la protection des données et à la vie privée, en même temps que les autres droits et valeurs existants. Sa réponse est disponible à l'adresse suivante: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Disponibles à l'adresse suivante: http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Cela comprend la fourniture d'un accès tant fixe que mobile à l'internet.

([8]) Quoique le principe ne s'applique pas aux FSI qui limitent la vitesse ou le volume de données qu'un abonné peut envoyer ou recevoir par des abonnements limitant la largeur de bande ou le volume. Par conséquent, conformément au principe de la neutralité de l'internet, les FSI pourraient continuer à offrir des abonnements limitant l'accès sur la base de critères tels que la vitesse ou le volume tant que cela n'implique pas un traitement discriminatoire en faveur ou à l'encontre d'un contenu particulier.

9. Le CEPD est conscient du fait que la neutralité de l'internet soulève d'autres questions, décrites plus avant ci-dessous, comme celles liées à l'accès à l'information. Ces questions ne sont abordées que dans la mesure où elles concernent ou affectent la protection des données à caractère personnel et la vie privée.

10. L'avis est structuré comme suit. La section II commence par un bref aperçu des pratiques des FSI en matière de filtrage. La section III décrit dans les grandes lignes le cadre juridique de l'UE sur la neutralité de l'internet. La section IV poursuit avec une description technique, suivie par une évaluation des implications pour la vie privée selon la technique utilisée. La section V analyse les modalités pratiques d'application du cadre de l'UE en matière de vie privée et de protection des données. S'appuyant sur cette analyse, la section VI contient des suggestions en vue d'initiatives politiques futures et cite les domaines dans lesquels une clarification et une amélioration du cadre juridique pourraient s'avérer nécessaires. La section VII contient les conclusions.

II. **NEUTRALITÉ DE L'INTERNET ET POLITIQUES DE GESTION DU TRAFIC**

Recours croissant aux politiques de gestion du trafic

11. En général, les FSI ne surveillent et n'influencent le trafic du réseau que dans certaines circonstances. Ils ont par exemple appliqué des techniques d'inspection et restreint les flux d'informations aux fins de préserver la sécurité du réseau, notamment pour lutter contre les virus. De manière générale, l'internet s'est donc développé tout en conservant un degré élevé de neutralité.

12. Toutefois, ces dernières années, certains FSI se sont intéressés à l'inspection du trafic du réseau afin d'appliquer des politiques différenciées, par exemple pour verrouiller certains services ou accorder un accès préférentiel à d'autres. On parle parfois à cet égard de «politiques de gestion du trafic» ([9]).

13. Les raisons pour lesquelles les FSI inspectent et différencient le trafic sont multiples. Les politiques de gestion du trafic peuvent ainsi aider les FSI à gérer le trafic en période de forte congestion, par exemple en accordant la priorité à certaines formes de trafic sensibles à la durée, comme la lecture vidéo en transit, et en réduisant l'importance d'autres formes de trafic pouvant l'être moins, comme le P2P ([10]). Par ailleurs, la gestion du trafic peut permettre aux FSI de générer des flux de recettes potentielles, issues de différentes sources possibles. D'une part, les FSI peuvent faire payer les fournisseurs de services de contenu, par exemple ceux dont les services nécessitent une largeur de bande supérieure, pour leur accorder la priorité (et donc la rapidité). Cela implique que l'accès à un service donné — de vidéo à la demande, par exemple — est plus rapide que l'accès à un service similaire n'ayant pas souscrit à la transmission à haute vitesse. D'autre part, des recettes peuvent être obtenues d'abonnés souhaitant payer plus (ou moins) pour certains types d'abonnements différenciés. Par exemple, un abonnement sans accès au P2P peut être moins cher qu'un autre avec accès illimité.

14. En plus des raisons propres aux FSI d'appliquer des politiques de gestion du trafic, d'autres parties peuvent également avoir intérêt à ce que les FSI utilisent ces politiques. Si les FSI gèrent leurs réseaux et inspectent le contenu transitant par leurs systèmes, elles peuvent renforcer leur capacité à détecter des usages présumés illicites comme des violations des droits d'auteur ou l'utilisation de contenu pornographique.

([9]) Voir par exemple le rapport de l'OFCOM intitulé *Site blocking to reduce online copyright infringement* (Verrouillage de sites pour réduire les violations des droits d'auteur en ligne), adopté le 27 mai 2011 et disponible à la page http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf «Certains FSI mettent déjà en œuvre des systèmes d'inspection de paquets de données dans leur réseau pour gérer le trafic et pour d'autres finalités. Nous supposons donc que ces systèmes peuvent être utilisés, même si cela implique un niveau élevé de complexité et de coûts pour ceux qui n'y ont pas déjà recours. Il est possible qu'à court ou à moyen terme, l'inspection approfondie des paquets ne puisse être utilisée que par les grands FSI vu les dépenses d'investissement requises».

([10]) La qualité des applications en temps réel telles que la lecture vidéo en transit dépend, entre autres, de la latence, c'est-à-dire du retard dû, par exemple, à la congestion du réseau.

Autres intérêts en jeu, y compris la protection des données et la vie privée

15. Cette tendance a déclenché un débat sur la légitimité de ce type de pratiques, et plus particulièrement sur la question de savoir si des obligations particulières garantissant la neutralité de l'internet ne devraient pas faire l'objet d'une nouvelle législation.

16. Le recours croissant des FSI aux politiques de gestion du trafic pourrait limiter l'accès à l'information. Si cette pratique devait se généraliser, et s'il devenait impossible (ou très coûteux) aux utilisateurs d'accéder à l'internet universel tel que nous le connaissons, elle mettrait en péril l'accès à l'information et la capacité des utilisateurs à envoyer et recevoir le contenu qu'ils souhaitent en utilisant les applications ou les services de leur choix. Un principe juridiquement contraignant sur la neutralité de l'internet pourrait éviter ce problème.

17. Ces considérations amènent le CEPD à s'intéresser aux implications de la gestion du trafic par les FSI pour la protection des données à caractère personnel et la vie privée. Plus particulièrement:

— Lorsque les FSI traitent des données relatives au trafic dans le seul but d'acheminer le flux d'informations de l'expéditeur au destinataire, ils effectuent en général un traitement limité de données à caractère personnel ([11]). De la même manière que les services postaux traitent les informations figurant sur l'enveloppe d'une lettre, les FSI traitent les informations nécessaires pour faire parvenir la communication au destinataire. Cela n'entre pas en conflit avec les exigences légales de la protection des données, de la vie privée et de la confidentialité des communications.

— En revanche, lorsque les FSI inspectent les données relatives aux communications afin de différencier chaque flux de communications et d'appliquer des politiques spécifiques pouvant être défavorables à certains individus, les implications sont plus importantes. Selon les circonstances du cas d'espèce et le type d'analyse effectuée, le traitement pourra être très attentatoire à la vie privée et aux données à caractère personnel d'un individu. Cela est plus évident lorsque les politiques de gestion révèlent le contenu des communications des individus sur l'internet, notamment les courriels envoyés et reçus, les sites web consultés, les fichiers téléchargés, etc.

III. APERÇU DU CADRE JURIDIQUE DE L'UE SUR LA NEUTRALITÉ DE L'INTERNET ET INITIATIVES POLITIQUES FUTURES

III.1. Le cadre juridique en bref

18. Jusqu'en 2009, les instruments législatifs de l'UE ne contenaient pas de dispositions faisant explicitement interdiction aux FSI de pratiquer le filtrage ou le verrouillage ou de facturer des coûts supplémentaires aux utilisateurs pour accéder à certains services. Ils ne contenaient pas non plus de dispositions reconnaissant explicitement ces pratiques. Dans une certaine mesure, cette situation était marquée par l'insécurité.

19. Le paquet sur les télécommunications de 2009 a changé la situation en comprenant des dispositions favorisant l'ouverture de l'internet. Par exemple, l'article 8, paragraphe 4, de la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques («directive cadre») fait obligation aux autorités réglementaires de renforcer la capacité des utilisateurs finaux à accéder au contenu, aux applications ou aux services de leur choix ([12]). Cette disposition s'applique à l'ensemble du réseau, et non au niveau des fournisseurs individuels. Le projet récent de conclusions du Conseil a également mis en exergue la nécessité de maintenir l'ouverture de l'internet ([13]).

([11]) Sont ici exclues les opérations visant à accroître la sécurité du réseau et à détecter les formes de trafic nuisibles, de même que les opérations nécessaires à la facturation et à l'interconnexion. Sont également exclues les obligations découlant de la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, 13.4.2006, p. 54) («directive relative à la conservation des données»).

([12]) Directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques telle que modifiée par la directive 2009/140/CE et le règlement (CE) n° 544/2009 (JO L 337 du 18.12.2009, p. 37).

([13]) Voir le point 3, sous e), où le Conseil reconnaît «la nécessité de maintenir l'ouverture de l'internet tout en garantissant qu'il peut continuer à fournir des services de haute qualité dans un cadre favorisant et respectant les droits fondamentaux tels que la liberté d'expression et la liberté d'entreprise», ainsi que le point 8, sous d), invitant les États membres à «promouvoir le caractère ouvert et neutre de l'internet comme leur objectif politique».

20. La directive «service universel» ([14]) contient des obligations plus concrètes. Les articles 20 et 21 énoncent des exigences de transparence concernant les limitations d'accès aux services et aux applications et les limitations de leur utilisation. Ils imposent également des niveaux minimaux de qualité des services.

21. Pour ce qui est des pratiques des FSI entraînant l'inspection des communications des individus, le considérant 28 de la directive modifiant la directive «service universel» et la directive «vie privée et communications électroniques» ([15]) souligne que «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». Le considérant 28 rappelle donc la nécessité d'obtenir, conformément à l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques», un accord à toute limitation basée sur le contrôle des communications. La section IV ci-dessous analyse plus en détail l'application de l'article 5, paragraphe 1, et le cadre juridique général relatif à la protection des données et à la vie privée.

22. Enfin, l'article 22, paragraphe 3, de la directive «service universel» permet désormais aux autorités réglementaires nationales d'imposer, si nécessaire, les exigences minimales en matière de qualité de service aux FSI afin de prévenir la dégradation du service et l'obstruction ou le ralentissement du trafic sur les réseaux publics.

23. Les dispositions précitées indiquent que l'ouverture de l'internet est largement souhaitée au niveau de l'UE (voir l'article 8, paragraphe 4, de la «directive cadre»). Cet objectif politique, qui s'applique à l'ensemble du réseau, n'est toutefois pas directement lié à des interdictions ou à des obligations imposées à des FSI individuels. Autrement dit, un FSI peut mettre en œuvre des politiques de gestion du trafic susceptibles d'empêcher l'accès à certaines applications à condition que les utilisateurs finaux soient pleinement informés et qu'ils aient exprimé leur accord librement, spécifiquement et indubitablement.

24. La situation peut varier d'un État membre à l'autre. Dans certains États membres, les FSI peuvent, dans des conditions spécifiques, mettre en œuvre des politiques de gestion du trafic, par exemple pour verrouiller des applications telles que la voix sur IP (dans le cadre d'un abonnement internet meilleur marché), à condition que les individus aient donné leur accord informé libre, spécifique et indubitable. D'autres États membres ont choisi de renforcer le principe de neutralité de l'internet. Ainsi, en juillet 2011, le Parlement néerlandais a adopté une loi interdisant de manière générale aux fournisseurs d'entraver ou de ralentir les applications ou services sur l'internet (tels que la voix sur IP), sauf lorsque cela est nécessaire pour réduire les effets de la congestion, pour des raisons d'intégrité ou de sécurité, pour lutter contre les pourriels ou pour se conformer à une décision de justice ([16]).

III.2. **La communication sur la neutralité de l'internet**

25. Dans sa communication sur la neutralité de l'internet ([17]), la Commission européenne a conclu que la situation sur la neutralité de l'internet devait être surveillée et faire l'objet d'une analyse plus poussée. Sa politique a été qualifiée d'attentiste, avant la prise en considération de nouvelles initiatives réglementaires.

([14]) Directive 2002/22/CE telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil 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, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (JO L 337 du 18.12.2009, p. 11). Comparer également l'article 1er, paragraphe 3, qui énonce que la directive n'impose ni n'interdit aux FSI de limiter l'accès des utilisateurs finals aux services et applications et/ou leur utilisation, lorsque ces limitations sont autorisées par le droit national et conformes au droit communautaire, mais prévoit une obligation de fournir des informations concernant ces conditions.

([15]) Directive 2009/136/CE du Parlement européen et du Conseil 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, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

([16]) L'amendement néerlandais original se trouve à la page suivante: https://zoek.officielebekendmakingen.nl/kst-32549-A.html Les raisons invoquées par la presse pour justifier ce choix politique n'avaient pas trait à des considérations liées à la protection des données et à la vie privée, mais plutôt à la nécessité de garantir que les utilisateurs ne sont pas privés d'accès à l'information ou qu'ils ne se voient pas offrir un accès limité à celle-ci. Il semble donc que les questions liées à l'accès à l'information aient motivé cet amendement.

([17]) Cf. note 4.

26. La communication de la Commission reconnaît que toute mesure et toute nouvelle initiative réglementaire fera l'objet d'une évaluation approfondie des aspects liés à la protection des données et à la vie privée. Le projet de conclusions du Conseil épingle également les questions en jeu en matière de protection des données et de vie privée ([18]).

27. La question à évaluer dans une perspective de la protection des données et de la vie privée consiste à déterminer si une politique attentiste est suffisante. Si le cadre de protection des données et de la vie privée prévoit actuellement certaines garanties, notamment à travers le principe de la confidentialité des communications, il semble nécessaire de surveiller étroitement le degré de respect des règles et d'émettre des orientations sur plusieurs aspects manquant singulièrement de clarté. Il convient en outre de réfléchir à la manière dont le cadre pourrait être précisé et amélioré plus avant à la lumière des évolutions de la technologie. Si la surveillance révèle que le marché se dirige vers une inspection massive et en temps réel des communications et met au jour des problèmes liés au cadre, des mesures législatives seront nécessaires. Des suggestions concrètes seront formulées à cet égard à la section VI.

IV. **INFORMATIONS TECHNIQUES ET IMPLICATIONS CONNEXES POUR LA VIE PRIVÉE ET LA PROTECTION DES DONNÉES**

28. Avant d'entrer dans le vif du sujet, il importe de mieux comprendre les techniques d'inspection que les FSI peuvent utiliser pour gérer le trafic et des conséquences que celles-ci peuvent avoir sur le principe de la neutralité de l'internet. Les implications de ces techniques pour la vie privée et la protection des données varient considérablement selon les techniques utilisées. Ces informations techniques sont nécessaires pour comprendre et appliquer correctement le cadre juridique en matière de protection des données décrit à la section V. Il convient cependant de noter qu'il s'agit là d'un domaine complexe en mutation permanente. La description qui suit ne se veut donc pas exhaustive et pleinement à jour, mais cherche uniquement à fournir les informations techniques indispensables à la bonne compréhension du raisonnement juridique.

IV.1. **Transmission d'informations sur l'internet: notions de base**

29. Lorsqu'un utilisateur transmet une communication sur l'internet, les informations transférées sont divisées en paquets. Ces paquets sont transmis de l'expéditeur au destinataire par l'internet. Chaque paquet comprend entre autres des données relatives à la source et à la destination. Les FSI peuvent en outre joindre à ces paquets des couches et protocoles supplémentaires ([19]), qui seront utilisés pour gérer les différents flux de trafic au sein de leur réseau.

30. Pour reprendre l'analogie du courrier postal, utiliser un protocole de transmission sur le réseau revient à inclure le contenu d'un courrier postal dans une enveloppe comprenant une adresse de destination qui est lue par le service postal pour pouvoir livrer le courrier. Le service postal peut utiliser des protocoles supplémentaires dans ses transits internes pour gérer toutes les enveloppes à transmettre, le but étant que chaque enveloppe parvienne à la destination indiquée par l'expéditeur. Sur la base de cette analogie, chaque paquet se compose de deux parties: les *données utiles IP*, qui comprennent le contenu de la communication et sont l'équivalent de la lettre. Elles contiennent des informations adressées uniquement au destinataire. La deuxième partie du paquet est l'*en-tête IP*, qui comprend entre autres les adresses de l'expéditeur et du destinataire et est l'équivalent de l'enveloppe. L'en-tête IP permet aux FSI et aux autres intermédiaires d'acheminer les données utiles IP de l'adresse d'origine à l'adresse de destination.

31. Les FSI et les autres intermédiaires font en sorte que les paquets IP voyagent à travers le réseau par des nœuds qui lisent les informations de l'en-tête IP, les vérifient par rapport à des tables de routage puis les transmettent au nœud suivant sur le chemin menant à la destination. Ce processus se répète tout au

([18]) Cf. point 4, sous e), où le Conseil relève «certaines inquiétudes exprimées principalement par des organisations de défense des consommateurs et les autorités chargées de la protection des données et concernant la protection des données à caractère personnel».

([19]) Comme la section IV.2 l'explique de manière plus détaillée, ces protocoles codent les informations transmises de bout en bout suivant une convention, comme le HTTP, le FTP, etc., de manière à ce que les parties à la communication puissent se comprendre.

long du réseau en adoptant l'approche du «service au mieux sans mémoire», étant donné que tous les paquets arrivant à un nœud sont traités de façon neutre. Lorsqu'ils ont été transmis au nœud suivant, il n'est pas nécessaire de conserver d'autres informations dans le routeur ([20]).

IV.2. **Techniques d'inspection**

32. Comme exposé ci-dessus, les FSI lisent les en-têtes IP afin de les acheminer vers leurs destinations. Toutefois, l'analyse du trafic (y compris des en-têtes IP et des données utiles IP) peut, comme indiqué précédemment, être effectuée à d'autres fins et au moyen de différents types de technologies. Les nouvelles tendances peuvent consister, par exemple, à ralentir certaines applications utilisées par les utilisateurs, comme le P2P, ou au contraire à augmenter la vitesse du trafic pour certains services comme la vidéo à la demande pour les abonnés privilégiés. Si toutes les techniques d'inspection exécutent *techniquement* une inspection des paquets, elles n'ont pas le même degré d'intrusion. Il existe deux grandes catégories de techniques d'inspection. L'une repose uniquement sur l'en-tête IP, l'autre porte également sur les données utiles IP.

Technique basée sur les informations de l'en-tête IP. L'inspection de l'en-tête d'un paquet IP révèle certains champs qui peuvent permettre aux FSI de mettre en œuvre une série de politiques spécifiques de gestion du trafic. Ces techniques basées uniquement sur l'inspection des en-têtes IP traitent à une autre fin (par exemple, pour différencier le trafic) des données qui, en principe, sont destinées à acheminer les informations. En regardant l'adresse IP d'origine, le FSI peut la relier à un abonné donné et lui appliquer des politiques spécifiques, par exemple acheminer le paquet à travers un lien plus rapide ou plus lent. En regardant l'adresse IP de destination, le FSP peut également lui appliquer des politiques spécifiques, par exemple bloquer ou filtrer l'accès à certains sites web.

Technique basée sur une inspection plus poussée. L'inspection approfondie des paquets permet aux FSI d'accéder aux informations adressées uniquement au destinataire de la communication. Pour revenir à l'exemple du service postal, cette approche équivaut à ouvrir l'enveloppe et à lire la lettre qui s'y trouve pour analyser le contenu de la communication (encapsulé dans les paquets IP) afin de lui appliquer une politique de réseau spécifique. Il existe plusieurs manières d'effectuer cette inspection, chacune d'entre elles présentant des menaces différentes pour la personne concernée.

— *Inspection approfondie des paquets basée sur l'analyse des protocoles et sur les données statistiques*. Outre le protocole IP, qui vise à permettre la transmission des données sur l'internet, il existe d'autres protocoles qui codent les informations transmises suivant une convention (transport, session, présentation et application, etc.). Le but de ces protocoles est de faire en sorte que les parties à la communication puissent se comprendre. Par exemple, certains protocoles sont associés à la navigation sur la Toile ([21]), d'autres au transfert de fichiers ([22]), etc. Par conséquent, les techniques d'inspection basées sur l'inspection des protocoles et combinées à une analyse statistique visent à rechercher des configurations ou empreintes digitales spécifiques dénotant la présence de tel ou tel protocole ([23]). Ces techniques d'inspection permettent aux FSI de déterminer le type de communication (courriel, navigation, téléchargement de fichiers) et, dans certains cas, d'identifier le service ou l'application spécifique utilisé, comme pour certaines communications de voix sur IP où les protocoles utilisés sont tout à fait propres à un vendeur ou prestataire de services déterminé. Le fait de connaître le type de communication utilisé peut permettre aux FSI de mettre en œuvre des politiques concrètes de gestion du trafic, par exemple bloquer le trafic sur la Toile. Il peut aussi constituer la première étape permettant au FSI de procéder à des analyses plus poussées pouvant nécessiter un accès intégral aux métadonnées et au contenu de la communication.

([20]) Les équipements de réseaux pour l'internet utilisent néanmoins des protocoles de routage qui enregistrent des activités, traitent les statistiques du trafic et échangent des informations avec d'autres équipements de réseaux afin d'acheminer des paquets IP par la voie la plus efficiente. Par exemple, lorsqu'un lien est encombré ou brisé, et qu'un routeur reçoit cette information, il met à jour sa table de routage avec un autre chemin n'utilisant pas ce lien. Il est aussi intéressant de noter la collecte et le traitement qui peuvent être effectués dans certains cas à des fins de facturation ou même conformément aux exigences de la directive relative à la conservation des données.

([21]) HTTP — protocole de transfert hypertexte — ou HTML — langage de balisage hypertexte.

([22]) FTP — protocole de transfert de fichiers.

([23]) Il existe plusieurs manières d'identifier les protocoles utilisés. Il est ainsi possible de rechercher des protocoles internes dans des champs spécifiques, par exemple pour identifier les ports utilisés pour établir la communication. Une caractérisation statistique d'un flux de communication peut également être déduite de l'analyse de certains champs spécifiques et de la corrélation des protocoles utilisés simultanément entre deux adresses IP.

— *Inspection approfondie des paquets basée sur l'analyse du contenu de la communication*. Enfin, il est également possible d'inspecter les métadonnées ([24]) et le contenu de la communication même. Cette technique consiste à intercepter tous les paquets IP faisant part du flux de communication original de manière à pouvoir reconstruire et analyser le contenu original de la communication. Par exemple, pour détecter les contenus nuisibles ou illégaux tels que les virus, la pédopornographie, etc., il est nécessaire de reconstruire le contenu même pour pouvoir l'analyser. Il convient de noter que, parfois, la communication peut être expressément cryptée de bout en bout par les parties concernées et que cette pratique empêchera les FSI de procéder à l'analyse du contenu de la communication.

IV.3. **Implications pour la vie privée et la protection des données**

33. Les techniques d'inspection basées sur les en-têtes IP, et plus particulièrement celles basées sur l'inspection des paquets, supposent de contrôler et de filtrer ces données et sont lourdes de conséquences sur le plan de la vie privée et de la protection des données. Elles peuvent également entrer en conflit avec le droit à la confidentialité des communications.

34. Le fait d'examiner les communications d'individus comporte en soi de graves implications pour la vie privée et la protection des données à caractère personnel. Le problème est cependant plus large puisque les implications pour la vie privée peuvent être encore plus importantes selon les effets recherchés par la surveillance et l'interception. En effet, on ne saurait comparer le fait de se borner à inspecter des communications, par exemple pour s'assurer que le système fonctionne correctement, et le fait d'inspecter les communications afin d'appliquer des politiques pouvant affecter les individus. Lorsque les politiques de trafic et de sélection ont pour seul but d'éviter la congestion du réseau, elles ne comportent habituellement aucune implication importante pour la vie privée des individus. En revanche, certaines politiques de gestion du trafic peuvent avoir pour objectif de verrouiller certains contenus ou d'influencer la communication, par exemple par la publicité comportementale. Dans ce cas, les effets sont plus intrusifs. Les appréhensions deviennent plus vives lorsque l'on se rend compte que ce type d'informations est collecté non pas pour un nombre limité de personnes, mais plutôt de manière systématique, pour tous les clients des FSI ([25]). Si tous les FSI adoptent des techniques de filtrage, cela peut donner lieu à une surveillance généralisée de l'utilisation de l'internet. En outre, si l'on considère attentivement le type d'informations traitées, les risques pour la vie privée paraissent de toute évidence élevés, étant donné que la majeure partie des informations collectées sera vraisemblablement de nature très sensible et qu'après avoir été collectées, elles seront à la disposition des FSI et de ceux qui pourraient les leur demander. Par ailleurs, les informations peuvent aussi avoir une grande valeur commerciale, ce qui en soi représente un risque élevé de détournement d'usage lorsque les finalités initiales peuvent facilement évoluer en une exploitation, commerciale ou autre, des informations collectées.

35. L'application correcte de la surveillance et des techniques d'inspection et de filtrage doit avoir lieu dans le respect des garanties applicables en matière de protection des données et de vie privée, qui fixent les limites de ce qui est autorisé dans des circonstances données. On trouvera à la section suivante un aperçu des garanties applicables en vertu du cadre actuel de l'UE en matière de protection des données et de vie privée.

V. **APPLICATION DU CADRE JURIDIQUE DE L'UE EN MATIÈRE DE VIE PRIVÉE ET DE PROTECTION DES DONNÉES**

36. Le cadre de l'UE en matière de protection des données à caractère personnel est neutre sur le plan technologique. En tant que tel, il ne réglemente pas des techniques d'inspection spécifiques telles que celles décrites ci-dessus. La directive «vie privée et communications électroniques» réglemente les questions liées à la vie privée dans le cadre de la fourniture de services de communication électronique dans

([24]) Chaque protocole possède des champs spécifiques dans son en-tête qui fournissent des données informelles supplémentaires sur la communication transmise. Par conséquent, le contenu de ces champs peut être qualifié de «métadonnées de la communication». Ces champs peuvent par exemple être le numéro de port utilisé: s'il s'agit du numéro 80, il y a de fortes chances que le type de communication concernée soit la navigation sur la toile.

([25]) Certes, les possibilités de traçage ne sont pas l'apanage des FSI. Les fournisseurs de réseaux publicitaires sont également capables de tracer les utilisateurs à travers les sites web en utilisant les cookies de tiers. Voir par exemple cet article universitaire récent montrant que Google est présent sur 97 des 100 sites web les plus visités, ce qui signifie que Google peut tracer les utilisateurs qui n'ont pas désactivé les cookies de tiers lorsqu'ils visitent ces sites web populaires: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning* (29 juillet 2011). Disponible à la page: http://ssrn.com/abstract=1898390 Le traçage d'utilisateurs à travers les cookies de tiers a été abordé par le groupe de travail «Article 29». Voir l'avis 2/2010 sur la publicité comportementale en ligne, adopté le 22 juin 2010 (WP 171).

des réseaux publics (le plus souvent, l'accès à l'internet et la téléphonie) ([26]), tandis que la directive relative à la protection des données réglemente le traitement des données de manière générale. Dans l'ensemble, ce cadre juridique énonce des obligations différentes s'appliquant aux FSI qui traitent et surveillent des données relatives au trafic et aux communications.

V.1. **Base juridique du traitement des données relatives au trafic et au contenu**

37. En vertu de la législation sur la protection des données, le traitement de données à caractère personnel, comme en l'espèce le traitement des données relatives au trafic et au contenu, doit reposer sur une base juridique adéquate. En plus de cette exigence générale, des exigences particulières peuvent également s'appliquer dans certains cas.

38. Le type de données à caractère personnel traitées par les FSI se rapporte en l'occurrence aux données relatives au trafic et au contenu des communications, qui sont protégés par le droit à la confidentialité de la correspondance consacré par l'article 8 CEDH ainsi que par les articles 7 et 8 de la Charte. Plus particulièrement, l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques», intitulé «Confidentialité des communications», impose aux États membres de garantir la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public. Dans le même temps, les dispositions précitées prévoient que le traitement des données relatives au trafic et au contenu par les FSI peut être autorisé dans certaines circonstances moyennant le consentement des utilisateurs, en édictant une interdiction 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 (cela) est légalement (permis), conformément à l'article 15, paragraphe 1». Ce point sera développé plus loin.

39. Outre le consentement des utilisateurs concernés, la directive «vie privée et communications électroniques» prévoit d'autres motifs pouvant légitimer le traitement des données relatives au trafic et au contenu par les FSI. Les fondements juridiques valables pour le traitement sont dans ce cas i) la fourniture du service; ii) la sauvegarde de la sécurité du service et iii) l'atténuation de la congestion. Les autres motifs possibles légitimant les politiques de gestion basées sur les données relatives au trafic ou aux communications sont examinés ci-dessous au point (*iv*).

i) Fondement juridique lié à la fourniture du service

40. Comme exposé à la section IV, les FSI traitent les informations sur les en-têtes IP à des fins consistant à acheminer chaque paquet de données IP à destination. L'article 6, paragraphes 1 et 2, de la directive «vie privée et communications électroniques» autorise le traitement des données relatives au trafic aux fins de l'acheminement d'une communication. Les FSI peuvent donc traiter les informations nécessaires à la fourniture du service.

ii) Fondement juridique lié à la sauvegarde de la sécurité du service

41. D'après l'article 4 de la directive «vie privée et communications électroniques», le FSI a l'obligation générale de prendre les mesures appropriées afin de garantir la sécurité de ses services. La pratique du filtrage des virus peut nécessiter le traitement des en-têtes IP et des données utiles IP. Compte tenu du fait que l'article 4 de ladite directive impose aux FSI d'assurer la sécurité du réseau, cette disposition légitime les techniques d'inspection basées sur les en-têtes IP et le contenu qui visent uniquement à atteindre cet objectif. Concrètement, cela implique que, dans les limites fixées par le principe de la proportionnalité (voir la section V.3), les FSI peuvent pratiquer la surveillance et le filtrage des données relatives aux communications pour lutter contre les virus et, de manière générale, assurer la sécurité du réseau ([27]).

([26]) Le considérant 10 de la directive «vie privée et communications électroniques» énonce que «[d]ans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels». Par ailleurs, le considérant 17 présente de l'intérêt pour le consentement de la personne concernée: «Aux fins de la présente directive, le consentement d'un utilisateur ou d'un abonné, que ce dernier soit une personne physique ou morale, devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive 95/46/CE».

([27]) Avis 2/2006 du groupe de travail «Article 29» 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 (WP 118). Dans cet avis, le groupe de travail considère que l'utilisation de filtres pour la finalité visée à l'article 4 peut être compatible avec l'article 5 de la directive «vie privée et communications électroniques».

iii) Fondement juridique lié à l'atténuation des effets de la congestion

42. La justification de ce fondement juridique se trouve au considérant 22 de la directive «vie privée et communications électroniques», qui explique l'interdiction du stockage des communications énoncée à l'article 5, paragraphe 1. Celle-ci n'interdit pas tout stockage automatique, intermédiaire et transitoire s'il a lieu dans le seul but d'effectuer la transmission et qu'il ne dure pas plus longtemps que le temps nécessaire à la transmission et à la gestion du trafic, pour autant que la confidentialité des informations reste garantie.

43. En cas de congestion se pose la question de savoir si les FSI peuvent envisager de réduire ou de retarder de manière aléatoire le trafic, ou alors de ralentir les communications qui ne sont pas sensibles à la durée, comme le P2P ou les échanges courriels, permettant ainsi au trafic vocal, par exemple, de passer à une qualité acceptable.

44. Vu qu'il est dans l'intérêt de l'ensemble de la société de garantir un réseau de communications utilisable, les FSI pourraient faire valoir que la hiérarchisation ou le ralentissement du trafic pour remédier à la congestion est une mesure légitime, nécessaire à la fourniture d'un service adéquat. Cela signifie que, dans ces cas-là et pour cette finalité-là, il existerait un fondement juridique général pour traiter des données à caractère personnel et que le consentement spécifique des utilisateurs ne serait plus nécessaire.

45. Dans le même temps, la possibilité d'interférer de cette manière n'est pas illimitée. Si les FSI doivent inspecter les communications, dans la perspective de la confidentialité, et en appliquant rigoureusement le principe de proportionnalité, ils doivent utiliser la méthode la moins intrusive dont ils disposent pour atteindre l'objectif (en évitant l'inspection approfondie des paquets) et l'appliquer uniquement pendant la durée nécessaire pour remédier à la congestion.

iv) Fondement juridique lié au traitement de données à d'autres fins

46. Les FSI peuvent également chercher à inspecter les données relatives au trafic et au contenu à d'autres fins, par exemple pour offrir des abonnements ciblés (comme un abonnement limitant l'accès au P2P ou augmentant la vitesse pour certaines applications). L'inspection et l'utilisation ultérieure de données relatives au trafic et aux communications à des fins autres que la fourniture du service, la garantie de sa sécurité et la lutte contre la congestion ne sont autorisées que dans des conditions strictes, conformément au cadre juridique.

47. Le cadre juridique consiste essentiellement en l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques», qui exige le consentement des utilisateurs concernés pour l'écoute, l'interception, le stockage ou d'autres moyens d'interception ou de surveillance des communications et des données relatives au trafic. Concrètement, cela implique qu'en vertu de l'article 5, paragraphe 1, le consentement des utilisateurs concernés par une communication est nécessaire pour légitimer le traitement des données relatives au trafic et aux communications.

48. Comme exposé ci-dessus, l'application de techniques d'inspection et de filtrage repose soit sur les entêtes IP, qui constituent les données relatives au trafic, soit sur l'inspection approfondie des paquets, qui porte également sur les données utiles IP et constitue les données relatives à la communication. Par conséquent, en principe, l'application de ces techniques à des fins autres que l'acheminement du service ou la sécurité serait interdite, sauf si le traitement est autorisé par un fondement juridique, comme le consentement (article 5, paragraphe 1). L'article 5, paragraphe 1, pourrait par exemple s'appliquer si un FSI décide d'offrir à ses clients l'accès à l'internet à un tarif réduit en échange de la réception de publicités comportementales, ce qui implique de recourir à l'inspection approfondie des paquets et donc des données relatives à la communication. Le consentement réel, spécifique et informé est dès lors nécessaire d'après l'article 5, paragraphe 1.

49. En outre, l'article 6 de la directive «vie privée et communications électroniques», intitulé «Données relatives au trafic», contient certaines règles qui s'appliquent spécifiquement aux données relatives au trafic. Il prévoit plus particulièrement la possibilité pour les FSI de traiter les données relatives au trafic

si les utilisateurs acceptent de recevoir des services à valeur ajoutée ([28]). Cette disposition précise l'exigence de consentement prévue à l'article 5, paragraphe 1, lorsque les données relatives au trafic sont concernées.

50. Dans la pratique, il n'est pas toujours aisé de déterminer, par exemple, les cas dans lesquels le consentement est nécessaire, et ceux dans lesquels la sécurité du réseau peut légitimer le traitement, notamment si les finalités des techniques d'inspection sont doubles (par exemple, éviter la congestion et fournir des services à valeur ajoutée). Il convient de souligner que le consentement ne saurait être considéré comme un moyen facile et général de se conformer aux principes de la protection des données.

51. Pour ce qui est de l'application du cadre, et plus particulièrement des différents aspects exposés ci-dessus, l'expérience est limitée. Il est essentiel de formuler de nouvelles orientations dans ce domaine, ainsi que la section VI l'explique de manière plus détaillée. En outre, d'autres aspects pertinents liés à l'obtention du consentement méritent eux aussi d'être pris en considération. Ils seront décrits ci-dessous.

V.2. **Questions liées au consentement informé en tant que fondement juridique**

52. Le consentement requis par les articles 5 et 6 de la directive «vie privée et communications électroniques» a la même portée que le consentement de la personne concernée tel que défini et précisé plus avant par la directive 95/46/CE ([29]). D'après l'article 2, point h), de la directive relative à la protection des données, on entend par «consentement de la personne concernée toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement». Récemment, le rôle du consentement et les conditions de sa validité ont été abordés par le groupe de travail «Article 29» dans son avis 15/2011 sur le consentement ([30]).

53. Les FSI qui demandent le consentement avant de pratiquer l'inspection et le filtrage des données relatives au trafic et au contenu doivent dès lors s'assurer que le consentement est libre et spécifique et qu'il est l'indication parfaitement informée des souhaits de l'individu par laquelle celui-ci donne son accord au traitement des données à caractère personnel le concernant. Le considérant 17 de la directive «vie privée et communications électroniques» le réaffirme: «(…) Le consentement peut être donné selon toute modalité 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». Voici à présent quelques exemples pratiques de ce qu'il y a lieu d'entendre par consentement libre, spécifique et informé dans ce contexte.

Consentement: indication libre, spécifique et informée de souhaits

54. *Consentement libre.* Les utilisateurs ne doivent pas subir de contraintes établissant un lien entre leur consentement et l'abonnement à l'internet auquel ils veulent souscrire.

55. Les individus ne donneraient pas librement leur accord s'ils devaient accepter la surveillance de leurs données de communication pour avoir accès à un service de communication, d'autant plus si *tous* les fournisseurs sur un marché donné pratiquent la gestion du trafic à des fins allant au-delà de la sécurité

([28]) Le considérant 18 contient une liste d'exemples de services à valeur ajoutée. Il n'apparaît pas clairement si les services auxquels les politiques de gestion du trafic s'appliquent peuvent être considérés comme relevant de cette liste. Les politiques de gestion du trafic visant à accorder la priorité à certains types de contenu peuvent être considérées comme fournissant une qualité de service. Par exemple, la gestion du trafic qui n'entraîne que le traitement des en-têtes IP et a pour objectif d'offrir des services de jeu à des prix haut de gamme, qui garantissent que le trafic personnel des utilisateurs lié au jeu est prioritaire sur le réseau, peut être considérée comme un service à valeur ajoutée. D'un autre côté, il n'est pas du tout évident s'il en va de même de la gestion du trafic visant à ralentir certains types de trafic, par exemple pour réduire l'importance du trafic lié au P2P.

([29]) Voir le considérant 17 et l'article 2, point f), de la directive «vie privée et communications électroniques».

([30]) Adopté le 13 juillet 2011 (WP 187).

du réseau. La seule solution serait alors de ne pas prendre d'abonnement du tout à un service internet. Étant donné que l'internet est devenu un outil essentiel tant à des fins professionnelles que de loisirs, le fait de ne pas souscrire à un service internet ne constitue pas une solution envisageable. Les individus n'auraient alors pas vraiment le choix, c'est-à-dire qu'ils ne seraient pas en mesure de donner librement leur consentement ([31]).

56. Le CEPD considère que la Commission et les autorités nationales doivent absolument surveiller le marché, notamment pour vérifier si ce scénario — à savoir, que les fournisseurs conditionnent les services de télécommunications à la surveillance des communications — se généralise. Les fournisseurs doivent proposer d'autres services, notamment un abonnement à l'internet qui ne soit pas soumis à la gestion du trafic, sans imposer des coûts plus élevés aux individus.

57. *Consentement spécifique*. Pour que le consentement soit spécifique, les FSI doivent obtenir le consentement pour la surveillance des données relatives au trafic et aux communications d'une manière claire et distinctive. D'après le groupe de travail «Article 29», «[p]our être spécifique, le consentement doit être intelligible. Il doit mentionner, de façon claire et précise, l'étendue et les conséquences du traitement des données. Il ne peut pas s'appliquer à un ensemble illimité d'activités de traitement. En d'autres termes, le contexte dans lequel le consentement s'applique est limité.» Il est peu probable qu'un consentement spécifique soit obtenu si le consentement à l'inspection des données relatives au trafic et aux communications est «noyé» dans le consentement général nécessaire pour souscrire au service. La spécificité implique plutôt d'utiliser des moyens ciblés pour obtenir le consentement, comme un formulaire de consentement spécifique ou une boîte distincte, clairement dédiée à la finalité de la surveillance (au lieu d'insérer l'information dans les conditions générales du contrat et d'exiger la signature du contrat en l'état).

58. *Consentement informé*. Pour que le consentement soit valable, il doit être informé. La nécessité de fournir des informations préalables adéquates découle non seulement de la directive «vie privée et communications électroniques» et de la directive relative à la protection des données, mais aussi des articles 20 et 21 de la directive «service universel», telle qu'amendée par la directive 2009/136/CE ([32]). La nécessité de l'information et du consentement est explicitement confirmée par le considérant 28 de la directive 2009/136/CE: «(…) 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». Ce considérant précise ensuite que «[s]elon 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 (…)».

59. Vu la complexité de ces techniques de surveillance, la communication préalable d'informations utiles est une des principales difficultés à surmonter pour obtenir un consentement valable. Les consommateurs doivent être informés d'une manière leur permettant de connaître les informations qui sont traitées, la manière dont elles sont utilisées, les incidences sur leur expérience d'utilisateur et le niveau d'intrusion dans leur vie privée que ces techniques impliquent.

60. Cela signifie non seulement que les informations doivent elles-mêmes être claires et compréhensibles par les utilisateurs moyens, mais aussi qu'elles doivent être communiquées directement aux individus d'une manière évidente qui leur empêche de les ignorer.

61. *Indication de souhaits*. D'après le cadre juridique applicable, le consentement requiert également une action positive de la part de l'utilisateur pour signifier son consentement. Un consentement implicite ne serait pas de nature à remplir cette condition. Cela confirme également la nécessité d'utiliser des moyens spécifiques pour obtenir le consentement permettant au FSI d'inspecter les données relatives au trafic et aux communications dans le cadre de l'application de politiques de gestion du trafic. Dans son récent avis sur le consentement, le groupe de travail «Article 29» a souligné la nécessité d'une grande précision pour obtenir le consentement concernant les différents éléments constitutifs du traitement de données.

([31]) Les dossiers passagers (PNR) offrent un exemple similaire. Dans ce cas, la question était de savoir si le consentement des passagers au transfert des données de réservation aux autorités américaines était valide. Le groupe de travail a considéré que le consentement des passagers ne pouvait pas être donné librement puisque les compagnies aériennes étaient obligées de transmettre les données avant le décollage et que les passagers n'avaient donc pas réellement le choix s'ils souhaitaient voyager en avion. Voir l'avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis.

([32]) Directive 2009/136/CE du Parlement européen et du Conseil 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 (Cf. note 15).

62. On pourrait faire valoir que si les parties à une communication ne veulent pas que les FSI interceptent celle-ci pour lui appliquer des politiques de gestion du trafic, elles peuvent toujours la crypter. Si cette approche peut être tenue pour utile sur le plan pratique, elle requiert cependant une certaine dose d'efforts et de connaissances techniques et ne saurait être assimilée à un consentement libre, spécifique et informé. Par ailleurs, l'utilisation de techniques de cryptage n'assure pas totalement la confidentialité d'une communication puisque le FSI pourra au moins accéder aux informations de l'en-tête IP afin d'acheminer la communication et qu'il sera également en mesure de la soumettre à une analyse statistique.

63. D'après l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques», le consentement des utilisateurs concernés doit être obtenu. Dans de nombreux cas, l'utilisateur et l'abonné ne feront qu'une seule et même personne, ce qui permet de recueillir le consentement au moment de la souscription au service de télécommunication. Dans d'autres cas, notamment lorsque plusieurs personnes sont potentiellement concernées, le consentement des utilisateurs en cause devra être obtenu séparément, ce qui peut poser des problèmes pratiques, comme on l'exposera ci-dessous.

Consentement de tous les utilisateurs concernés

64. L'article 5, paragraphe 1, prévoit que le consentement de l'utilisateur est nécessaire pour légitimer le traitement. Le consentement de *tous les utilisateurs* concernés par une communication doit être obtenu. La justification sous-jacente est qu'une communication concerne habituellement au moins deux personnes (l'expéditeur et le destinataire). Par exemple, si un FSI analyse les données utiles IP se rapportant à un courriel, il inspecte des informations qui ont trait tant à l'expéditeur qu'au destinataire du courrier électronique.

65. Lorsqu'ils surveillent et interceptent les données relatives au trafic et aux communications (par exemple, le trafic sur la toile), les FSI peuvent se contenter d'obtenir le consentement de l'utilisateur, c'est-à-dire, de l'abonné parce que l'autre partie à la communication — dans ce cas, un site web consulté — ne peut pas être considérée comme un «utilisateur concerné» ([33]). La situation peut être toutefois plus complexe lorsque cette surveillance suppose d'inspecter le contenu de courriels et donc des données à caractère personnel de leurs expéditeurs et de leurs destinataires, qui peuvent ne pas entretenir tous les deux une relation contractuelle avec le même FSI. En effet, dans ces cas-là, le FSI traiterait des données à caractère personnel (nom, adresse électronique et données relatives au contenu potentiellement sensibles) d'individus qui ne sont pas ses clients. D'un point de vue pratique, l'obtention du consentement de ces individus peut s'avérer plus ardue, car elle doit avoir lieu au cas par cas plutôt qu'à l'occasion de la souscription au service de télécommunication. Il ne serait pas non plus réaliste de présumer que le consentement de l'abonné a également été donné au nom des autres utilisateurs, comme cela est souvent le cas des ménages privés.

66. Dans ce contexte, le CEPD considère que les FSI doivent respecter les exigences légales existantes et mettre en œuvre des politiques qui n'entraînent pas la surveillance et l'inspection d'informations. Cela est d'autant plus essentiel dans le cas des services de communication qui impliquent des tierces parties n'étant pas en mesure de donner leur accord à la surveillance, notamment pour ce qui est des courriels envoyés et reçus (ce n'est pas le cas lorsque la finalité repose sur des considérations liées à la sécurité).

67. Dans le même temps, il convient de noter que la législation nationale transposant l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques» ne donne pas toujours satisfaction sur ce point et que, de manière générale, il semble que de meilleures orientations soient plutôt nécessaires quant aux exigences que ladite directive impose dans ce contexte. Le CEPD invite dès lors la Commission à jouer un rôle plus actif à cet égard et à prendre une initiative qui pourrait bénéficier des contributions des autorités de contrôle réunies au sein du groupe de travail «Article 29» et d'autres parties prenantes. Au besoin, la Cour de justice pourrait être saisie pour faire toute la clarté sur la portée et les conséquences de l'article 5, paragraphe 1.

([33]) Nonobstant les cas où le trafic sur des sites web suppose le transfert de données à caractère personnel comme des photos de personnes physiques identifiables publiées sur un site web. Le traitement de ces informations doit reposer sur une base juridique, mais il ne serait pas couvert par l'article 5, paragraphe 1, dans la mesure où ces personnes ne seraient pas des «utilisateurs concernés».

V.3. **Proportionnalité — Principe de la minimisation des données**

68. L'article 6, point c), de la directive relative à la protection des données consacre le principe de la proportionnalité ([34]), qui s'applique aux FSI étant donné qu'ils sont les responsables du traitement au sens de la directive lorsqu'ils se livrent à des activités de surveillance et de filtrage.

69. Selon ce principe, les données à caractère personnel ne peuvent être traitées que dans la mesure où elles sont «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement». L'application de ce principe suppose de déterminer si les moyens utilisés pour traiter les données et les types de données à caractère personnel utilisées sont adéquats et s'ils sont raisonnablement susceptibles d'atteindre leurs objectifs. Si la conclusion est que le volume de données collectées est plus important que nécessaire, alors le principe n'est pas respecté.

70. Le respect du principe de la proportionnalité par certaines techniques d'inspection doit être évalué au cas par cas. Il n'est pas possible de dégager des conclusions in abstracto. Il est toutefois possible d'attirer l'attention sur plusieurs aspects concrets qui doivent être appréciés lors de l'évaluation du respect du principe de la proportionnalité.

71. *Le volume d'informations traitées*. Une surveillance maximale des communications des clients des FSI est excessive et illégale dans la plupart des cas. Le fait que celle-ci peut être effectuée par des moyens qui apparaissent abscons aux individus et qu'il peut leur être difficile de comprendre ce qui se passe renforce les incidences sur leur vie privée. Les FSI doivent déterminer les moyens disponibles qui sont les moins intrusifs pour atteindre le résultat requis. Par exemple, la surveillance des en-têtes IP peut-elle atteindre le résultat requis, au lieu de l'inspection approfondie des paquets? Même lorsque l'inspection approfondie des paquets est utilisée, l'identification d'un nombre limité de protocoles peut fournir les informations nécessaires. La mise en œuvre de garanties en matière de protection des données, y compris la pseudo-anonymisation, peut également présenter un certain intérêt. Le résultat de l'évaluation doit confirmer que le traitement des données est proportionné.

72. *Les effets du traitement (liés directement aux finalités)*. La proportionnalité peut faire défaut dans certains cas, lorsque les FSI appliquent des politiques de gestion du trafic pour exclure l'accès à certains services sans permettre en contrepartie aux utilisateurs de bénéficier équitablement des avantages qui en découlent.

73. Il importe de rappeler que le principe de la proportionnalité continue de s'appliquer même si d'autres exigences légales contraignantes ont été satisfaites, notamment si un FSI a, par exemple, obtenu le consentement des individus pour procéder à la surveillance du contenu. Cela implique que le traitement des données effectué par la surveillance du contenu peut encore être illégal s'il viole le principe fondamental sous-jacent de la proportionnalité.

V.4. **Mesures de sécurité et organisationnelles**

74. L'article 4 de la directive «vie privée et communications électroniques» impose expressément aux FSI de prendre des mesures d'ordre technique et organisationnelle afin de garantir que i) seules des personnes autorisées peuvent avoir accès aux données à caractère personnel 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.

75. D'autre part, en vertu de l'article 4, paragraphes 2 et 3, de la directive «vie privée et communications électroniques», les FSI sont également tenus d'avertir les autorités nationales compétentes respectives en cas de violation de données, ainsi que les personnes concernées au cas où la divulgation est de nature à les affecter négativement.

76. Le traitement des données à caractère personnel comprises dans des communications qui vise à appliquer des politiques de gestion du trafic peut donner aux FSI l'accès à des données encore plus sensibles que celles relatives au trafic.

([34]) Comme exposé ci-dessus, la directive relative à la protection des données se rapporte à toutes les questions concernant la protection des droits et libertés fondamentaux, qui ne sont pas expressément couvertes par la directive «vie privée et communications électroniques».

77. Par conséquent, les politiques de sécurité élaborées par les FSI doivent comprendre des garanties spécifiques pour faire en sorte que les mesures prises soient adéquates au regard de ces risques. Dans le même temps, les autorités nationales compétentes qui vérifient ces mesures doivent être particulièrement exigeantes. Enfin, il convient de s'assurer que des procédures d'avertissement effectives sont mises en place pour informer les personnes concernées dont les données ont été violées et qui peuvent donc être affectées négativement.

VI. **SUGGESTIONS DE MESURES POLITIQUES ET LÉGISLATIVES**

78. Les techniques d'inspection basées sur les données relatives au trafic et à l'inspection des données utiles IP, c'est-à-dire du contenu des communications, peuvent révéler l'activité des utilisateurs sur l'internet: sites web consultés et activités sur ces sites, utilisation d'applications P2P, fichiers téléchargés, courriels envoyés et reçus, de qui, à quel sujet et dans quels termes, etc. Les FSI peuvent chercher à utiliser ces informations pour donner la priorité à certaines communications, comme la vidéo à la demande. Ils peuvent aussi les utiliser pour identifier des virus ou façonner des profils pour les besoins de publicités comportementales. Ces actions interfèrent avec le droit à la confidentialité des informations.

79. Les implications pour la vie privée seront plus ou moins importantes selon les techniques utilisées et les circonstances de chaque cas. Plus l'interception et l'analyse des informations collectées sont poussées, plus elles entrent en conflit avec le principe de la confidentialité des communications. Les finalités pour lesquelles la surveillance a lieu et les garanties appliquées en matière de protection des données constituent également des éléments clés pour déterminer le degré d'intrusion dans la vie privée et les données à caractère personnel des individus. Le verrouillage et la surveillance à des fins de lutte contre les logiciels malveillants, assortis de limitations strictes de la conservation et de l'utilisation des données inspectées, ne sauraient être comparés à des situations où les informations sont enregistrées pour constituer des profils servant à la publicité comportementale.

80. En principe, le CEPD considère que, s'il est interprété et appliqué correctement et si son application est dûment contrôlée, le cadre existant de l'UE en matière de vie privée et de protection des données à caractère personnel est approprié pour garantir que le droit à la confidentialité est préservé et, de manière générale, que la protection de la vie privée et des données des individus n'est pas mise en péril ([35]). Les FSI ne peuvent utiliser ces mécanismes sauf s'ils appliquent correctement le cadre juridique. Plus particulièrement, les éléments pertinents du cadre que les FSI doivent prendre en considération et respecter sont, entre autres, les suivants:

— Les FSI peuvent appliquer des politiques de gestion du trafic visant à assurer la sécurité du service lors de sa fourniture, notamment en limitant la congestion, conformément aux articles 4 et 6 de la directive «vie privée et communications électroniques».

— Les FSI doivent disposer d'un autre fondement juridique spécifique, et éventuellement du consentement des utilisateurs, pour appliquer des politiques de gestion du trafic qui supposent de traiter les données relatives au trafic ou aux communications à des fins autres que celles susmentionnées. Par exemple, le consentement informé des utilisateurs est nécessaire pour surveiller et filtrer les communications des individus dans le but de limiter (ou d'autoriser) l'accès à certains services et applications tels que le P2P ou la voix sur IP.

— Le consentement doit être libre, explicite et informé. Il doit être indiqué par une action positive. Ces exigences mettent fortement l'accent sur la nécessité d'intensifier les efforts visant à informer correctement les individus d'une manière qui soit directe, compréhensible et spécifique de sorte qu'ils puissent évaluer les effets des pratiques et prendre *in fine* une décision en connaissance de cause. Vu la complexité de ces techniques, la communication préalable d'informations utiles est une des principales difficultés à surmonter pour obtenir un consentement valable. En outre, les utilisateurs qui ne consentent à aucune forme de surveillance ne doivent pas s'exposer à des conséquences préjudiciables (notamment financières).

([35]) Sans préjudice de la nécessité de modifier la législation sur la base d'autres considérations, notamment dans le contexte de la révision générale du cadre juridique de l'UE en matière de protection des données afin de le rendre plus efficace dans le contexte des nouvelles technologies et de la mondialisation.

— Le principe de la proportionnalité joue un rôle crucial lorsque les FSI appliquent des politiques de gestion du trafic, quels que soient le fondement juridique du traitement et la finalité: fournir le service, éviter la congestion ou offrir des abonnements ciblés avec ou sans accès à certains services et applications. Ce principe limite la capacité des FSI à surveiller le contenu des communications des individus lorsque cela implique de traiter des informations excessives ou de réserver les avantages au seul profit des FSI. Ce qui peut être réalisé par les FSI sur le plan logistique dépendra du niveau d'intrusion des techniques, des résultats escomptés (qui peuvent leur rapporter des avantages) et des garanties spécifiques appliquées en matière de vie privée et de protection des données. Avant de déployer les techniques d'inspection, les FSI doivent évaluer si celles-ci sont conformes au principe de la proportionnalité.

81. Bien que le cadre juridique comprenne actuellement des conditions et des garanties pertinentes, il est nécessaire d'accorder une attention particulière à la question de savoir si les FSI respectent effectivement les exigences légales, s'ils fournissent les informations nécessaires aux consommateurs leur permettant de prendre des décisions éclairées et s'ils observent le principe de proportionnalité. Au niveau national, les autorités compétentes pour les questions précitées sont notamment les autorités nationales chargées des télécommunications, d'une part, et les autorités chargées de la protection des données, d'autre part. Au niveau de l'UE, l'ORECE figure parmi les organismes concernés. Le CEPD peut également être appelé à jouer un rôle dans ce contexte.

82. Outre la surveillance du degré actuel de respect de la réglementation, vu le caractère relativement récent de la possibilité d'inspecter massivement et en temps réel les communications, certains aspects liés à l'application du cadre qui ont été abordés dans le présent avis nécessitent une analyse plus approfondie et une clarification ultérieure. Parmi les orientations présentant un intérêt particulier dans plusieurs domaines, citons:

— la détermination des pratiques d'inspection qui sont légitimes pour garantir le bon déroulement du trafic et qui ne nécessitent pas le consentement des utilisateurs, comme la lutte contre les pourriels. Outre le caractère intrusif de la surveillance appliquée, des aspects tels que le niveau de perturbation du trafic qui en résulterait sont pertinents;

— la détermination des techniques d'inspection qui peuvent être mises en œuvre à des fins de sécurité, et qui peuvent ne pas nécessiter le consentement des utilisateurs;

— la détermination des conditions dans lesquelles le consentement de l'individu est requis, notamment le consentement de tous les utilisateurs concernés, et des paramètres techniques acceptables pour garantir que la technique d'inspection n'entraîne pas un traitement de données qui n'est pas proportionné aux objectifs poursuivis;

— en outre, dans les trois cas précités, des orientations peuvent s'avérer nécessaires en ce qui concerne l'application des garanties nécessaires en matière de protection des données (limitation des finalités, sécurité, etc.).

83. Étant donné que les compétences dans ce domaine sont partagées entre le niveau national et l'UE, le CEPD considère qu'il est essentiel d'échanger des vues et des expériences afin de trouver des approches harmonisées en la matière. À cet effet, il suggère la création d'une plate-forme ou d'un groupe d'experts qui réunirait des représentants des autorités réglementaires nationales, le groupe de travail «Article 29», le CEPD et l'ORECE. Le premier objectif de cette plate-forme serait d'émettre des orientations, au moins sur les points cités ci-dessus, afin de garantir des approches solides et harmonisées et des conditions équitables. Le CEPD appelle la Commission à organiser cette initiative.

84. Enfin, et ce n'est pas le moins important, tant les autorités nationales que leurs homologues de l'UE, et notamment l'ORECE et la Commission européenne, doivent s'intéresser de près aux évolutions du marché dans ce domaine. Du point de vue de la protection des données et de la vie privée, le scénario qui verrait les FSI appliquer de manière routinière des politiques de gestion du trafic en offrant des abonnements basés sur le filtrage de l'accès au contenu et aux applications poserait de graves problèmes. S'il devait se réaliser un jour, une législation devrait être adoptée pour remédier à cette situation.

VII. **CONCLUSIONS**

85. Le recours croissant des FSI aux techniques de surveillance et d'inspection affecte la neutralité de l'internet et la confidentialité des communications, ce qui soulève d'importantes questions concernant la protection de la vie privée et des données à caractère personnel des utilisateurs.

86. Bien que la communication de la Commission sur l'ouverture et la neutralité de l'internet en Europe aborde brièvement ces questions, le CEPD estime qu'il est nécessaire de prendre de nouvelles initiatives pour la mise en place d'une politique satisfaisante sur la voie à suivre. Dans le présent avis, il contribue dès lors au débat politique en cours sur la neutralité de l'internet, plus particulièrement en ce qui concerne les aspects liés à la protection des données et à la vie privée.

87. Le CEPD considère que les autorités nationales et l'ORECE doivent surveiller la situation du marché. Cette surveillance devrait avoir pour effet d'indiquer clairement si le marché évolue vers une inspection massive et en temps réel des communications et de révéler les éventuels problèmes liés au respect du cadre juridique.

88. La surveillance du marché doit aller de pair avec une analyse plus approfondie des effets des nouvelles pratiques en matière de protection des données et de la vie privée sur l'internet. Le présent avis décrit certains domaines qui bénéficieraient d'une certaine clarification. Si des agences et des organismes de l'UE tels que l'ORECE, le groupe de travail «Article 29» et le CEPD sont bien placés pour préciser les conditions d'application du cadre, le CEPD considère qu'il incombe à la Commission de coordonner et de diriger le débat. Aussi l'invite-t-il à prendre à cet effet une initiative associant toutes les parties prenantes au sein d'une plate-forme ou d'un groupe de travail. Parmi les questions nécessitant une analyse plus poussée, les points suivants devraient être abordés:

— déterminer les pratiques d'inspection qui sont légitimes pour assurer le bon déroulement du trafic et qui peuvent être utilisées à des fins de sécurité;

— déterminer les conditions dans lesquelles le consentement de l'individu est requis, notamment le consentement de tous les utilisateurs concernés, et les paramètres techniques acceptables pour garantir que la technique d'inspection n'entraîne pas un traitement de données qui n'est pas proportionné aux objectifs poursuivis;

— dans les cas précités, des orientations peuvent s'avérer nécessaires en ce qui concerne l'application des garanties nécessaires en matière de protection des données (limitation des finalités, sécurité, etc.).

89. En fonction de ces conclusions, des mesures législatives supplémentaires s'avéreront peut-être nécessaires. Dans ce cas, la Commission devrait proposer des mesures politiques visant à renforcer le cadre juridique et à garantir la certitude juridique. De nouvelles mesures devraient préciser les conséquences pratiques du principe de la neutralité de l'internet, comme cela s'est déjà fait dans certains États membres, et garantir que les utilisateurs peuvent vraiment faire un choix, notamment en obligeant les FSI à leur offrir des connexions non surveillées.

Fait à Bruxelles, le 7 octobre 2011.

Peter HUSTINX

Contrôleur européen de la protection des données