Aanbeveling nr 05/2012 van 11 april 2012

Betreft: Aanbeveling over netneutraliteit, deep packet inspection en bescherming van de persoonlijke levenssfeer en persoonsgegevens in de telecomsector (CO-AR-2012-002)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op het verslag van de heer voorzitter;

Brengt op 11 april 2012 de volgende aanbeveling uit:

I. Inleiding

1. Het begrip netneutraliteit[1] komt volgens de EDPS *"voort uit de visie dat informatie op internet onpartijdig moet worden doorgegeven, ongeacht de inhoud, bestemming of bron, en dat de gebruikers moeten kunnen beslissen welke toepassingen, diensten en apparatuur zij willen gebruiken. Dit betekent dat* ISPs[2] *niet naar eigen goeddunken de toegang tot bepaalde toepassingen, zoals peer-to-peer („P2P") en dergelijke, voorrang kunnen geven of mogen vertragen[3]."* In dit kader werd in een eerder wetsvoorstel[4] de illustratieve vergelijking gemaakt met de vrijheid van de gebruikers van het (klassieke, analoge[5]) elektriciteitsnet.

2. Het BIPT[6] verwijst voor de definitie van netneutraliteit naar de Amerikaanse professor Tim Wu volgens dewelke het draait *"om het principe dat een openbaar netwerk met maximaal nut alle inhoud, sites, en platformen op dezelfde manier tracht te behandelen, waardoor het alle informatie kan vervoeren en alle toepassingen kan aanvaarden."*

3. "deep packet inspection" (hierna "DPI") is een techniek die op verschillende wijzen kan worden toegepast. Deze techniek wordt intussen massaal aangewend door Europese ISPs voor "netbeheer" ("traffic management"), soms bandbreedtebeheer of "traffic shaping" genoemd met "afknijpen van bandbreedte" (zie hierna). DPI-gebaseerde netwerkfuncties die nog kritischer zijn voor de bescherming van de persoonlijke levenssfeer in vergelijking met netbeheer zijn realtime netwerkmonitoring voor interceptie, potentieel in enkele landen zelfs met massale interceptie en het profileren van bepaalde doelen. Ook online injectie van een bepaalde inhoud zoals voor online gerichte reclame behoort vandaag tot de meest excessieve technische mogelijkheden[7].

---

[1] Citaat uit het advies van de Europese toezichthouder voor gegevensbescherming over netneutraliteit, beheer van verkeersstromen en bescherming van de persoonlijke levenssfeer en persoonsgegevens, PB 8 februari 2012, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:NL:PDF

[2] Internet service providers

[3] ISP's mogen wel beperkingen opleggen aan de overdrachtssnelheid of de hoeveelheid informatie die een abonnee kan verzenden of ontvangen in het geval van abonnementen met bandbreedte- of volumebegrenzing. Derhalve zouden ISP's op grond van het netneutraliteitsbeginsel nog steeds abonnementen met beperkte toegang tot internet op basis van criteria als snelheid of volume mogen aanbieden, mits daarbij niet wordt gediscrimineerd op grond van inhoud.

[4] *"Vandaag kan elke burger vrij zijn elektriciteitsleverancier kiezen, alsook de uitrusting voor zijn aansluiting op het elektriciteitsnet. Ook de internetgebruiker moet (opnieuw) volledig vrij zijn in het gebruik van zijn internettoegang. Een elektriciteitsleverancier laat zich niet in met de keuze van het merk van de huishoudtoestellen of het aantal dergelijke toestellen in het huis van een particulier; het enige wat hij doet is de klant de gepaste hoeveelheid elektriciteit verschaffen (en factureren)."* Zie punt 3.1. van de toelichting bij het wetsvoorstel tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie, teneinde de neutraliteit van de internetnetwerken te waarborgen, Kamer, DOC 53, 1467/001.

[5] De vraag kan terecht worden gesteld of deze redenering enkel opgaat voor het telecommunicatienetwerk, of ook voor het elektriciteitsnet van de toekomst, zijnde "smart grid".

[6] Advies van de Raad van het BIPT van 5 oktober 2011

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

4. DPI systemen inspecteren automatisch ganse datapakketten[8] die in het netwerk circuleren als deel van een communicatie. Men kan hierbij tot op diepte van diverse lagen het netwerkverkeer[9] bekijken, waarbij er voor elke (herverpakte) laag een "header" en een "payload" is. Anderzijds is het ook niet zo dat bij elke toepassing van DPI alle lagen worden gescand, dit is soms niet noodzakelijk en duur[10].

5. De techniek van DPI, gebruikt ten behoeve van netbeheer, wordt soms, zij het niet zonder kritiek[11], aan de hand van het normale klassieke postverkeer uitgelegd. Als rekening wordt gehouden met deze kritiek zou een correctere versie van de postanalogie betekenen dat drie verschillende postpakken die telkens in elkaar zijn gestoken met als inhoud een echte brief tot op een bepaald niveau door de post worden geopend, waarna (minstens) bepaalde stempels, barcodes edm op de pakketten worden vergeleken met een bestaande stempel/barcode edm lijst en waarbij men beslist om het pakket al dan niet, of trager te bezorgen naargelang het beleid van de post. Kennisname van de echte inhoud van de communicatie is bij DPI uiteraard ook een technische (zij het illegale en dus minder voorkomende) mogelijkheid, of de boodschap versleuteld is of niet, net als de wijziging, versnelling en vertraging van de boodschap volgens het beleid van de ISP.

II. Context - Netneutraliteit

6. Op 19 april 2011 heeft de Europese Commissie² een mededeling over het open internet en netneutraliteit in Europa[12] goedgekeurd, waaruit de wil blijkt sinds de sluiting van het nieuwe EU telecompakket in 2009 om netneutraliteit te verankeren als Europese beleidsdoelstelling en Europees regelgevingsprincipe dat door nationale regelgevingsinstanties moet worden bevorderd. De Europese Commissie wees o.m. op het gegeven dat *"nationale regelgevende instanties overeenkomstig artikel 8, lid 4, onder g), van de kaderrichtlijn[13] verplicht* (zijn) de *belangen van de burgers van de Europese Unie te bevorderen, door het vermogen van de eindgebruikers te bevorderen om toegang te krijgen tot informatie en deze te verspreiden of om gebruik te maken van toepassingen en diensten".*

---

[8] De header en een deel van de gegevens. Zie Mochalski, Klaus en Schulze, Hendrik, IPpoque, White Paper. Deep Packet Inspection. Technology, Applications & Net Neutrality, te raadplegen op http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf en pagina 2 van de studie 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) en IP (Interne Protocol). Zie pagina 2 van voormelde whitepaper gepubliceerd ophttp://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[10] Zie pagina 3 van voormelde white paper.

[11] Zie pagina 3 van voormelde white paper

[12] Mededeling van de Commissie "Het Open internet en netneutraliteit in Europa", COM (2011) 222 definitief, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:NL:PDF

[13] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 (kaderrichtlijn).

7. De EDPS formuleerde ook een standpunt over netneutraliteit, althans wat de aspecten in verband met gegevensbescherming en privacy betreft. In haar recente opinie[14] stelde zij "*Netneutraliteit verwijst naar een debat over de vraag of het internetaanbieders (Internet Service Providers — „ISP's[15]") moet zijn toegestaan de toegang tot internet te beperken, filteren of blokkeren, of anderszins de prestaties van internet te beïnvloeden".*

8. Nederland was in 2011[16], zij het niet zonder kritiek[17], de eerste lidstaat van de EU die het concept van netneutraliteit in nationale wetgeving omzette. Dit na ruime persaandacht toen een van de Nederlandse operatoren in mei 2011 aan investeerders bekend maakte variabele tarieven te willen hanteren voor gebruikers die bepaalde gratis communicatietoepassingen zoals WhatsApp[18] installeerden. Analisten stelden hierbij de vraag waar deze operator plots de kennis vandaan haalde rond de sterke toename in gebruik van deze toepassing bij haar klanten, waarna deze operator toegaf analytische software te gebruiken om de gewoontes van haar individuele gebruikers in kaart te brengen[19], terwijl anderzijds op het dalend inkomen uit het SMS verkeer werd gewezen.

9. Positief is dat sinds kort ook in België het debat over netneutraliteit werd opgestart, o.m. in de schoot van de gebruikersgroep BELTUG[20],

10. In de Kamer werden diverse voorstellen dienaangaande gelanceerd
    - wetsvoorstel van 17 mei 2011[21] tot wijziging van de Wet van 13 juni 2005 betreffende de elektronische communicatie, teneinde de neutraliteit van de internetnetwerken te waarborgen, ingediend door de Kamerleden Deom en consorten;
    - voorstel tot herziening van de Grondwet van 18 mei 2011[22], herziening van artikel 23, teneinde er het beginsel van de neutraliteit van de internetnetwerken in op te nemen, ingediend door de Kamerleden Deom en consorten;

---

[14] Advies van de Europese toezichthouder voor gegevensbescherming over netneutraliteit, beheer van verkeersstromen en bescherming van de persoonlijke levenssfeer en persoonsgegevens, PB 8 februari 2012, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:NL:PDF;

[15] Dit omvat het aanbieden van zowel vaste als mobiele internettoegang.

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

[17] Het advies van de raad van het BIPT van 5 oktober 2012 verwijst als volgt naar de kritiek van Europees commissaris Neelie Kroes op het wetgevend optreden van Nederland: "Ze betreurde het feit dat Nederland ervoor had gekozen op eigen houtje te handelen wat betreft de regulering van internet en uitte haar vrees dat de Nederlandse houding schadelijke gevolgen kan hebben voor de markt"

[18] Whatsapp is een is een berichtenapplicatie voor mobiele telefoons. De applicatie is ontworpen voor smartphones en maakt het mogelijk om gratis met elkaar te smsen, chatten en bestanden zoals foto's met elkaar te delen. Oorspronkelijk werd het ontworpen voor de iPhone, later werd het ook beschikbaar voor andere besturingssystemen zoals Android, Blackberry, Windows Phone 7, Symbian en Nokia Series 40

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

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

[21] Zie de persoonlijke weblog van de volksvertegenwoordiger dhr. Peter Dedecker (http://peterdedecker.eu/blog/netneutraliteit) en het wetsvoorstel gepubliceerd op http://www.dekamer.be/FLWB/PDF/53/1467/53K1467001.pdf

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

- wetsvoorstel van 1 juni 2011[23] tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie, wat betreft de netneutraliteit, ingediend door de Kamerleden Van den Bergh en consorten;

11. Tenslotte heeft ook het BIPT dienaangaande een advies[24] gepubliceerd, dat in de problematiek van netneutraliteit vnl. verwijst naar het onderzoek door het Orgaan van Europese regelgevende instanties voor elektronische communicatie ("BEREC"), en het voorlopig afwachtende standpunt van de vice-voorzitter van de Europese Commissie dienaangaande (zie hierna).

III. Context – Deep Packet Inspection

12. De mogelijke impact van de techniek van DPI op de bescherming van de persoonlijke levenssfeer werd de afgelopen jaren onder de aandacht gebracht door diverse actoren binnen en buiten Europa[25]. De Groep 29[26] en de Internationale werkgroep van Berlijn over dataprotectie in telecommunicatie[27] formuleerden dienaangaande een standpunt.

13. Op 6 maart 2012 publiceerde[28] BEREC haar eerste bevindingen over de gerapporteerde praktijken van netbeheer, na hiertoe te zijn verzocht door de vice-voorzitter van de Europese Commissie[29]. Hoewel er sprake is van een grote variatie aan praktijken in de lidstaten blijkt de meest voorkomende praktijk van "netbeheer" in Europa te bestaan in het blokkeren en/of afknijpen van peer to peer (P2P) verkeer en het blokkeren van Voice over IP verkeer, typisch via DPI.

14. Uit publieke rapporteringen van de toezichthouder in Nederland[30] in 2011 bleek reeds dat algemeen sprake is van het analyse van dataverkeer voor "netwerkbeheer" door de vier grootste Nederlandse ISP's[31], waarbij bij de analyse wordt kennis genomen van meer

---

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

24 Advies van de Raad van het BIPT van 5 oktober 2011 betreffende de wijzigingen van 7 en 12 juli 2011 aan het wetsvoorstel tot wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie teneinde de neutraliteit van de internetnetwerken te garanderen, gepubliceerd op http://www.bipt.be/ShowDoc.aspx?objectID=3628&lang=nl

25 Ze de discussie in UK in 2008 betreffende de onderneming Phorm, Zie een Canadees studierapprot op http://www.christopher-parsons.com/blog/wp-content/uploads/2011/04/Parsons-Deep_packet_inspection.pdf

26 Zie punt 3.1. advies 1/2009

27 Internationale werkgroep dataprotectie in telecommunicatie (groep van Berlijn). http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821

28 http://erg.eu.int/. Zie onderzoek BEREC aangehaald in COM (2011) 222 definitief en http://berec.europa.eu/doc/2012/TMI_press_release.pdf

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

30 http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3438 en http://www.opta.nl/nl/download/publicatie/?id=3439 : "Het college stelt vast dat alle onderzochte mobiele netwerkaanbieders in meer of mindere mate technieken gebruiken om datapakketten te monitoren en te analyseren die over hun mobiele netwerken getransporteerd worden. Daarbij worden gegevensstromen en applicaties geïdentificeerd en daarvoor vindt de analyse soms op diep niveau plaats. Een analyse op diep niveau houdt in dit verband in dat meer dan alleen de header van een datapakket bekeken wordt door de aanbieder."

31 KPN en Vodafone, Tele2 en T-Mobile

verkeer dan alleen de informatie die bestemd is voor de afhandeling. Zo wordt het gebruik van type applicatie (Whatsapp, google talk, twitter,…) op een bepaald ogenblik door de eindgebruiker in zicht gebracht, en eventueel geblokkeerd.

15. In tegenstelling tot voormeld debat rond netneutraliteit stelt de Commissie vast dat het specifieke debat in België[32] over de risico's en wettelijke voorwaarden voor DPI nog vrij onontwikkeld is. Dit terwijl de markt zich volop ontwikkelt in de ons omringende landen[33] en minstens een Belgische ISP[34] in 2011 van start is gegaan om DPI te testen op het P2P verkeer van haar abonnees, hetgeen enige ruchtbaarheid veroorzaakte in de Nederlandstalige media. Een volksvertegenwoordiger bestempelde dit reeds als ontoelaatbaar[35].

IV. Aanbeveling voor een wettelijke omkadering van netneutraliteit

16. In haar advies 10/2012 van 21 maart 2012[36] stelde de Commissie reeds dat zij van oordeel was dat de wetgever ook het nieuwe Europese beginsel van netneutraliteit zou dienen wettelijk te verankeren in de wet van 13 juni 2005. Zij kondigde hierbij aan over de thema's van netneutraliteit en deep packet inspection een aparte aanbeveling te formuleren.

17. De Commissie schaart zich voluit achter de Europese oproep[37] tot wettelijke verankering van het beginsel van netneutraliteit, bij voorkeur in de Wet van 13 juni 2005, via de invoering van (onder meer) een definitie van het neutraliteitsbeginsel. Zij is met andere woorden geen verdediger van de stelling dat de (technische) omzetting van de (complexe) Europese telecomwetgeving zal volstaan om de ongerustheden weg te nemen die tot op heden

---

[32] Zie Schriftelijke vraag nr. 5-2393 van Alexander De Croo (Open Vld) d.d. 26 mei 2011 aan de minister voor Ondernemen en Vereenvoudigen, gepubliceerd op http://www.senate.be/www/?MIval=/Vragen/SchriftelijkeVraag&LEG=5&NR=2393&LANG=nl. In dit antwoord op een parlementaire vraag in de Senaat van 7 juli 2011 aan de vorige minister van ondernemen en vereenvoudigen in België toonde de bevoegde minister alvast geen grote bekommernis over deze problematiek : "Ik heb op dit ogenblik geen weet van Belgische telecommunicatieaanbieders die DPI overwegen toe te passen en in dit stadium komt het mij niet opportuun voor om de bedrijven hierover te bevragen." Verder werd enkel verwezen naar artikel 124 van de wet van 13 juni 2005 en artikel 314bis Sw.

[33] Recente pers maakte ook gewag van het toepassen van de DPI techniek op abonnees van Orange in Frankrijk met het oog op direct marketingdoeleinden van Orange diensten, hetgeen zou blijken uit de algemene voorwaarden van de betreffende ISP die ongewijzigd bleven sinds 2008. http://www.cnetfrance.fr/news/orange-utilise-les-donnees-relatives-au-trafic-des-abonnes-39768678.htm

[34] Een gekende Vlaamse ISP kondigde in de media van 23 juni 2011 aan over gaan tot het testen (voor onbepaalde duur) van "traffic management" of "traffic shaping" (Grommen, S., Telenet knijpt p2P verkeer af, Datanews / Knack, 23 juni 2011.) Volgens de woordvoerder van deze ISP zou het niet gaan om het kijken naar de inhoud van het dataverkeer. Wel werd niet uitgesloten dat men andere vorm van inmenging in het dataverkeer van gebruikers test. Belgacom zou voorlopig niet aan traffic shaping of DPI doen. Volgens de Commissie is "traffic shaping" is wel degelijk een vorm van DPI in de zin van de working party telecom. Het gaat nog altijd om een inmenging in het verkeer van de gebruikers.

[35] Zie http://peterdedecker.eu/blog/netneutraliteit : *"De operator transporteert gegevens van A naar B en moeit zich niet met die gegevens zelf. DPI is dan ook uit den boze, net als het afremmen of blokkeren van bepaalde individuele datastromen. Dat stinkt naar Chinese toestanden en gaat regelrecht in tegen de democratische waarden van het vrije internet. Zonder vrij internet ook geen ontwikkeling van nieuwe, innovatieve diensten"*

[36] Advies betreffende het wetsontwerp houdende diverse bepalingen inzake elektronische communicatie.

[37] Zie hiervoor

worden geuit in verband met netneutraliteit[38]. Zij wees er in voormeld advies reeds op dat de complexiteit van de Europese telecomwetgeving zelf een complicerende factor is, naast het gebrek aan kennis van "jan modaal" over de impact van voormelde technieken teneinde een effectieve bescherming van de persoonsgegevens van de betrokkenen te bekomen. In deze aanbeveling wenst zij ook in te gaat op de risico's verbonden aan DPI en de bestaande vereisten onder het Europese gegevensbeschermingsrecht waarmee ook rekening zal dienen te worden gehouden na afronding van het onderzoek door BEREC (zie hierna)

18. Er zou meer aandacht dienen te gaan naar de toepassing van netneutraliteit op de diverse markten waarin de betrokkenen steeds meer op geautomatiseerde wijze (zullen) worden geprofileerd voor uiteenlopende doeleinden (preciezere laadprofielen verkregen door DPI en slimme meters worden gebruikt voor netbeheer, evenwichtsbeheer of andere doeleinden zoals dienstuitsluiting, blacklisting, direct marketing, product en prijsdifferentiatie,…). De toenemende profileringsdrang- en capaciteiten van diverse markten op het gebruik van basisdiensten (telecom, energie,..) zal steeds meer vragen stellen, gelet op de duidelijke Europese tendens tot een betere bescherming van natuurlijke personen tegen profilering.

19. Gebrek aan neutraliteit bij profilering in dergelijke markten (energieprofielen van de gebruikers,... kan vroeg of laat leiden tot oncontroleerbare excessen (zwarte lijsten, ontransparante tariefsystemen aan de hand van het profiel van de betrokkene,…).

V. Beoordeling : de (on)schuld van Deep Packet Inspection en aanbevelingen

20. Het afschermen van persoonsgegevens met behulp van geautomatiseerde procédés is een verwerking van persoonsgegevens die valt onder de WVP (zie de definitie van "verwerking" in artikel 1 § 2 WVP).

21. Een misverstand is dat DPI niet zo erg zou zijn, omdat het gaat om "testen", omdat de ISP enkel het type verkeer zou detecteren en de ISP geen kennis zou nemen van de inhoud, en dat de ISP niet bekijkt welke gegevens of bestanden via P2P worden gedeeld of gedownload[39], of omdat het gaat om "normaal netbeheer".

22. Hoewel de Commissie erkent dat DPI een techniek is die voor verschillende doeleinden en op verschillende lagen van het verkeer kan worden toegepast, treedt zij voormelde redeneringen niet bij. DPI voor doeleinden van netbeheer betekent al vrij vlug het real time detecteren en manipuleren van het type verkeer van de betrokkene. De

[38] Dit is de stelling die het BIPT verdedigt in de conclusie van haar advies van 5 oktober 2011.
[39] Zie http://klantenservice.telenet.be/content/daalt-mijn-internetsnelheid-als-ik-peer-peer-diensten-gebruik

classificatiecapaciteit en accuratesse van moderne DPI systemen ondervinden quasi geen hinder van door gebruikers toegepaste encryptie[40].

23. DPI is ook geen onschuldige bewerking omdat er ook sprake is van kennisname van het bestaan van een communicatie, waarbij vier elementen worden gecombineerd. Er is (1) een verwerking van persoonsgegevens[41], met (2) een evaluatie van het type verkeer van de betrokkene in functie van (3) een (voor de betrokkene ongekend) profielgebaseerd beleid[42] van de ISP waarbij gericht wordt gezocht naar vooraf bepaalde markeringspunten of patronen[43] in het verkeer, waaruit (4) concrete gevolgen of beslissingen ressorteren voor de betrokkene. Er is ook potentieel tot "gedragsmonitoring" aanwezig, zoals het onmogelijk maken om gebruik te maken van legale, concurrerende diensten van de ISP, of een cijfermatig nagaan hoeveel gebruikers reeds overgestapt zijn naar een concurrerende dienst[44] waarna de betrokkenen het voorwerp kunnen uitmaken van zgn. "retentiemarketing".

24. Het is tenslotte niet evident om te bepalen wat een "normaal netbeheer" is. Het schrijven van een juridische wettelijke definitie van netbeheer is wellicht onvoldoende. BEREC en het BIPT zouden dienaangaande ook technische standaarden voor normaal "traffic management" kunnen schrijven, hoewel ook hier geldt dat deze technische oplossing op zich onvoldoende bescherming geeft indien men geen rekening houdt met de druk om andere, hoge risicotoepassingen van DPI te ontwikkelen, en het gebrek aan technische kennis en de redelijke verwachtingen van de betrokkenen in de context van een neutraal netbeheer (zie hierna).

5.1. Legale DPI toepassingen

25. Gebruik van de techniek van DPI kan variëren van potentieel legitiem tot manifest illegaal gebruik. Legaal gebruik van DPI zal in de praktijk zeer contextgebonden zijn en vooral afhangen van de vraag of er (1) een degelijke wettelijke omkadering is (artikel 8 EVRM),

---

[40] Pagina 5 http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf die verwijs naar een studie van januari 2009 van het European Advanced Networking Test Center (EANTC). Deze test is gepubliceerd op http://www.internetevolution.com/document.asp?doc_id=178633

[41] Voor de analyse van deze elementen zie het advies 04/2007 van de Groep 29 WP 136 van 20 juni 2007 over het begrip persoonsgegeven. Deze definitie weerspiegelt de bedoeling van de Europese wetgever een brede definitie van persoonsgegevens te geven, waaraan tijdens het gehele wetgevingsproces is vastgehouden. De woordkeuze vraagt om een ruime interpretatie

[42] Zgn. "customer class load profiling". Zie Aanbeveling CM/Rec(2010)13 van 23 november 2010 van de Raad van Ministers over de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering, gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864
explanatory memorandum gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029&Site=CM

[43] Zie pagina 3 van de White paper http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

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

zeker voor de hoogste risico's of (2) er afdoende voorafgaande informatie en transparantie is van de gebruiker aangaande of dat DPI deel uitmaakt van de redelijke verwachtingen van de betrokkene, (3) of de finaliteiten duidelijk en legitiem zijn, en of (4) DPI op proportionele wijze wordt toegepast (hoe diep kan of moet men het berichtenverkeer gaan inspecteren, is er een noodzaak en bestaande technische alternatieven[45] voor het actief gaan afknijpen of blokkeren).

26. De Commissie stelt vast dat er verwarring en veel discussie bestaat over de al dan niet legitieme toepassingsvormen van DPI. Het standpunt hierover verschilt naargelang de actoren, waaronder overheden, NGO's[46], de technologiesector[47], juristen[48] en de private sector (advertentieindustrie, copyrightindustrie,…)[49].

27. Correct, legaal gebruik van DPI is mogelijk, zoals bijvoorbeeld in beveiligings- en firewalltechnologie[50]. Het is volgens de Europese Commissie ook *"algemeen aanvaard dat netwerkexploitanten een aantal methoden van verkeersbeheer moeten toepassen om een efficiënt gebruik van hun netwerken te verzekeren en dat een aantal IP-diensten, zoals realtime televisie over het internet (IPTV) en videoconferenties, een speciaal beheer van het verkeer kunnen vereisen om een vooraf bepaalde hoge kwaliteit van de dienstverlening te kunnen verzekeren."*[51] Andere toepassingen van DPI die tot op heden weinig kritiek oogsten zijn de toepassingen van DPI in spamfilters, virusfilters voor e-mailverkeer, cachesystemen (voor webpagina's), toepassingen voor probleemoplossing,…[52]

28. De Commissie merkt op dat het in voormelde voorbeelden telkens gaat om toepassingen waarvan de gemiddelde gebruiker redelijkerwijze kan verwachten dat zijn netwerkverkeer wordt onderzocht (bvb dat een antivirussoftware in het verkeer naar virussen zoekt) (zie artikel 4 § 1, 2° WVP).

---

[45] Bvb het toekennen van prioriteiten aan verschillende klassen toepassingen heeft niet noodzakelijk een impact op de kwaliteit van de dienst. Zie pagina 7 van voormelde white paper.
[46] Zie bvb https://nodpi.org/ en http://www.badphorm.co.uk/page.php?2
[47] bvb verkopers van deze technologie wijzen op de mogelijkheden van DPI voor bepaalde applicaties of netwerkfuncties indien verder wordt gegaan dan de symbolische grens van de eerste (IP) laag. http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf
[48] Bvb over de zaak Sabam t 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
[50] http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf?1292413821
[51] Mededeling van de Commissie "Het Open internet en netneutraliteit in Europa", COM (2011) 222 definitief, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:NL:PDF
[52] Zie pagina 3 van http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

5.2. Risico's bij bepaalde toepassingen van DPI

29. Bepaalde toepassingen van DPI vertonen duidelijk een hoog risico voor de bescherming van de persoonlijke levenssfeer. Hierna volgt een opsomming van de meest opvallende risico's.

30. Er is volgens bestaande studies een duidelijk risico van arbitraire interpretatie van het begrip "netbeheer" en "lobbygedreven interventies"[53] op het dataverkeer (zie hierna).

31. De mogelijkheid van ISPs om het dataverkeer te verstoren, en **om het gebruik van goedkopere, innoverende diensten van derden** (bvb Whatsapp, Skype,… toepassing) te blokkeren of te verhinderen is een eerste risico. De pers bestempelde dit eerder als het optreden door ISP's als "zelfbenoemde tolheffenaars op het mobiele internet"[54]. De Europese Commissie stelde *"Dat sommige exploitanten, om redenen die niets te maken hebben met beheer van het verkeer, legale diensten (in het bijzonder spraakdiensten over het internet –Voice over IP) kunnen blokkeren of terugschroeven wanneer deze diensten met hun eigen aanbod concurreren, kan dan weer beschouwd worden als een aanslag op het open karakter van het internet."*[55] Een Duitse ontwikkelaar van DPI technologie prijst tenslotte aan haar klanten de mogelijkheid aan om met behulp van DPI eigen inkomen te beschermen tegen directe competitie[56], indien klanten bijvoorbeeld Skype gebruiken.

32. DPI werd reeds toegepast voor **direct marketing** doeleinden (onder meer online reclame op basis van surfgedrag) door samenwerking tussen ISPs en derde partijen[57]. De Groep van Berlijn uitte dienaangaande een duidelijk voorbehoud[58].

33. DPI werd ook (zogenaamd) ingeroepen voor het bestrijden van **auteursrechtelijke inbreuken**[59], hetzij door ISPs zelf hetzij onder druk van derden. Voor het Hof van Justitie[60]

---

[53] Zie de term die wordt gebruikt in een onderzoeksrapport rond netneutraliteit gepubliceerd op 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". Zie O'Brien, Kevin J., Dutch lawmakers Adopt Net Neutrality law, New York Times, 22 Juni 2011, gepubliceerd op http://www.nytimes.com/2011/06/23/technology/23neutral.html?_r=1;

[55] Mededeling van de Commissie "Het Open internet en netneutraliteit in Europa", COM (2011) 222 definitief, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:NL:PDF

[56] Zie de rubriek "Revenue Protection and generation", pagina 10 http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[57] Zie Pfanner, Eric, 3 Internet Providers in Deal for tailored Ads, New York Times, 18 Februari 2008, gepubliceerd op http://www.nytimes.com/2008/02/18/technology/18target.html?_r=1
Gekende partijen die akkoorden nastreefden met ISPs in de VS waren (voorheen) NebuAd, Phorm, Adzilla en project Rialto. In de afgelopen jaren viel vooral het gebruik van Phorm door BT op in de discussies. Zie http://www.guardian.co.uk/commentisfree/libertycentral/2011/apr/14/phorm-cps-justice-bt

[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 maart 2011; Zie ook het rapport van OFCOM getiteld „Site blocking to reduce online copyright infringement" van 27 mei 2011, „Sommige ISP's passen al systemen voor „packet inspection" in hun netwerk toe voor verkeersstroombeheer en andere doeleinden; we nemen daarom aan dat dit beheer uitvoerbaar is, zij het dat het veel complexiteit en kosten met zich meebrengt voor wie nog

en de Nederlandse wetgever[61] werd reeds betoogd dat het alleszins niet de bedoeling zijn dat, onder druk van bepaalde culturele bedrijfstakken, DPI wordt toegepast door ISPs als preventieve en actieve maatregel tot monitoring van alle klanten.

34. Uit voormelde zaak voor Het Hof van Justitie blijkt ook dat netneutraliteit niet de verantwoordelijkheid is van ISPs, maar dat de lidstaten een evenwichtige balans moeten waarborgen tussen de bescherming van de houders van intellectuele rechten (recht op eigendom) en de bescherming van de fundamentele rechten van de individuen die door zulke maatregelen worden getroffen (artikel 8 EVRM). Uit deze zaak blijkt het risico op een **gebrek aan gebalanceerd, neutraal gebruik van DPI**, en de nood om een expliciete wettelijke basis en garanties voor de betrokkenen te geven bij gebruik van DPI. Uit voormelde zaak blijkt dat als concrete maatregelen aan de orde zijn : meer beperkingen in tijd en focus qua monitoring naar bepaalde (ipv alle) klanten toe en het zich onthouden van het viseren van elk gebruik van peer to peer technologie (met andere woorden technologische neutraliteit).

35. Ook de vaagheid van de beleidscommunicaties van sommige ISPs vormt een risico. De werkelijke doelstellingen voor het afknijpen van P2P technologie en de "afknijppercentages"[62] die variëren van ISP tot ISP,… worden niet altijd duidelijk vermeld. ISPs hebben de mogelijkheid om het dataverkeer vrijwillig te verstoren. Dit houdt een duidelijk **risico in voor "function creep"**[63]**.** Dit wil zeggen het risico voor verborgen, illegitieme doelstellingen van DPI[64] onder het mom van vage, eventueel arbitrair door de ISP geïnterpreteerde noties zoals "netbeheer" die potentieel ingaan tegen het beginsel van netneutraliteit.

---

niet van dergelijke diensten gebruikmaakt. Wellicht dat gezien de vereiste kapitaalinvesteringen DPI op korte tot middellange termijn alleen kan worden ingezet door de grotere ISP's

[60] Zie H v J, Zaak C-70/10 van 24 november 2001 in de zaak Scarlet t SABAM, gepubliceerd op htttp://curia.europa.eu

[61] In de Nederlandse memorie van toelichting bij de wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen vatte men deze situatie goed samen: *"Op grond van het compromis tussen Raad van Ministers en Parlement blijft een lidstaat de mogelijkheid houden om gebruikers geheel of gedeeltelijk af te sluiten van internet. Echter bij deze maatregelen moet uiterste zorgvuldigheid worden betracht. Op grond van het nieuwe lid 3 bis van artikel 1 van de Kaderrichtlijn mogen dergelijke maatregelen alleen worden opgelegd indien zij passend, evenredig en noodzakelijk zijn in een democratische samenleving. Bovendien moeten zij worden uitgevoerd met inachtneming van adequate procedurele waarborgen overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, en de algemene beginsel van recht van de Europese Unie, waaronder doeltreffende rechtsbescherming en eerlijke rechtsbedeling. Dit betekent dat uitgegaan moet worden van de onschuld van de af te sluiten gebruiker en dat eerst in een eerlijke en onpartijdige procedure moet worden bezien of er voldoende gronden zijn om tot het afsluiten of beperken van de toegang over te gaan voordat een gebruiker geheel of gedeeltelijk van internet wordt afgesloten. In de bedoelde procedure moet bovendien hoor en wederhoor mogelijk zijn. Ook moet het mogelijk zijn in beroep te gaan tegen een beslissing om geheel of gedeeltelijk af te sluiten"* (zie https://zoek.officielebekendmakingen.nl/kst-32549-3.html)

[62] http://www.zdnet.be/news/132291/telenet-teruggefloten-rond-p2p-vertraging/, de beperkte informatie in http://klantenservice.telenet.be/content/daalt-mijn-internetsnelheid-als-ik-peer-peer-diensten-gebruik en 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/ en http://wiki.vuze.com/w/Bad_ISPs#Belgium

[64] zoals het vermijden van legale, goedkopere concurrentie via P2P of VOIP technologie op de Belgische mediamarkt door de betrokken ISP.

36. Bij voormelde Belgische ISP sleept de "testfase" van het afknijpen van P2P verkeer aan sinds midden 2011. Intussen is er ook voor dezelfde ISP een gebrek aan afdoende transparantie naar de gebruikers toe vastgesteld door de JEP[65]. Het valt op dat sommige spelers in de mediasector en distributiesector (bvb BBC,…)[66] de P2P technologie juist als een efficiënte, betrouwbare techniek bestempelden om tegen een lage kost mediaboodschappen of livestreams te verzorgen, terwijl vandaag gebruikers onvoldoende duidelijk worden geïnformeerd over de echte doelstellingen en rechtsgevolgen van het afknijpen van P2P technologie.

37. De Commissie wijst er tenslotte op dat voormeld gebrek aan transparantie uiteraard ook een specifieke controle of toerekenbaarheid (verminderde toerekenbaarheid of "accountability") in de weg staat.

5.3. Bestaande beginselen en verplichtingen onder de WVP die van toepassing zijn op DPI

38. De Commissie wees eerder[67] op de complementariteit tussen de WVP en de Wet van 13 juni 2005. Zij wenst hierna een aantal aantekeningen te maken bij bestaande plichten en bepalingen van de WVP die zij van bijzonder belang acht.

39. Elk verwerking via DPI dient gebaseerd te zijn op een van de gevallen vermeld in artikel 5 WVP[68].

40. Een eerste mogelijkheid is dat DPI wordt verricht in de context van politionele of gerechtelijke procedures[69], dit wil zeggen in toepassing van 5c) en 5 e) WVP.

41. Voor andere toepassingen van DPI door ISPs wordt hierna de mogelijkheid tot toepassing van artikel 5 a) WVP (toestemming), 5 b) WVP (overeenkomst met ISP) en 5f) WVP onderzocht.

42. Gelet op de potentiële belangenvermenging in hoofde van de afknijpende ISPs (zie hiervoor) bestaat het risico dat de telecommunicatieovereenkomsten (dus een beroep op

---

[65] http://www.zdnet.be/news/132291/telenet-teruggefloten-rond-p2p-vertraging/
[66] Zie http://www.p2p-next.org/?page=content&id=264A360A217FB3FE8BD82CB9C928CBCF&mid=6BED2EAC3D127503EF53456A25D9204E
[67] Zie advies 10/2012 van 21 maart 2012.
[68] De groep 29 stelde eerder in haar advies 01/2009. dat de rechtsgronden voor de verwerking van verkeersgegevens door openbaar beschikbare elektronische communicatiediensten en voor de verwerking van persoonsgegevens door de daarvoor verantwoordelijke zijn vervat in artikel 6 van de Richtlijn 2002/58/EG en artikel 7 en artikel 17 van de richtlijn over gegevensbescherming (omgezet door de artikelen 5 en 16 WVP)
[69] Zie artikel 90 Sv. en artikel 125 Wet van 13 juni 2005

artikel 5 b) WVP) met de betrokkenen of de "toestemming"[70] van de betrokkene (artikel 5 a) WVP) op zich genomen onvoldoende garanties bieden tot neutrale legitimering van DPI verwerkingen en teneinde te garanderen dat ISPs ook afdoende maatregelen nemen tot bescherming van de betrokkenen tegen het afknijpen van hun telecommunicatieverkeer en de verwerking van profielgegevens die verkregen zijn door DPI.

43. Er kunnen tenslotte diverse legitieme belangen bestaan om DPI in te roepen door ISPs (artikel 5 f) WVP), die de wetgever kan bepalen of die geen bijzondere bedenkingen oproepen in functie van de redelijke verwachtingen van de betrokkenen (zie de gevallen vermeld in de randnummers 25 tot en met 28.

44. Voor elke verwerking van persoonsgegevens dient elke **doelstelling** te worden gecommuniceerd. Deze doelstelling dient uitdrukkelijk omschreven en gerechtvaardigd te zijn (artikelen 4 § 1, 1° 4 § 1 2° en 9 § 1 WVP). Dit impliceert ook een verbod om DPI toe te passen zonder dat welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden voorhanden zijn (artikel 4 § 1, 2° WVP). De courant door ISPs gebruikte term "testen" en "netbeheer" zijn in dat opzicht veel te vaag (zie hiervoor onder randnummer 34)

45. Respect voor de **informatieplicht** door private actoren is essentieel, doch wordt vaak[71] verwaarloosd. De aanvullende informatieplicht onder het artikel 74 van het wetsontwerp[72] geldt onverminderd artikel 9 WVP. De ISPs dienen op hun websites dus rekening te houden met artikel 9 WVP[73]. Dienen te worden meegedeeld : de passende maatregelen die worden genomen om de rechten van de betrokkenen onder de WVP te respecteren, of er sprake is van medewerking van de ISP met een derde (bvb Phorm,…), en wat de concrete gevolgen zijn van de toepassing van DPI technologie.

46. DPI kan zoals elke analysetechniek ook leiden tot verkeerde, veralgemeende conclusies of de verwerking van **gevoelige persoonsgegevens** in de zin van de artikelen 6,7 of 8 WVP (bvb de betrokken gebruiker downloadt illegaal auteursrechtelijk beschermde werken,…).

47. **Geautomatiseerde maatregelen** (bvb afknijpen van alle P2P verkeer, pakketdifferentiatie, routing van IP-paketten en filtering) die verder gaan dan een redelijk

---

[70] Er is geen sprake van toestemming indien DPI uitmaakt van het beleid van de ISP. Dit staat ook los van de vraag of toestemming ("cookie consent") vereist is onder het gewijzigde artikel 5.3. van de Richtlijn 2002/58/EG. DPI betreft niet de opslag in eindapparatuur van de gebruiker of abonnee. De toenemende vraag naar netneutraliteit is zoals eerder vermeld de drijvende motivering om DPI ook reglementair aan banden te leggen.
[71] Zie randnummer 60 van het advies 10/2012 van 21 maart 2012
[72] Wetsontwerp houdende diverse bepalingen inzake elektronische communicatie
[73] Zie randnummer 102 en volgende van voormelde Canadese Richtlijn 2009-657

verkeersbeheer en **die voor de betrokkene rechtsgevolgen zou hebben**[74] of die de betrokkene in aanmerkelijke mate treffen[75] vallen onder het verbod in artikel 12bis WVP. De Commissie stelt vast dat geautomatiseerde afknijpverwerkingen beperkingen kunnen inhouden op het gebruik van legale, goedkopere en innovatieve diensten van derden (Whatsapp, Skype, Spotify…) die concurreren met de diensten van de ISPs. Eenzijdige maatregelen van ISPs (die ook mediadiensten aanbieden) kunnen de betrokkenen potentieel benadelen. Zo kan goedkoper gebruik van de P2P technologie aangeboden door concurrenten onmogelijk worden gemaakt (bvb voor diensten van muziek zoals Spotify[76], video op aanvraag of internetTV of andere toekomstige spelers in de Europese mediamarkt die P2P willen gebruiken als distributiemiddel). Dit nadeel is in het opzicht van artikel 12bis WVP niet irrelevant.

48. Hoewel de overeenkomst of de wet een grondslag kan omschrijven om geautomatiseerde beslissingen te ondersteunen, moet de overeenkomst of wetgever ook **passende maatregelen voorzien om de gerechtvaardigde belangen van de betrokkenen te beschermen** (zie artikel 12bis laatste lid WVP en aanbevelingen hierna). De Commissie acht de overeenkomst hiervoor minder geschikt (zie randnummer 41), en wijst er op dat netneutraliteit en het beiden van passende maatregelen vooral een zaak si van de wetgever of regulator.

49. DPI roept tenslotte vragen op in verband met **beveiligingsincidenten** bij ISPs, en het beleid aangaande het afhandelen van dataverkeer bij ISP's. Kan een werknemer van een ISP misbruik maken van de DPI technologie voor eigen gewin, bijvoorbeeld door het in kaart brengen van het applicatiegebruik van de bestaande klanten, zonder dat dit het beleid is van de ISP? Meer externe transparantie is nodig rond vragen wie onder welke voorwaarden dataverkeer kan blokkeren, of derden kunnen verzoeken om het afhandelen van internetverkeer anders te behandelen (bvb marketeers, werkgevers) aan een ISP betreffende een bepaalde websites (bvb vakvereniging[77], …).

---

[74] Bvb aanrekenen van extra kosten

[75] Bvb beperken van snelheid ("throttling") of blokkeren van (bepaalde types van) internetverkeer.

[76] Zo gebruikt de commerciële dienst Spotify tot 30 % P2P technologie. Zie 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 en http://www.csc.kth.se/~gkreitz/spotify-p2p11/kreitz-spotify-p2p11.pdf

[77] Dit voorbeeld blijkt uit een Canadese zaak van augustus 2005 waarbij een Canadese ISP (Telus) de toegang blokkeerde tot een website die was opgericht door een vakbond.

5.4. Aanbevelingen omtrent een duidelijkere wettelijke omkadering van en betere controle op DPI

50. Op basis van de opmerkingen in randnummers 37 tot en met 46 formuleert de Commissie derhalve hierna drie concrete aanbevelingen.

5.4.1. Aanbeveling 1 : definitie van "normaal netbeheer" (teneinde artikel 5 f) WVP te kunnen toepassen)

51. Voor zover het niet gaat om DPI in de context van politionele of gerechtelijke procedures[78] ziet de Commissie meer heil in het baseren van bepaalde toepassingen van DPI door ISP's op artikel 5 f) WVP voor wat de wetgever of de regulator als legale toepassing van DPI heeft erkend. Zij wijst op de legale toepassingen vermeld in randnummer 25 tot en met 28. De logica is onder meer dat de wetgever of het BIPT best kunnen bepalen wat moet worden verstaan onder het vage begrip "normaal netbeheer", met respect voor het beginsel van netneutraliteit en technologische neutraliteit ten aanzien van technieken zoals VOIP en P2P en de vereiste risicoinschatting. Het ware beter om een wetgevende of regulatoire tussenkomst te gebruiken die de meest neutrale basis vormt op basis waarvan de betrokkenen hun redelijke verwachtingen kunnen baseren (artikel 4 § 1, 2° WVP), in plaats van de notie van "normaal netbeheer" aan de arbitraire appreciatie van elke ISP over te laten in de overeenkomst met de ISP.

5.4.2. Aanbeveling 2 : genuanceerde, multidisciplinaire aanpak van DPI via vereiste voorafgaand privacyonderzoek, a posteriori controle, ...

52. Gelet op het evoluerende Europese gegevensbeschermingsrecht inzake profilering[79] zal de (Europese) wetgever en het BIPT een genuanceerde, multidisciplinaire aanpak dienen te ontwikkelen voor toepassing van DPI die met meer factoren rekening houdt dan een economische marktanalyse.

53. Gebruik van de techniek van DPI zal met andere woorden verder nauwgezet moeten worden opgevolgd door de diverse toezichthoudende instanties inzake gegevensbescherming (Groep 29), teneinde een privacybeoordeling ("privacy impact assessment") te kunnen maken naast de marktafweging die de Europese Commissie nog plant op basis van de studie van BEREC.

---

[78] Zie artikel 90 Sv. en artikel 125 Wet van 13 juni 2005

[79] Zie aanbeveling CM/Rec(2010)13 van 23 november 2010 van de Raad van Ministers over de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering, gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864
explanatory memorandum gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029&Site=CM

54. Voor de meest extreme vormen van DPI met directe rechtsgevolgen voor de betrokkenen, (bvb bij geautomatiseerde beslissingen zonder passende wettelijke waarborgen in de zin van artikel 12bis WVP of verwerking van gevoelige persoonsgegevens) moeten de bestaande verbodsbepalingen uit de WVP en de Richtlijn 95/46/EG worden toegepast.

55. Ook de Europese vereiste van voorafgaand onderzoek[80] (hoge risico's bij bepaalde toepassingen van DPI) en desgevallend controle a posteriori door de Commissie en/of het BIPT kunnen deel uitmaken van een meer genuanceerde en technologieneutrale aanpak van DPI. De grenzen van profileringsmogelijkheden, alternatieven / noodzaak van DPI en bewaringsbeleid van gegevens en begeleidende garanties bij profilering dienen te worden omschreven. De Commissie neemt zich voor om dit aspect verder op te volgen.

5.4.3. Aanbeveling 3 : verhoogde informatieplicht door aanvullende wijziging van de wet 13 juni 2005 bij gebruik van DPI

56. Artikel 74 van het wetsontwerp houdende diverse bepalingen inzake elektronische communicatie, wijzigt artikel 113 § 5 van de Wet van 13 juni 2005 door meer transparantie te voorzien[81] bij gebruik van "DPI" of netbeheer ten aanzien van het BIPT en de betrokkenen.

57. Gelet op de risico's verbonden aan het gebruik van de techniek van DPI acht de Commissie de toepassing van het nieuwe artikel 113 § 5 van de Wet van 13 juni 2005 onvoldoende. De wetgever dient een meer gericht toezicht op het gebruik van de techniek van DPI door ISPs te waarborgen.

---

[80] Artikel 20 Richtlijn 95/46/EG

[81] Deze nieuwe bepaling luidt als volgt : "1. De Lid-Staten geven aan welke verwerkingen mogelijk specifieke risico's voor de persoonlijke rechten en vrijheden inhouden en dragen er zorg voor dat zij voor de aanvang van de verwerking onderzocht worden.
2. Deze voorafgaande onderzoeken worden uitgevoerd door de toezichthoudende autoriteit na ontvangst van een aanmelding van de voor de verwerking verantwoordelijke, of door de functionaris voor de gegevensbescherming, die in twijfelgevallen de toezichthoudende autoriteit moet raadplegen.
3. De Lid-Staten kunnen een dergelijk onderzoek ook uitvoeren in het kader van de voorbereiding van een maatregel van het nationale parlement ofwel van een op een dergelijke wettelijke maatregel gebaseerde maatregel waarin de aard van de verwerking is omschreven en passende waarborgen zijn opgenomen."
"§ 5. Ondernemingen die openbare elektronische-communicatienetwerken aanbieden, alsook ondernemingen die openbare elektronische-communicatiediensten verstrekken leveren het Instituut informatie over door de aanbieder ingestelde procedures om het verkeer te meten en vorm te geven, om te voorkomen dat een netwerkaansluiting overzadigd of overbelast wordt.
Diezelfde ondernemingen publiceren op hun website informatie ten behoeve van de eindgebruikers over de wijze waarop deze procedures gevolgen kunnen hebben voor de kwaliteit van de dienstverlening. De informatie wordt voor publicatie eveneens aan het Instituut verstrekt .
Het Instituut beschikt over een termijn van een maand om zijn eventuele opmerkingen te formuleren. De ondernemingen mogen de informatie pas publiceren nadat rekening is gehouden met deze opmerkingen."

58. Op basis van de WVP kunnen de wetgever en/of het BIPT vandaag concretere waarborgen voorzien of aanmoedigen betreffende het gebruik van DPI, waaronder :

- het officieel oplijsten van de toepassingsvormen van DPI, en wanneer en voor welk type verkeer en doeleinden dit al dan niet kan worden toegepast met vooraf bepaalde modaliteiten (bewaring/opslag, initiatie intern of extern verzoek, ernst van de gevolgen voor de betrokkenen, transparantie, rechtsmiddelen en procedurele garanties…). Dit overzicht dient ruimer te zijn dan het juridisch of technisch bepalen van een juridische definitie of standaard voor netbeheer, door de concrete gebruiksdoelstelling te bepalen en de concrete risicograad voor de betrokkenen hierbij objectief en concreet vast te leggen (artikel 4 § 1, 2° WVP).
- per finaliteit waarvoor DPI wordt aangewend meer aandacht te geven voor proportionaliteitsbeginsel vooraleer de meest verregaande vormen van DPI (afknijpen, blokkeren, …) worden toegepast (artikel 4 § 1, 3° WVP). Dit wil zeggen meer uniformiteit brengen in de (te) ruime beslissingsmarge van ISPs over de vraag welke applicaties welke prioriteit dienen te krijgen[82], vooraleer de ISP kan beslissen om te blokkeren of af te knijpen. Ook het gebruik van geaggregeerde informatie voor netwerkplanning door ISPs kan worden aangehaald (de persoonsgegevens dienen afdoende te worden gecodeerd, waardoor het risico op commercieel hergebruik wordt vermeden)[83] (artikel 16 § 4 WVP);
- een specifieke informatieplicht voor ISPs dient te worden ingevoerd aangaande het al dan niet gebruik van DPI op een voor de doelgroep begrijpelijke wijze, die meer inhoudt dan de vermelding in het privacybeleid en/of algemene voorwaarden van de ISP's. ISPs zouden hun beleid inzake netbeheer met of zonder behulp van DPI[84] zeer duidelijk en openlijk als doelstelling voor de verwerking moeten communiceren naar alle betrokkenen toe (vnl. hun klanten en potentiële klanten). Dit bijvoorbeeld in de vorm van een FAQ, met uitleg rond de techniek van DPI aan de gebruikers. De specifieke informatieplicht kan een reglementaire basis onder de WVP krijgen via het voorzien van een Koninklijk besluit, genomen op basis van de huidige bewoording "bijkomende informatie" (door de Koning te bepalen na advies van de Commissie) in de zin van artikel 9 § 1 e) WVP.
- specifieke beveiligingsmaatregelen in te voeren inzake DPI (artikel 16 § 4 WVP). In navolging van andere markten zoals de elektriciteitsmarkt waar het netbeheer en de levering van diensten werden gesplitst, aan te moedigen dat een "third trusted party" eventueel benodigd neutraal afknijpingsverkeer evalueert, organiseert en coördineert. Dit

[82] Zie pagina 7 van voormelde white paper.
[83] Zie randnummer 105 van de Richtlijn 2009-657 van de Canadese Radio-televisie en Telecommunicatiecommissie, gepubliceerd op http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm
[84] Zie pagina 9 van voormelde white paper.

kan door het bepalen van technische standaarden voor netbeheer en opvolgende controle door BIPT (artikel 16 § 4 WVP)

- De toepassing van DPI door medewerkers van ISPs zou dienen te worden gelogd. (artikel 16 § 4 WVP).

De Commissie besluit :

Netneutraliteit

Het beginsel van netneutraliteit raakt aan de basisvraag wie onder welke voorwaarden en voor welke doeleinden controle kan uitoefenen op het verwerken van persoonsgegevens via publieke elektronische netwerken, en dient volgens Europa prioritair in de nationale wetgeving te worden omgezet, teneinde een betere bescherming van de betrokkenen te garanderen. De Commissie schaart zich voluit achter een dergelijke Europese vraag, bij voorkeur via wettelijke verankering van het beginsel van netneutraliteit in de Wet van 13 juni 2005, via de invoering van (onder meer) een definitie van het neutraliteitsbeginsel.

Tenslotte acht de Commissie het nuttig dat het debat wordt opgestart over de toepassing van het beginsel van netneutraliteit buiten de telecomsector, gelet op de toegenomen profileringsdrang in de elektriciteitssector die de gelijke behandeling van de betrokkenen en hun neutrale toegang tot basisdiensten kan beknotten via maatregelen zoals blokkeren, afknijpen, blacklisting of een ontransparante diversificatie van tariefformules of behandeling (eisen waarborg voor toegang tot basisdiensten)…

DPI

Het Europese gegevensbeschermingsrecht legt meer en meer[85] de nadruk op de noodzaak voor de wetgevers om voor de toepassingen met hoge risico's voor de betrokkenen en voor automatische toepassing van profielgebaseerde maatregelen passende beschermingsmaatregelen te voorzien . De Commissie wees in deze aanbeveling op hogere risico's die blijken uit bepaalde toepassingen van de techniek van DPI (bvb afknijpen van legaal P2P verkeer, gebruik voor direct marketing, mogelijke automatische beslissingsvormen gebaseerd op DPI met nadelige effecten voor betrokkenen,…).

De Commissie is voorstander voor een technologieneutrale aanpak van DPI. Niet het gebruik van de techniek van DPI op zich is problematisch. Echter, het niveau van toepassing, de mogelijke toepassingsvormen van DPI met hoger risico voor de betrokkenen vergen een regulering. Bij de

[85] via de voorafgaande onderzoeksplicht en de bescherming van het profileren van natuurlijke personen

toepassing van de techniek van DPI dient men het beginsel van netneutraliteit steeds te respecteren.

De Commissie is ook voorstander van een Europees multidisciplinair onderzoek van de diverse toepassingen van deze technologie. Dit wil zeggen dat de Groep 29 en de EDPS vroeg of laat ook een beoordeling zullen dienen toe te voegen aan de marktanalyse die de Europese Commissie zal verrichten aan de hand van de informatie die is verzameld via BEREC.

De Commissie wijst meteen ook op de verplichting om rekening te houden met de bestaande verbodsbepalingen en verplichtingen onder het Europese gegevensbeschermingsrecht en de WVP ingevolge de artikelen 4 § 1, 2°, 6 tem 8, 9, 12bis en 16 § 4 WVP. De Commissie roept de wetgever en/of het BIPT op om de betrokkenen nog beter te beschermen door een explicietere uitwerking van deze bestaande artikelen te geven voor elke toepassing van DPI. Dit in aanvulling van de bescherming via de bijkomende informatieplicht onder artikel 74 van het wetsontwerp houdende diverse bepalingen inzake elektronische communicatie.

De Commissie behoudt zich voor om op dat vlak de Europese discussies nauwgezet op te blijven volgen en indien nodig concretere aanbevelingen te formuleren ten aanzien van de wetgever en het BIPT, mocht op Europees vlak worden nagelaten om een Europese privacybeoordeling te verzoeken aan de Groep 29.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere