Recommandation n° 05/2012 du 11 avril 2012

Concerne : recommandation relative à la neutralité de l'internet, à la technologie "deep packet inspection" et à la protection de la vie privée et des données à caractère personnel dans le secteur des télécommunications (CO-AR-2012-002)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 30 ;

Vu le rapport de monsieur le Président ;

Émet le 11 avril 2012 la recommandation suivante :

I. INTRODUCTION

1. D'après le Contrôleur européen de la Protection des données[1] (ci-après le "CEPD"), le principe de la 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[2] ne peuvent hiérarchiser ou ralentir arbitrairement l'accès à certains services ou applications tels que le poste à poste (P2P), etc.[3]"*. Dans ce cadre, une proposition de loi antérieure[4] avait établi une comparaison explicative avec la liberté des utilisateurs du réseau d'électricité (classique, analogue[5]).

2. Pour la définition de la neutralité de l'internet, l'Institut belge des services postaux et des télécommunications[6] (ci-après l' "IBPT") se réfère au professeur américain Tim Wu, selon qui il s'agit *"du principe selon lequel un réseau public d'utilité maximale aspire à traiter tous les contenus, sites et plateformes de la même manière, ce qui lui permet de transporter toute forme d'information et d'accepter toutes les applications."*

3. La technologie "deep packet inspection" (inspection approfondie des paquets) (ci-après le "DPI") est une technologie qui peut être appliquée de différentes façons. Elle est massivement appliquée par les FSI européens à des fins de "gestion du réseau" ("traffic management"), parfois appelée "gestion de la bande passante" ou "traffic shaping" ("mise en forme du trafic"), avec "limitation de la bande passante" (voir ci-après). Des fonctions réseaux basées sur le DPI qui sont encore plus critiques pour la protection de la vie privée que la gestion du réseau sont celles qui permettent l'observation du réseau en temps réel à des fins d'interception - de potentielle à massive dans certains pays – et de profilage de certaines intentions. L'injection en ligne d'un certain contenu, notamment à des fins de publicité

---

[1] Citation issue de l'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*, JO du 8 février 2012, publié sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:FR:PDF.

[2] Les fournisseurs de services internet.

[3] Les FSI peuvent néanmoins limiter 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.

[4] *"Aujourd'hui, n'importe quel citoyen est libre de choisir son fournisseur d'électricité, ainsi que les équipements de raccordement au réseau. L'internaute doit également retrouver, ou conserver, une totale liberté d'utilisation de sa connexion au réseau. Un fournisseur d'électricité ne se préoccupe pas de la marque ou du nombre d'appareils électroménagers installés chez un particulier, si ce n'est pour lui fournir (et facturer) la puissance adaptée."* Voir le point 3.1. des développements de la proposition de loi du 13 juin 2005 *relative aux communications électroniques en vue de garantir la neutralité des réseaux Internet*, Chambre, DOC 53, 1467/001.

[5] On est en droit de se demander si ce raisonnement tient uniquement pour le réseau des télécommunications ou également pour le réseau d'électricité futur, à savoir le "smart grid" (réseau intelligent).

[6] Avis du Conseil de l'IBPT du 5 octobre 2011.

comportementale en ligne, fait également partie aujourd'hui des possibilités techniques les plus excessives[7].

4. Les systèmes DPI inspectent automatiquement des paquets entiers de données[8] qui circulent sur le réseau en tant que parties d'une communication. Ils peuvent approfondir cette inspection en scannant différentes "couches" ("layers") du trafic réseau[9], où chaque couche (qui s'emboîte dans une autre couche) possède un "header" (en-tête) et un "payload" (charge utile). Toutefois, chaque application DPI ne scanne pas la totalité des couches ; c'est en effet parfois inutile et coûteux[10].

5. Pour expliquer la technique du DPI utilisée à des fins de gestion du réseau, on la compare parfois, non sans soulever des critiques[11], au trafic postal classique. Pour tenir compte de ces critiques et donner une version plus correcte de l'analogie avec la poste, il faudrait utiliser l'image d'un colis composé de trois paquets différents, emboîtés les uns dans les autres, dont le paquet central contiendrait une lettre. Ce colis serait ouvert par la poste jusqu'à un certain paquet. Ensuite, certains cachets, codes-barres, etc. figurant sur les paquets seraient comparés avec une liste de cachets, codes-barres, etc. et, en fonction de la politique du bureau de poste, celui-ci déciderait de remettre ou non le colis ou de ralentir son envoi. La prise de connaissance du véritable contenu de la communication est également une possibilité technique (bien qu'illégale et donc moins fréquente) du DPI, que le message soit crypté ou non, tout comme la modification, l'accélération ou le ralentissement du message, selon la politique du FSI.

II. Contexte – Neutralité de l'internet

6. Le 19 avril 2011, la Commission européenne a adopté une communication intitulée "L'Internet ouvert et la neutralité de l'Internet en Europe"[12], qui révèle la volonté qui existe, depuis la conclusion du nouveau Paquet Télécom de l'UE de 2009, de consacrer la neutralité de l'internet et d'en faire un objectif politique et un principe réglementaire au niveau européen, que les autorités réglementaires nationales devront promouvoir. La Commission européenne

---

[7] Mochalski, Klaus en Schulze, Hendrik, IPpoque, *White Paper. Deep Packet Inspection. Technology, Applications & Net Neutrality*, à consulter sur http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf.

[8] L'en-tête et une partie des données. Voir la page 2 de l'étude http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf.

[9] IMF (Internet Message Format), SMTP (Simple Mail Transfer Protocol), TCP (Transmission Control Protocol) et IP (Intern Protocol). Voir la page 2 du *Whitepaper* susmentionné, publié sur http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[10] Voir la page 3 du *White Paper* susmentionné.

[11] Voir la page 3 du *White Paper* susmentionné.

[12] Communication de la Commission "L'Internet ouvert et la neutralité de l'Internet en Europe", COM(2011) 222 final, publiée sur http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011_fr.pdf.

avait notamment souligné que *"l'article 8, paragraphe 4, point g), de la directive "cadre"*[13] *exige des autorités réglementaires nationales qu'elles défendent les intérêts des citoyens de l'Union européenne en favorisant la capacité de l'utilisateur final à accéder à l'information et à en diffuser, ainsi qu'à utiliser des applications et des services"*.

7. Le CEPD a également exprimé une opinion sur la neutralité de l'internet, du moins en ce qui concerne les aspects relatifs à la protection des données et de la vie privée. Dans cette opinion récente[14], il a déclaré que *"La neutralité de l'Internet a trait à un débat d'actualité visant à déterminer si les fournisseurs de services Internet (FSI)*[15] *peuvent être autorisés à limiter, filtrer ou verrouiller l'accès à l'Internet ou affecter ses performances"*.

8. En 2011, les Pays-Bas ont été le premier État membre de l'UE à transposer, non sans critiques[16], le concept de la neutralité de l'internet dans la législation nationale[17]. Ceci après qu'en mai 2011, l'attention de la presse eût été fortement attirée quand un des opérateurs néerlandais fit connaître à des investisseurs son intention de pratiquer des tarifs variables pour des utilisateurs qui installaient des applications de communication gratuites telles que WhatsApp[18]. À ce moment-là, des analystes avaient demandé d'où cet opérateur tenait soudainement que l'utilisation de cette application était en forte augmentation chez ses clients. L'opérateur en question avait alors reconnu utiliser un logiciel d'analyse pour déterminer les habitudes de ses utilisateurs individuels[19], tout en se référant, d'autre part, à la baisse des revenus provenant du trafic des SMS.

9. Ce qui est positif, c'est que depuis peu, le débat sur la neutralité de l'internet s'est également ouvert en Belgique, notamment au sein du groupe d'utilisateurs BELTUG[20].

---

[13] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 (directive "cadre").

[14] 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*, JO du 8 février 2012, publié sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:FR:PDF.

[15] Cela comprend la fourniture d'un accès aussi bien fixe que mobile à l'Internet.

[16] L'avis du conseil de l'IBPT du 5 octobre 2012 renvoie à la critique de la Commissaire européenne Neelie Kroes sur l'intervention législative des Pays-Bas dans les termes suivants : *"Elle a regretté le fait que les Pays-Bas avaient choisi de faire cavalier seul sur le terrain de la régulation de l'Internet et a évoqué ses craintes que l'attitude néerlandaise ait des conséquences dommageables pour le marché."*

[17] http://www.rijksoverheid.nl/onderwerpen/ict/netneutraliteit et https://zoek.officielebekendmakingen.nl/kst-32549-3.html.

[18] WhatsApp est une application de messagerie pour téléphones mobiles. L'application a été développée pour les smartphones et permet d'envoyer des SMS, de chatter et de partager des fichiers tels que des photos gratuitement. À l'origine, l'application avait été développée pour l'iPhone et ensuite, elle a également été rendue disponible pour les autres systèmes d'exploitation tels qu'Android, Blackberry, Windows Phone 7, Symbian Nokia Series 40.

[19] O'Brien, Kevin J., Dutch lawmakers Adopt Net Neutrality law, New York Times, 22 juin 2011, publié sur http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=1.

[20] http://www.beltug.be/page/3/Who_is_BELTUG/.

10. Plusieurs propositions en la matière ont été déposées à la Chambre :

    - proposition de loi du 17 mai 2011 [21] modifiant la loi du 13 juin 2005 *relative aux communications électroniques en vue de garantir la neutralité des réseaux Internet*, déposée par les députés Deom et consorts ;

    - proposition de révision de la Constitution du 18 mai 2011[22] complétant l'article 23, afin de consacrer le principe de la neutralité des réseaux Internet, déposée par les députés Deom et consorts ;

    - proposition de loi du 1er juin 2011 [23] modifiant la loi du 13 juin 2005 *relative aux communications électroniques, en ce qui concerne la neutralité du réseau*, déposée par les députés Van den Bergh et consorts.

11. Enfin, l'IBPT a également publié un avis [24] en la matière qui, en ce qui concerne la problématique de la neutralité de l'internet, renvoie principalement à l'étude réalisée par l'Office des régulateurs européens des communications électroniques (ORECE ou BEREC en anglais) ainsi qu'à la position provisoirement attentiste en la matière du vice-président de la Commission européenne (voir ci-après).

III. Contexte – Deep Packet Inspection

12. Ces dernières années, plusieurs acteurs – au sein et en dehors de l'Europe – ont attiré l'attention sur l'impact potentiel de la technologie DPI sur la protection de la vie privée[25]. Le Groupe 29[26] et le Groupe de travail international sur la protection des données dans les télécommunications ou Groupe de Berlin[27] ont formulé un point de vue en la matière.

13. Le 6 mars 2012, l'ORECE a publié ses premières conclusions sur les pratiques rapportées de gestion du réseau [28], après y avoir été invité par le vice-président de la Commission européenne[29]. Bien que l'on constate une grande diversité de pratiques au sein des États

---

[21] Voir le blog personnel du député Peter Dedecker (http://peterdedecker.eu/blog/netneutraliteit) et la proposition de loi publiée sur http://www.dekamer.be/FLWB/PDF/53/1467/53K1467001.pdf.

[22] Voir http://www.lachambre.be/doc/flwb/pdf/53/1471/53k1471001.pdf et http://www.numerama.com/magazine/18867-le-ps-belge-veut-inscrire-la-neutralite-du-net-dans-la-constitution.html.

[23] Voir http://www.dekamer.be/doc/flwb/pdf/53/1536/53k1536001.pdf#search="netneutraliteit" et http://www.clickx.be/print/130923/wetsvoorstel-netneutraliteit-is-klaar/.

[24] Avis du Conseil de l'IBPT du 5 octobre 2011 sur les amendements des 7 et 12 juillet 2011 à la proposition de loi modifiant la loi du 13 juin 2005 *relative aux communications électroniques en vue de garantir la neutralité des réseaux Internet*, publié sur http://www.ibpt.be/ShowDoc.aspx?objectID=3628&lang=FR.

[25] Voir le débat au Royaume-Uni en 2008 concernant l'entreprise Phorm, voir un rapport d'étude canadien sur http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf.

[26] Voir le point 3.1. de l'avis n° 1/2009.

[27] Groupe de travail international sur la protection des données dans les télécommunications (Groupe de Berlin). http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.

[28] http://erg.eu.int/. Voir l'enquête BEREC citée dans COM(2011) 222 final et http://berec.europa.eu/doc/2012/TMI_press_release.pdf.

[29] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/623&type=HTML.

membres, il s'avère que la pratique la plus courante de "gestion du réseau" en Europe consiste à bloquer et/ou à limiter le trafic de poste à poste (P2P) et à bloquer le trafic Voice over IP (téléphonie par Internet), typiquement via le DPI.

14. En 2011, des rapports publics du contrôleur des Pays-Bas[30] de 2011 révélaient déjà l'existence généralisée de l'analyse du trafic des données en vue de "gestion du réseau" par les quatre plus grands FSI nationaux[31]. Lors de cette analyse, ceux-ci prenaient connaissance de plus d'éléments du trafic que les seules informations destinées à le régler. Ainsi, le type d'application (WhatsApp, Google talk, Twitter, …) utilisée par l'utilisateur final était à un moment donné affiché et éventuellement bloqué.

15. Contrairement au débat susmentionné sur la neutralité de l'internet, la Commission constate qu'en Belgique, le débat spécifique[32] sur les risques et les conditions légales du DPI est encore assez peu développé. Ceci alors que dans les pays voisins[33], le marché est en pleine expansion et qu'en 2011, au moins un FSI belge[34] a commencé à tester le DPI sur le trafic P2P de ses abonnés, ce qui a suscité quelques remous dans les médias néerlandophones. Un député a déjà qualifié cette initiative d' "intolérable"[35].

---

[30] http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3438 et http://www.opta.nl/nl/download/publicatie/?id=3439 : "Le collège constate que tous les fournisseurs de réseau examinés utilisent, dans une mesure plus ou moins grande, des techniques d'observation et d'analyse de paquets de données qui sont transportées sur leurs réseaux mobiles. Des flux de données et des applications sont alors identifiées, nécessitant une analyse à un niveau parfois approfondi. Une analyse approfondie implique à cet égard davantage que la seule consultation du header d'un paquet de données par le fournisseur." [Traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]

[31] KPN, Vodafone, Tele2 et T-Mobile.

[32] Voir la Question écrite n° 5-2393 d'Alexander De Croo (Open Vld) du 26 mai 2011 au ministre pour l'Entreprise et la Simplification, publiée sur http://www.senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=5&NR=2393&LANG=nl. Dans cette réponse à une question parlementaire posée au Sénat le 7 juillet 2011 à l'ancien ministre pour l'Entreprise et la Simplification en Belgique, le ministre compétent ne se montrait en tout cas pas très préoccupé par cette problématique : *"Je ne connais actuellement aucun fournisseur belge de télécommunications qui envisage de recourir au DPI et à ce stade il ne me semble pas opportun d'interroger les firmes à ce propos."* Pour le reste, il s'est contenté de renvoyer à l'article 124 de la loi du 13 juin 2005 et à l'article 314*bis* du Code pénal.

[33] Récemment, la presse française faisait également état de l'application par Orange de la technique du DPI sur ses abonnés à des fins de marketing direct de services Orange, comme en attesteraient les conditions générales du FSI en question, inchangées depuis 2008. http://www.cnetfrance.fr/news/orange-utilise-les-donnees-relatives-au-trafic-des-abonnes-39768678.htm.

[34] Un FSI flamand bien connu a annoncé dans les médias du 23 juin 2011 qu'il allait procéder à des tests (pour une durée indéterminée) de "traffic management" ou "traffic shaping" (Grommen, S., "Telenet knijpt p2p verkeer af", Datanews / Knack, 23 juin 2011). Selon le porte-parole de ce FSI, il ne s'agirait pas d'examiner le contenu du trafic de données. Il n'est toutefois pas exclu que l'on teste une autre forme d'intrusion dans le trafic de données des utilisateurs. Belgacom ne pratiquerait pas actuellement le "traffic shaping" ou le DPI. Selon la Commission, le "traffic shaping" constitue bel et bien une forme de DPI au sens du working party telecom. Il s'agit toujours d'une intrusion dans le trafic des utilisateurs.

[35] Voir http://peterdedecker.eu/blog/netneutraliteit : *"L'opérateur transporte des données de A vers B, sans se mêler de ces données elles-mêmes. Le DPI est donc inadmissible, tout comme le ralentissement ou le bocage de certains flux de données individuels. Cela a des relents de situations à la chinoise et est totalement contraire aux valeurs démocratiques de l'Internet libre. Sans Internet libre, il n'y a pas non plus de développement de services nouveaux et novateurs"*. [Traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]

IV. Recommandation pour un encadrement légal de la neutralité de l'internet

16. Dans son avis n° 10/2012 du 21 mars 2012[36], la Commission a déjà déclaré qu'elle estimait que le législateur devrait également ancrer dans la loi du 13 juin 2005 le nouveau principe européen de neutralité de l'internet. Elle a également annoncé son intention de formuler une recommandation distincte sur les thèmes de la neutralité de l'internet et du deep packet inspection.

17. La Commission se rallie entièrement à l'appel européen[37] d'ancrer légalement le principe de la neutralité de l'internet, de préférence dans la loi du 13 juin 2005, par le biais de l'introduction (notamment) d'une définition du principe de neutralité. Autrement dit, elle n'est pas partisane de la position selon laquelle la transposition (technique) de la législation européenne (complexe) en matière de télécoms suffira à dissiper les inquiétudes exprimées jusqu'à présent en ce qui concerne la neutralité de l'internet[38]. Dans l'avis susmentionné, la Commission a déjà attiré l'attention sur le fait qu'outre le manque de connaissances du citoyen moyen concernant l'impact des techniques susmentionnées, la complexité de la législation européenne sur les télécoms proprement dite constituait un facteur de complication pour parvenir à une protection effective des données à caractère personnel des personnes concernées. Dans la présente recommandation, elle souhaite également aborder les risques liés au DPI ainsi que les exigences existantes en vertu du droit européen en matière de protection des données dont il faudra également tenir compte au terme de l'étude effectuée par l'ORECE (voir ci-après).

18. Une plus grande attention devrait être consacrée à l'application de la neutralité de l'internet aux divers marchés dans lesquels les personnes concernées sont (seront) de plus en plus profilées de façon automatique pour toutes sortes de finalités (des profils de téléchargement plus précis obtenus par la technologie DPI et des compteurs intelligents sont utilisés pour la gestion du réseau, la gestion de l'équilibre ou pour d'autres finalités telles que l'exclusion de certains services, l'inscription sur une liste noire, le marketing direct, la différentiation de produits et de prix, …). La propension croissante au profilage et les capacités grandissantes en la matière de divers marchés concernant l'utilisation de services de base (télécoms, énergie, …) soulèveront de plus en plus de questions, vu la tendance européenne claire de parvenir à une meilleure protection des personnes physiques contre le profilage.

19. Le manque de neutralité lors du profilage dans ce genre de marchés (profils énergétiques des utilisateurs, …) peut conduire tôt ou tard à des excès incontrôlables (inscriptions sur des listes

[36] Avis relatif au projet de loi portant des dispositions diverses en matière de communications électroniques.

[37] Voir ci-avant.

[38] Telle est la position défendue par l'IBPT dans la conclusion de son avis du 5 octobre 2011.

noires, systèmes tarifaires non transparents sur la base du profil de la personne concernée, …).

V. Examen : la (non) culpabilité du Deep Packet Inspection et recommandations

20. Le verrouillage de données à caractère personnel à l'aide de procédés automatisés constitue un traitement de données à caractère personnel qui relève de la LVP (voir la définition de "traitement" à l'article 1, § 2 de la LVP).

21. Un malentendu veut que le DPI ne serait pas vraiment grave parce qu'il consiste à "tester", parce que le FSI ne détecterait que le type de trafic, qu'il ne prendrait pas connaissance du contenu et qu'il n'examinerait pas quelles données ou quels fichiers sont partagés ou téléchargés[39] via P2P ou parce qu'il s'agit d'une "gestion normale du réseau".

22. Bien que la Commission reconnaisse que le DPI est une technique qui peut être appliquée pour différentes finalités et à différents niveau du trafic, elle n'adhère pas à ces arguments. L'utilisation du DPI à des fins de gestion du réseau devient assez rapidement synonyme de détection et de manipulation en temps réel du type de trafic de la personne concernée. Les capacités de classification et la précision des systèmes modernes de DPI ne sont pas gênées par le cryptage appliqué par les utilisateurs[40].

23. Le DPI n'est pas non plus un traitement anodin car il implique également la prise de connaissance de l'existence d'une communication, en combinant quatre éléments. On est en présence (1) d'un traitement de données à caractère personnel[41], (2) avec une évaluation du type de trafic de la personne concernée en fonction (3) d'une politique (inconnue pour la personne concernée) du FSI basée sur le profilage[42], où on recherche de façon ciblée des attributs ("markers") ou des schémas prédéfinis [43] dans le trafic, entraînant (4) des conséquences ou des décisions concrètes pour la personne concernée. Il existe aussi une potentialité d' "observation du comportement", afin par exemple d'empêcher l'utilisation de

---

[39] Voir http://klantenservice.telenet.be/content/daalt-mijn-internetsnelheid-als-ik-peer-peer-diensten-gebruik.

[40] Voir la page 5 http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf qui renvoie à une étude de janvier 2009 de l'European Advanced Networking Test Center (EANTC). Ce test est publié sur http://www.internetevolution.com/document.asp?doc_id=178633.

[41] Pour l'analyse de ces éléments, voir l'avis 04/2007 du Groupe 29 WP 136 du 20 juin 2007 sur le concept de données à caractère personnel. Cette définition reflète l'intention du législateur européen de donner une large définition des données à caractère personnel, à laquelle on s'est tenu tout au long du processus législatif. Le choix des mots demande une interprétation large.

[42] Ce que l'on appelle le "customer class load profiling". Voir la Recommandation CM/Rec(2010)13 du 23 novembre 2010 du Comité des Ministres aux États membres *sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, publiée sur https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

[43] Voir la page 3 du *White paper* http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

service concurrents légaux du FSI ou de vérifier, chiffres à l'appui, combien d'utilisateurs sont déjà passés à un service concurrent[44], après quoi les utilisateurs peuvent faire l'objet de ce que l'on appelle du "marketing de rétention".

24. Enfin, il n'est pas évident de définir en quoi consiste une "gestion normale du réseau". Rédiger une définition juridique légale de la gestion de l'internet est peut-être insuffisant. En la matière, l'ORECE et l'IBPT pourraient également définir des normes techniques pour un "traffic management" normal, bien qu'ici aussi, on puisse affirmer que cette solution technique offre en soi une protection insuffisante si l'on ne tient pas compte de la pression exercée pour développer d'autres applications à haut risque du DPI, du manque de connaissances techniques et des prévisions raisonnables des personnes concernées dans le contexte d'une gestion neutre de l'internet (voir ci-après).

5.1. Applications légales du DPI

25. L'utilisation de la technique du DPI peut varier de potentiellement légitime à manifestement illégale. Dans la pratique, l'utilisation légale du DPI sera fortement liée au contexte et dépendra surtout de la question de savoir si (1) il existe un bon cadre légal (article 8 de la CEDH), surtout pour les risques les plus élevés, si (2) l'utilisateur a reçu suffisamment d'informations préalables et a bénéficié d'une transparence suffisante en la matière ou si le DPI fait partie des prévisions raisonnables de l'utilisateur, (3) si les finalités poursuivies sont claires et légitimes, et si (4) l'application du DPI est proportionnelle (jusqu'où peut-on inspecter les communications, la limitation ou le blocage actifs sont-ils nécessaires, existe-il des alternatives techniques[45]).

26. La Commission constate qu'il existe une confusion ainsi que de nombreuses discussions concernant les formes d'application légitimes ou non du DPI. Le point de vue à cet égard diffère selon les acteurs, parmi lesquels on trouve des autorités, des ONG[46], le secteur des technologies [47], des juristes [48] et le secteur privé (industrie de la publicité, des droits d'auteur, …)[49].

---

[44] Voir http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=1.

[45] Par exemple accorder des priorités à différentes classes d'applications n'a pas nécessairement d'impact sur la qualité du service. Voir la page 7 du *White Paper* susmentionné.

[46] Voir par exemple https://nodpi.org/ et http://www.badphorm.co.uk/page.php?2.

[47] Par ex., des vendeurs de cette technologie attirent l'attention sur les possibilités du DPI pour certaines applications ou fonctions réseau si l'on dépasse la limite symbolique de la première couche (IP) http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[48] Par exemple à propos de l'affaire Sabam Sabam c Tiscali : Note d'observations, Filtrage P2P : possibilités techniques et obstacles juridiques, RDTI, 30/2008.

[49] http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf.

27. Il est possible d'utiliser le DPI de façon correcte et légale, comme par exemple dans la technologie de la sécurisation et du firewall[50]. D'après la Commission européenne, il est également *"largement admis que les opérateurs de réseau doivent adopter certaines méthodes de gestion du trafic pour veiller à l'utilisation efficace de leurs réseaux et que certains services IP, comme la TV sur IP en temps réel et la vidéoconférence, peuvent exiger une gestion spéciale du trafic pour garantir une qualité de service élevée, d'un niveau prédéfini."*[51] Parmi les autres applications DPI peu critiquées jusqu'à présent, citons celles qui sont présentes dans les filtres anti spam, les filtres antivirus pour les communications électroniques, les systèmes de "cache" (pour les pages web), les applications pour la résolution de problèmes, …[52]

28. La Commission observe que les exemples susmentionnés concernent toujours des applications dont l'utilisateur moyen peut raisonnablement prévoir qu'elles inspectent son trafic internet (par exemple, qu'un logiciel antivirus scanne le trafic à la recherche de virus) (voir l'article 4, § 1, 2° de la LVP).

5.2. Risques liés à certaines applications du DPI

29. Certaines applications du DPI présentent manifestement un risque élevé pour la protection de la vie privée. Voici un relevé des risques les plus interpellants.

30. D'après des études existantes, il existe un risque manifeste d'interprétation arbitraire des notions de "gestion du réseau" et d' "interventions dictées par des groupes de pression"[53] sur le trafic des données (voir ci-après).

31. La possibilité pour des FSI de perturber le trafic des données et de bloquer ou d'empêcher **l'utilisation de services meilleur marché, innovants de tiers** (par exemple les applications WhatsApp, Skype, …) constitue un premier risque. La presse a déjà qualifié ce comportement de FSI comme étant celui de "percepteurs autoproclamés de taxes sur l'internet mobile"[54]. La Commission européenne a déclaré que *"Toutefois, le fait que certains opérateurs, pour des raisons ne tenant pas à la gestion du trafic, puissent bloquer ou dégrader des services licites (notamment de voix sur IP) qui concurrencent leurs propres*

---

[50] http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.

[51] Communication de la Commission "L'Internet ouvert et la neutralité de l'Internet en Europe", COM(2011) 222 final, publiée sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:FR:HTML.

[52] Voir la page 3 de http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf.

[53] Voir les termes utilisés dans un rapport d'étude sur la neutralité de l'internet, publié sur : http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000280933/Net+neutrality%3A+Innovation+and+differentiation+are+not+polar+opposites.pdf.

[54] "self-appointed toll collectors of the mobile internet". Voir O'Brien, Kevin J., Dutch lawmakers Adopt Net Neutrality law, New York Times, 22 juin 2011, publié sur http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=1.

services, peut être considéré comme allant à l'encontre de l'ouverture d'Internet."[55] Enfin, un développeur allemand de technologie DPI vante auprès de ses clients la possibilité d'utiliser le DPI pour protéger leurs propres revenus contre la concurrence directe[56], si des clients utilisent Skype, par exemple.

32. Le DPI a déjà été appliqué à des fins de **marketing direct** (notamment pour de la publicité comportementale en ligne) par le biais d'une collaboration entre des FSI et des tiers[57]. Le Groupe de Berlin a émis une réserve claire à ce sujet[58].

33. Le DPI a également été invoqué (soi-disant) pour la prévention des **infractions aux droits d'auteur**[59], soit par les FSI eux-mêmes, soit sous la pression de tiers. Pour la Cour de Justice[60] et le législateur néerlandais[61], il a déjà été démontré que l'intention ne peut absolument pas être que, sous la pression de certains secteurs culturels, le DPI soit appliqué par des FSI en tant que mesure préventive et active visant à surveiller tous les clients.

34. Il ressort également de l'affaire susmentionnée portée devant la Cour de Justice que la neutralité de l'internet ne relève pas de la responsabilité de FSI mais que les États membres doivent préserver un équilibre entre la protection des détenteurs de droits intellectuels (droit à la propriété) et la protection des droits fondamentaux des individus qui sont touchés par de

---

[55] Communication de la Commission "L'Internet ouvert et la neutralité de l'Internet en Europe", COM(2011) 222 final, publiée sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:FR:HTML.

[56] Voir la rubrique "Revenue Protection and generation", page 10 http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[57] Voir Pfanner, Eric, 3 Internet Providers in Deal for tailored Ads, New York Times, 18 février 2008, publié sur http://www.nytimes.com/2008/02/18/technology/18target.html?_r=1.
Les parties connues aux USA pour rechercher des accords avec des FSI étaient (auparavant) NebuAd, Phorm, Adzilla et le projet Rialto. Ces dernières années, on a surtout parlé de l'utilisation de Phorm par BT. Voir http://www.guardian.co.uk/commentisfree/libertycentral/2011/apr/14/phorm-cps-justice-bt.

[57] http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.

[58] http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821.

[59] MEEUS, Roland, "Muziekindustrie vraagt downloaders te vervolgen als internetpedofielen", De Morgen, 19 mars 2011. Voir également le rapport de l'OFCOM intitulé *"Site blocking to reduce online copyright infringement"* du 27 mai 2011. Certains FSI appliquent déjà des systèmes d' "inspection de paquets" dans leur réseau pour la gestion du trafic et pour d'autres finalités ; nous considérons dès lors que cette gestion est réalisable, bien qu'elle soit très complexe et très coûteuse pour quiconque n'utilise pas encore ce type de services. Peut-être que, vu les investissements en capital requis, le DPI ne pourra être utilisé, à court ou à moyen terme, que par les plus gros FSI.

[60] Voir Cour de Justice, Affaire C-70/10 du 24 novembre 2001 dans l'affaire Scarlet contre SABAM, publiée sur http://curia.europa.eu.

[61] L'exposé des motifs de la modification de la loi néerlandaise sur les télécommunications mettant en œuvre les directives révisées sur les télécommunications résume bien cette situation : " *Sur la base du compromis entre le Conseil des Ministres et le Parlement, un État membre conserve la possibilité d'exclure totalement ou partiellement des utilisateurs de l'Internet. Toutefois, ces mesures nécessitent la plus grande minutie. En vertu du nouvel alinéa 3bis de l'article 1er de la Directive cadre, elles ne peuvent être appliquées que si elles sont adéquates, proportionnelles et nécessaires au bon fonctionnement d'une société démocratique. Elles doivent en outre être exécutées dans le respect des garanties procédurales ad hoc, conformément à la Convention Européenne pour la Protection des Droits de l'Homme et des Libertés Fondamentales et au principe général du droit de l'Union européenne, dont la protection juridictionnelle efficace et le droit à un procès équitable. Cela signifie que l'utilisateur à exclure doit être présumée innocente présumé innocent et qu'il faut tout d'abord examiner, dans le cadre d'une procédure équitable et impartiale, s'il existe des motifs suffisants pour procéder à la fermeture ou à la limitation de l'accès avant qu'un utilisateur soit partiellement ou totalement exclu d'Internet. La procédure en question doit également prévoir l'audition des deux parties. Une possibilité de recours doit également être prévue contre une décision d'exclusion totale ou partielle"* (voir https://zoek.officielebekendmakingen.nl/kst-32549-3.html). [Traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]

telles mesures (article 8 de la CEDH). Cette affaire met en évidence le risque que représente **l'absence d'une utilisation équilibrée et neutre de la technologie DPI** ainsi que la nécessité d'offrir une base légale explicite et des garanties aux personnes concernées en cas d'utilisation de cette technologie. Dans ce contexte, les mesures concrètes qui sont proposées sont : limiter davantage le temps et le ciblage en ce qui concerne la surveillance de certains clients (plutôt que de tous) et s'abstenir de viser toute utilisation de la technologie P2P (autrement dit observer une neutralité technologique).

35. Le manque de clarté des communications stratégiques de certains FSI constitue également un risque. Ainsi, les finalités réelles de la limitation de la technologie P2P et les "taux de limitation"[62] qui varient d'un FSI à l'autre, … ne sont pas toujours clairement indiqués. Les FSI ont la possibilité de perturber volontairement le trafic des données. Cela comporte un **risque** manifeste **de "function creep"**[63], c'est-à-dire un risque de finalités cachées, illégitimes du DPI[64] sous le couvert de notions vagues, voire interprétées de façon arbitraire par le FSI, telles que la "gestion du réseau", lesquelles sont potentiellement contraires au principe de la neutralité de l'internet.

36. Chez le FSI belge susmentionné, la "phase de test" de la limitation du trafic P2P dure depuis mi-2011. Entre-temps, un manque de transparence envers les utilisateurs a été constaté par le JEP[65] (Jury voor Ethische Praktijken inzake reclame - Jury d'Éthique Publicitaire). Il est frappant de constater que certains acteurs du secteur des médias et de la distribution (par exemple la BBC, …)[66] qualifiaient précisément la technologie P2P de technique efficace et fiable pour fournir, diffuser à bas coût des messages médiatiques ou du streaming en live alors qu'aujourd'hui, les utilisateurs ne sont pas informés de façon suffisamment claire des véritables finalités et des conséquences juridiques de la limitation de la technologie P2P.

37. La Commission attire enfin l'attention sur le fait que le manque de transparence évoqué ci-avant compromet évidemment aussi un contrôle ou une imputabilité spécifiques (imputabilité ou "accountability" réduite).

---

[62] http://www.zdnet.be/news/132291/telenet-teruggefloten-rond-p2p-vertraging/, les informations limitées dans http://klantenservice.telenet.be/content/daalt-mijn-internetsnelheid-als-ik-peer-peer-diensten-gebruik.

et http://webwereld.nl/nieuws/108311/upc-kneep-40-procent-torrentverkeer-af.html.

[63] http://dpi.priv.gc.ca/index.php/essays/dpi-the-future-is-out-there/ et http://wiki.vuze.com/w/Bad_ISPs#Belgium.

[64] Comme lorsque le FSI concerné veut éviter la concurrence légale, moins coûteuse via la technologie P2P ou VOIP sur le marché belge des médias.

[65] http://www.zdnet.be/news/132291/telenet-teruggefloten-rond-p2p-vertraging/.

[66] Voir http://www.p2p-next.org/?page=content&id=264A360A217FB3FE8BD82CB9C928CBCF&mid=6BED2EAC3D127503EF53456A25D9204E.

5.3. Principes et obligations existants dans la LVP qui sont applicables au DPI

38. La Commission a déjà souligné précédemment[67] la complémentarité entre la LVP et la loi du 13 juin 2005. Elle souhaite formuler ci-après plusieurs remarques concernant des obligations et des dispositions existantes de la LVP qu'elle estime particulièrement importantes.

39. Tout traitement via la technologie DPI doit être basé sur un des cas mentionnés à l'article 5 de la LVP[68].

40. Une première possibilité est que le DPI soit effectué dans le contexte de procédures policières ou judiciaires[69], c'est-à-dire en application de l'article 5 c) et e) de la LVP.

41. Pour d'autres applications du DPI par des FSI, on examinera ci-après la possibilité d'appliquer l'article 5 a) (consentement), 5 b) (contrat avec le FSI) et 5 f) de la LVP.

42. Compte tenu de la confusion possible d'intérêts dans le chef des FSI pratiquant la limitation (voir ci-avant), le risque existe que les contrats de télécommunications (donc un recours à l'article 5, b) de la LVP) avec les personnes concernées ou le "consentement"[70] de la personne concernée (article 5, a) de la LVP) n'offrent pas en soi suffisamment de garanties pour une légitimation neutre d'un traitement DPI et pour des mesures efficaces prises par les FSI en vue de protéger les personnes concernées contre la limitation de leur trafic de télécommunications et contre le traitement de données relatives à leur profil obtenues par DPI.

43. Enfin, divers intérêts légitimes peuvent exister pour invoquer le recours par des FSI à la technologie DPI (article 5 f) de la LVP). Ces intérêts peuvent être déterminés par le législateur ou n'appellent aucune remarque particulière par rapport aux prévisions raisonnables des personnes concernées (voir les cas mentionnés aux points 25 à 28 inclus).

44. Pour tout traitement de données à caractère personnel, il convient de communiquer chaque **finalité**. Cette finalité doit être explicite et légitime (article 4, § 1, 1° et 2° et article 9, § 1 de

---

[67] Voir l'avis n° 10/2012 du 21 mars 2012.

[68] Le Groupe 29 avait déjà indiqué précédemment dans son avis 01/2009 que les fondements juridiques justifiant le traitement des données relatives au trafic par les services de communications électroniques accessibles au public ainsi que le traitement des données à caractère personnel par le responsable du traitement des données sont exposés à l'article 6 de la Directive 2002/58/CE/ ainsi qu'aux articles 7 et 17 de la directive sur la protection des données (transposée par les articles 5 et 16 de la LVP).

[69] Voir l'article 90 du Code d'Instruction criminelle et l'article 125 de la loi du 13 juin 2005.

[70] Il n'est pas question de consentement si le DPI fait partie de la politique du FSI. Cela n'est pas non plus lié à la question de savoir si le consentement ("cookie consent") est requis en vertu de l'article 5.3 modifié de la Directive 2002/58/CE. Le DPI ne concerne pas le stockage dans l'équipement terminal d'un utilisateur ou d'un abonné. Comme mentionné précédemment, la demande croissante de la neutralité de l'internet constitue la motivation première pour également brider le DPI sur le plan réglementaire.

la LVP). Cela implique également une interdiction d'appliquer le DPI en l'absence de finalités déterminées, explicites et légitimes (article 4, § 1, 2° de la LVP). Les termes "tests" et "gestion du réseau" couramment utilisés par des FSI sont à cet égard beaucoup trop vagues (voir ci-dessus le point 34).

45. Le respect de **l'obligation d'information** par les acteurs privés est essentiel, bien que souvent[71] négligé. L'obligation d'information complémentaire reprise à l'article 74 du projet de loi[72] s'applique sans préjudice de l'article 9 de la LVP. Sur leurs sites Internet, les FSI doivent donc tenir compte de l'article 9 de la LVP[73]. Il convient en particulier de communiquer quelles mesures appropriées sont prises pour garantir le respect des droits des personnes concernées au sens de la LVP, s'il existe une collaboration du FSI avec un tiers (par exemple Phorm, …) et quelles sont les implications concrètes de l'application de la technologie DPI.

46. Comme toute technique d'analyse, le DPI peut également mener à des conclusions erronées, généralisées, ou au traitement de **données à caractère personnel sensibles** au sens des articles 6, 7 ou 8 de la LVP (par exemple l'utilisateur concerné télécharge illégalement des œuvres protégées par le droit d'auteur, …).

47. **Toute mesure automatisée** (telle que la limitation de tout trafic P2P, la différentiation de paquets, le routage de paquets IP et le filtrage) qui va au-delà d'une gestion raisonnable du trafic et **qui peut produire des effets juridiques à l'égard de la personne concernée**[74] ou l'affecter de manière significative[75] tombe sous le coup de l'interdiction formulée à l'article 12*bis* de la LVP. La Commission constate que les traitements automatisés de limitation peuvent impliquer des restrictions à l'utilisation de services légaux, moins coûteux et novateurs de tiers (WhatsApp, Skype, Spotify,…) qui sont en concurrence avec les services des FSI. Des mesures unilatérales de FSI (qui proposent également des services média) peuvent également potentiellement léser les personnes concernées. En effet, cela peut empêcher l'utilisation potentiellement légale et moins coûteuse de la technologie P2P offerte par des concurrents pour des services de musique, de vidéo à la demande ou de télévision par internet (par exemple Spotify[76] ou d'autres futurs acteurs du marché européen des médias qui entendront utiliser le P2P comme moyen de distribution). Un tel inconvénient n'est pas insignifiant au regard de l'article 12*bis* de la LVP.

---

[71] Voir le point 60 de l'avis n° 10/2012 du 21 mars 2012.

[72] Projet de loi portant des dispositions diverses en matière de communications électroniques.

[73] Voir les points 102 et suivants de la Directive 2009-657 du Conseil de la radiodiffusion et des télécommunications canadiennes, publiée sur http://www.crtc.gc.ca/fra/archive/2009/2009-657.htm.

[74] Par exemple l'imputation de frais supplémentaires.

[75] Par exemple la limitation de la vitesse ("throttling") ou le blocage du trafic Internet (ou de certains types de trafic Internet).

[76] Ainsi, le service commercial Spotify utilise la technologie P2P jusqu'à 30 %. Voir http://www.lemonde.fr/technologies/article/2012/03/19/la-diffusion-de-musique-sur-internet-un-univers-d-astuces-et-de-compromis_1671854_651865.html et http://www.csc.kth.se/~gkreitz/spotify-p2p11/kreitz-spotify-p2p11.pdf.

48. Bien que le contrat ou la loi puisse définir un fondement pour soutenir des décisions automatisées, le contrat ou le législateur doit également prévoir **des mesures adéquates pour protéger les intérêts légitimes des personnes concernées** (voir l'article 12*bis*, dernier alinéa de la LVP et les recommandations ci-après). La Commission estime que le contrat est moins approprié à cette fin (voir le point 41) et souligne que la neutralité de l'internet et la définition de mesures adéquates relèvent surtout de la responsabilité du législateur ou du régulateur.

49. Le DPI soulève enfin des questions concernant des **incidents de sécurité** au sein de FSI et concernant la politique relative au règlement du trafic de données par des FSI. Peut-on envisager qu'un employé d'un FSI détourne la technologie DPI par appât du gain, par exemple en analysant l'utilisation de l'application par les clients existants, sans que cela soit la politique du FSI ?). Une plus grande transparence externe est nécessaire concernant les questions de savoir qui peut bloquer le trafic de données et à quelles conditions, si des tiers (par exemple des spécialistes du marketing, des employeurs) peuvent demander à un FSI de régler autrement le trafic de l'internet concernant un site internet déterminé (par exemple celui d'une organisation syndicale[77]).

5.4. Recommandations concernant un cadre légal plus clair et un meilleur contrôle du DPI

50. Sur la base des remarques formulées aux point 37 à 46 inclus, la Commission formule ci-après trois recommandations concrètes.

5.4.1. Recommandation 1 : définition de la notion de "gestion normale du réseau (afin de permettre l'application de l'article 5, f) de la LVP)

51. Dans la mesure où il ne s'agit pas de DPI dans le contexte de procédures policières ou judiciaires[78], la Commission considère plus intéressant de baser certaines applications de DPI par des FSI sur l'article 5, f) de la LVP pour ce que le législateur ou le régulateur a reconnu comme application légale du DPI. Elle attire l'attention sur les applications légales mentionnées aux points 25 à 28 inclus. La logique est notamment que le législateur ou l'IBPT sont les mieux placés pour déterminer ce que doit recouvrir la notion vague de "gestion normale du réseau", dans le respect du principe de la neutralité de l'internet et de la neutralité technologique vis-à-vis de techniques telles que le VOIP et le P2P, ainsi que de

[77] Cet exemple est tiré d'une affaire canadienne d'août 2005 où un FSI canadien (Telus) avait bloqué l'accès à un site Internet créé par un syndicat.

[78] Voir l'article 90 du Code d'instruction criminelle et l'article 125 de la loi du 13 juin 2005.

l'évaluation des risques requise. Il vaut mieux recourir à une intervention législative ou régulatoire - qui constitue la base la plus neutre sur laquelle les personnes concernées peuvent fonder leurs prévisions raisonnables (article 4, § 1, 2° de la LVP) -, plutôt que de laisser l'interprétation de cette notion de "gestion normale du réseau" à l'appréciation arbitraire de chaque FSI dans le contrat conclu avec celui-ci.

5.4.2. Recommandation 2 : approche nuancée et pluridisciplinaire du DPI via l'exigence d'un examen préalable du respect de la vie privée, un contrôle a posteriori, ...

52. Compte tenu de l'évolution du droit européen de protection des données en matière de profilage [79], le législateur (européen) et l'IBPT devront mettre au point une approche pluridisciplinaire pour l'application de la technologie DPI qui prend en compte davantage de critères qu'une analyse de marché économique.

53. Autrement dit, l'utilisation de la technologie DPI devra continuer à faire l'objet d'un suivi minutieux par les diverses instances de contrôle en matière de protection des données (Groupe 29) afin de pouvoir effectuer une évaluation de l'impact sur la vie privée ("privacy impact assessment") en plus de l'analyse de marché que la Commission européenne planifie encore sur la base de l'étude de l'ORECE.

54. Pour les formes les plus extrêmes de DPI produisant des effets juridiques directs à l'égard des personnes concernées (par exemple en cas de décisions automatisées sans garanties légales adéquates au sens de l'article 12*bis* de la LVP ou en cas de traitement de données à caractère personnel sensibles), les dispositions prohibitives existantes issues de la LVP et de la Directive 95/46/CE doivent en tout cas déjà être appliquées.

55. L'exigence européenne d'examen préalable [80] (risques élevés dans le cas de certaines applications de DPI) et, le cas échéant, le contrôle a posteriori par la Commission et/ou l'IBPT peuvent faire partie d'une approche du DPI qui soit plus nuancée et plus neutre sur le plan technologique. Les limites des possibilités de profilage, les alternatives au DPI /la nécessité d'y recourir, la politique de conservation des données et les garanties accompagnant le profilage doivent être définies. La Commission a l'intention de continuer à suivre cet aspect.

---

[79] Voir la Recommandation CM/Rec(2010)13 du 23 novembre 2010 du Comité des Ministres aux États membres *sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, publiée sur https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282010%2913&Language=lanFrench&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864. Exposé des motifs publié sur https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029&Site=CM

[80] Article 20 de la Directive 95/46/CE.

5.4.3. Recommandation 3 : obligation d'information accrue grâce à une nouvelle modification de la loi du 13 juin 2005 en cas de recours au DPI

56. L'article 74 du projet de loi portant des dispositions diverses en matière de communications électroniques modifie l'article 113, § 5 de la loi du 13 juin 2005 en prévoyant une plus grande transparence[81] à l'égard de l'IBPT ou des personnes concernées lors du recours au DPI ou à la gestion du réseau.

57. Eu égard aux risques liés à l'utilisation de la technique du DPI, la Commission estime que l'application du nouvel article 113, § 5 de la loi du 13 juin 2005 est insuffisante. Le législateur doit garantir un contrôle plus ciblé de l'utilisation de la technique du DPI par des FSI.

58. Sur la base de la LVP, le législateur et/ou l'IBPT peuvent aujourd'hui prévoir ou encourager des garanties plus concrètes concernant l'utilisation du DPI, parmi lesquelles :

- le relevé officiel des formes d'application de DPI ainsi que des moments, des finalités et des types de trafic auxquels cette technologie peut ou non s'appliquer, sous certaines modalités préalablement définies (conservation/stockage, initiation d'une requête interne ou externe, gravité des conséquences pour les personnes concernées, transparence, instruments juridiques et garanties procédurales, …). Ce relevé doit aller au-delà de l'élaboration juridique ou technique d'une définition juridique ou d'une norme pour la gestion du réseau, en fixant les finalités d'utilisation concrètes et en définissant de façon objective et concrète le degré de risque concret pour les personnes concernées (article 4, § 1, 2° de la LVP) ;
- par finalité pour laquelle la technologie DPI est utilisée, une attention accrue pour le principe de proportionnalité avant d'appliquer les formes les plus poussées de DPI (limitation, blocage, …) (article 4, § 1, 3° de la LVP). Cela implique d'apporter davantage d'uniformité dans la (trop) grande marge de manœuvre des FSI concernant la question de savoir quelles applications doivent bénéficier de quelles priorités[82], avant que l'ISP puisse décider de procéder au blocage ou à la limitation. On peut également citer l'utilisation de données agrégées pour la planification du réseau par des FSI (les données à caractère

[81] Cette nouvelle disposition est libellée comme suit : *"1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre.*

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées."

[82] Voir la page 7 du *White Paper* susmentionné.

personnel traitées doivent être suffisamment codées, évitant ainsi le risque de réutilisation à des fins commerciales)[83] (article 16, § 4 de la LVP) ;

- l'obligation spécifique du FSI d'informer l'utilisateur, de manière intelligible, s'il utilise ou non le DPI, ce qui ne se résume pas à une simple mention dans sa politique de respect de la vie privée et/ou dans ses conditions générales. Les FSI devraient communiquer leur politique de gestion du réseau avec ou sans l'aide de la technologie DPI[84], en tant que finalité du traitement, de façon très claire et très ouverte à toutes les personnes concernées (surtout à leur clients effectifs et potentiels). Cela pourrait se faire sous la forme d'une FAQ, avec des explications aux utilisateurs. L'obligation d'information spécifique peut trouver une base réglementaire dans la LVP en prévoyant un arrêté royal, pris sur la base des termes actuels "informations supplémentaires" (à déterminer par le Roi après avis de la Commission) au sens de l'article 9, § 1, e) de la LVP ;
- l'introduction de mesures de sécurité spécifiques concernant le DPI (article 16, § 4 de la LVP). À l'exemple d'autres marchés tels que celui de l'électricité où la gestion du réseau et la fourniture de services ont été scindées, encourager l'intervention d'un "trusted third party" pour évaluer, organiser et coordonner une éventuelle limitation nécessaire et neutre du trafic. C'est possible en définissant des normes techniques pour la gestion du réseau et un contrôle subséquent par l'IBPT (article 16, § 4 de la LVP) ;
- l'application du DPI par des collaborateurs de FSI devrait faire l'objet d'une journalisation (article 16, § 4 de la LVP).

[83] Voir le point 105 de la Directive 2009-657 du Conseil de la radiodiffusion et des télécommunications canadiennes, publiée sur http://www.crtc.gc.ca/fra/archive/2009/2009-657.htm.

[84] Voir la page 9 du *White Paper* susmentionné.

La Commision décide :

Neutralité de l'internet

Le principe de la neutralité de l'internet touche à la question fondamentale de savoir qui peut exercer un contrôle du traitement de données à caractère personnel via des réseaux électroniques publics, sous quelles conditions et pour quelles finalités. L'Europe considère que ce principe doit être transposé en priorité dans la législation nationale afin de garantir une meilleure protection des personnes concernées. La Commission se rallie entièrement à une telle demande européenne, de préférence via l'ancrage du principe de neutralité de l'internet dans la loi du 13 juin 2005, par le biais de l'introduction (entre autres) d'une définition du principe de neutralité.

Enfin, la Commission estime utile d'entamer le débat sur l'application de la neutralité de l'internet en dehors du secteur des télécommunications, vu la propension croissante au profilage dans le secteur de l'électricité qui peut compromettre le traitement égal des personnes concernées ainsi que leur accès neutre à des services de base via des mesures telles que le blocage, la limitation, l'inscription sur des listes noires ou une diversification non transparente de formules tarifaires ou de traitement (exiger des garanties pour l'accès à des services de base), …

DPI

Le droit européen de protection des données met de plus en plus l'accent[85] sur la nécessité pour les législateurs de prévoir des mesures de protection adéquates pour les applications à hauts risques pour les personnes concernées et pour l'application automatique de mesures basées sur le profilage. Dans la présente recommandation, la Commission a attiré l'attention sur des risques plus élevés qui ressortent de certaines applications de la technique du DPI (par exemple la limitation du trafic P2P légal, l'utilisation à des fins de marketing direct, de possibles formes de décisions automatisées basées sur le DPI avec des effets nuisibles pour les personnes concernées, …).

La Commission est favorable à une approche du DPI neutre sur le plan technologique. En soi, l'utilisation de la technologie du DPI n'est pas problématique. Toutefois, le niveau d'application, les formes d'application potentielles du DPI avec un risque plus élevé pour les personnes concernées nécessitent une réglementation. En cas d'application de la technique du DPI, le principe de la neutralité de l'internet doit toujours être respecté.

La Commission est également partisane d'une étude pluridisciplinaire européenne des diverses applications de cette technologie. Cela signifie que le Groupe 29 et le CEPD devront tôt ou tard

[85] Via l'obligation d'évaluation préalable et la protection contre le profilage de personnes physiques.

également ajouter une appréciation à l'analyse de marché que la Commission européenne effectuera sur la base des informations collectées via l'ORECE.

La Commission attire également d'emblée l'attention sur l'obligation de tenir compte des dispositions prohibitives et des obligations existantes, en vertu du droit européen de protection des données et de la LVP, sur la base des articles 4, § 1, 2°, 6 à 9 inclus, 12*bis* et 16, § 4 de la LVP. La Commission appelle le législateur et/ou l'IBPT à encore mieux protéger les personnes concernées en associant à chaque application du DPI des effets plus explicites de ces articles existants. Ceci en complément de la protection offerte via l'obligation d'information supplémentaire imposée par l'article 74 du projet de loi portant des dispositions diverses en matière de communications électroniques.

La Commission se réserve le droit de continuer à suivre minutieusement les débats européens dans ce domaine et, si nécessaire, de formuler des recommandations plus concrètes à l'égard du législateur et de l'IBPT si l'on négligeait, sur le plan européen, de demander une évaluation européenne en matière de vie privée au Groupe 29.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere