I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА ДАННИТЕ

Становище на Европейския надзорен орган по защита на данните относно неутралността на интернет, управлението на трафика и защитата на правото на неприкосновеност на личния живот и на личните данни

(2012/C 34/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 16 от него,

като взе предвид Хартата на основните права на Европейския съюз, и по-специално членове 7 и 8 от нея,

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([1]),

като взе предвид Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни ([2]), и по-специално член 41, параграф 2 от него,

като взе предвид Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации ([3]),

ПРИЕ НАСТОЯЩОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

I.1. Общи положения

1. На 19 април 2011 г. Комисията прие Съобщение относно отвореното и неутрално интернет пространство в Европа ([4]).

2. Настоящото становище може да се разглежда като реакция на ЕНОЗД по отношение на това съобщение и има за цел да даде своя принос към текущия политически дебат в рамките на ЕС относно неутралния характер на интернет, особено относно аспекти, свързани със защитата на личните данни и неприкосновеността на личния живот.

([1]) ОВ L 281, 23.11.95 г., стр. 31, „Директива за защита на личните данни“.
([2]) ОВ L 8, 12.1.2001 г., стр. 1, „Регламент за защита на личните данни“.
([3]) ОВ L 201, 31.7.2002 г., стр. 37, изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. (виж бележка под линия 15), „Директива за правото на неприкосновеност на личния живот и електронни комуникации“.
([4]) COM(2011) 222 окончателен.

3. Становището се основава на отговора ([5]) на ЕНОЗД по отношение на обществената консултация, проведена от Комисията относно отвореното и неутрално интернет пространство в Европа, което предхожда съобщението на Комисията. ЕНОЗД също така разгледа неотдавнашния проект за заключения на Съвета относно неутралния характер на интернет ([6]).

I.2. **Концепцията за неутралния характер на интернет**

4. Неутралността на интернет се позовава на текущ дебат относно това дали на доставчиците на интернет услуги (ISPs ([7])) следва да им бъде разрешено да ограничават, филтрират или блокират достъпа до интернет или да оказват по друг начин влияние върху функционирането му. Концепцията за неутралния характер на интернет се основава на становището, че информацията в интернет следва да се предава безпристрастно без оглед на съдържанието, посоката или източника и че потребителите следва да могат да решават какви приложения, услуги и хардуер искат да използват. Това означава, че доставчиците на интернет услуги не могат по техен собствен избор да дават приоритет на или да забавят достъпа до определени приложения или услуги, като например равноправен достъп (P2P), и т.н. ([8])

5. Филтрирането, блокирането и проверката на трафика в мрежата поражда важни въпроси, които често са пренебрегвани или оставяни за последващо разглеждане, относно поверителността на съобщенията и зачитането на неприкосновеността на личния живот на физическите лица и техните лични данни, когато използват интернет. Например определени техники за проверка, които включват наблюдение на съдържанието на съобщения, посетени уебсайтове, изпратени и получени електронни писма, времето, когато това се извършва, и т.н., позволяват филтриране на съобщенията.

6. Като проверяват съобщителните данни, доставчиците на интернет услуги могат да нарушат поверителността на съобщенията, което е основно право, гарантирано от член 8 на Европейската конвенция за защита на правата на човека и основните свободи („ЕКЗПЧ“) и членове 7 и 8 от Хартата на основните права на Европейския съюз („Хартата“). Поверителността е защитена допълнително и във вторичното законодателство на ЕС, а именно член 5 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

I.3. **Акцент и структура на становището**

7. ЕНОЗД счита, че към поверителността на съобщенията, както и някои други последици върху неприкосновеността на личния живот и защитата на данните, трябва да бъде насочен сериозен политически дебат относно неутралния характер на интернет.

8. Настоящото становище допринася за текущия дебат в ЕС и неговата цел е тристепенна:

— То насочва вниманието към значението на неприкосновеността на личния живот и защитата на данните в текущите дискусии относно неутралния характер на интернет. По-специално в него се подчертава необходимостта да се спазват съществуващите правила относно поверителността на съобщенията. Следва да бъдат позволени единствено практики, при които се спазват тези правила.

— Неутралността на интернет е свързана със сравнително нови технологични възможности и опитът, относно прилагането на правната рамка, не е голям. Следователно настоящото становище предоставя насоки за това как доставчиците на интернет услуги трябва да прилагат и спазват правната рамка за защита на данните, ако участват във филтриране, блокиране и проверка на трафика в мрежата. Това би следвало да бъде от полза за доставчиците на интернет услуги, както и за органите, отговарящи за прилагането на рамката.

— В рамките на обхвата на защитата на данните и неприкосновеността на личния живот в становището се определят области, които изискват специално внимание и които могат да изискват действия на равнище ЕС. Това е от особено значение с оглед на текущия дебат на равнище ЕС и политическите мерки, които могат да бъдат предприети от Комисията в този контекст.

([5]) В отговора си ЕНОЗД подчертава колко е важно да се вземат под внимание въпроси, свързани със защитата на данните и неприкосновеността на личния живот, заедно с други съществуващи права и ценности. Отговорът е наличен на адрес: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Налично на адрес http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Това включва предоставянето както на фиксиран, така и на мобилен достъп до интернет.

([8]) Въпреки че не се прилага принципът за доставчици на интернет услуги, които поставят ограничения върху скоростта или количеството информация, абонатът е в състояние да изпраща или получава информация чрез абонаменти с честотна лента или ограничения на обема. Следователно съгласно принципа за неутралност на интернет доставчиците на интернет услуги все още могат да предлагат абонамент за достъп, ограничавайки достъпа, основан на критерии като скорост или обем, дотолкова, че да е необходима дискриминация в полза на или срещу определено съдържание.

9. ЕНОЗД е наясно, че неутралността на интернет поражда други въпроси, описани по-долу, като тези, свързани с достъпа до информация. Тези въпроси се разглеждат само до степента, до която са свързани със или оказват въздействие върху защитата на данните и неприкосновеността на личния живот.

10. Становището е структурирано по следния начин. Раздел II започва с представяне на кратък преглед на практиките за филтриране от доставчиците на интернет услуги. В раздел III се очертава законодателната рамка на ЕС относно неутралния характер на интернет. Раздел IV продължава с техническо описание, последвано от оценка на последиците върху неприкосновеността на личния живот, в зависимост от използваната техника. В раздел V се анализират практическите детайли по отношение на прилагането на текущата рамка на ЕС за правото на неприкосновеност на личния живот и защитата на данните. Като се основава на анализа, раздел VI съдържа предложения за по-нататъшно развитие на политиката и в него се определят областите, в които може да е необходимо изясняване и подобряване на правната рамка. Раздел VII съдържа заключенията.

II. **НЕУТРАЛНОСТ НА ИНТЕРНЕТ И ПОЛИТИКИ ЗА УПРАВЛЕНИЕ НА ТРАФИКА**

Все по-често прилагане на политиките за управление на трафика

11. Традиционно доставчиците на интернет услуги участват в наблюдение и оказване на влияние върху трафика в мрежата само при ограничени обстоятелства. Например доставчици на интернет услуги са прилагали техники за проверка и са ограничавали информационни потоци с цел да се запази сигурността на мрежата, напр. за борба с вируси. Следователно, най-общо казано, интернет се е разраснал, като същевременно е запазил голяма степен на неутралност.

12. През последните години обаче,някои доставчици на интернет услуги проявяват интерес към проверката на трафика в мрежата с цел да се разграничат и да се прилагат различни политики, свързани с него, като например да се блокират специфични услуги или да се даде предимство на достъпа до други. Това понякога се нарича „политики за управление на трафика“ ([9]).

13. Причините доставчиците на интернет услуги да проверяват и диференцират трафика са многобройни. Политиките за управление на трафика например могат да помогнат на доставчиците на интернет услуги да управляват трафика в периоди на голямо претоварване посредством даване на приоритет на определен трафик, който е чувствителен спрямо фактора време, например при предаване на видеоизображение в реално време и посредством понижаване на други видове трафик, които са по-малко чувствителни спрямо фактора време, например равноправният достъп (P2P) ([10]). Освен това управлението на трафика може да бъде средство за доставчиците на интернет услуги да получат възможен приходен поток, който би могъл да произхожда от различни източници. От друга страна доставчиците на интернет услуги могат да събират такси от доставчиците на услуги, като например тези, чийто услуги изискват използването на по-голяма широчина на лентата, като в замяна им дават приоритет (а по този начин и скорост). Това би означавало, че достъпът до някои услуги, например услуги за предоставяне на видео по заявка, ще бъде по-бърз, отколкото достъпът до друга, подобна услуга, за която не е договорена по-висока скорост на предаване. Приходи могат да бъдат получени и от абонати, интересуващи се от това да плащат по-високи (или по-ниски) такси за определени видове диференцирани абонаменти. Например абонамент без достъп до P2P би могъл да бъде по-евтин, отколкото такъв, който дава право на неограничен достъп.

14. В допълнение към личните причини на доставчиците на интернет услуги за прилагането на политиките за управление на трафика е възможно и други страни да имат интерес от прилагането на политиките за управление на трафика от доставчиците на интернет услуги. Ако доставчиците на интернет услуги управляват техните мрежи и участват в проверката на съдържанието, което преминава през тяхното оборудване, е много вероятно те да увеличат капацитета си за засичане на предполагаема неправомерна употреба, напр. нарушаване на авторски права или използване с порнографска цел.

([9]) Виж например доклад на OFCOM, озаглавен „Блокиране на сайтове за намаляване на онлайн нарушаването на авторските права“, приет на 27 май 2011 г. и наличен на адрес: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Някои доставчици на интернет услуги вече внедряват системи за проверка на пакетите с интернет данни в тяхната мрежа, за управление на трафика и други цели, така че ние приемаме, че могат да бъдат внедрени, въпреки че това би било свързано с висока степен на сложност и разходи, за тези които все още не използват такива услуги. Може да се каже, че предвид необходимите капиталови инвестиции в краткосрочен до средносрочен план задълбочената проверка на пакетите с интернет данни може да бъде използвана единствено от по-големите доставчици на интернет услуги“.

([10]) Качеството на приложенията в реално време, като предаване на видеоизображение, освен всичко друго зависи и от латентността, т.е. забавяне например в резултат на претоварване на мрежата.

Други засегнати интереси, включително защита на данните и неприкосновеност на личния живот

15. Тази тенденция предизвика дискусия относно законността на този вид практики и по-специално за това дали определени задължения по отношение на неутралния характер на интернет следва да бъдат доразвити от законодателството.

16. Възможно е повишеното прилагане на политиките за управление на трафика от доставчиците на интернет услуги да ограничи достъпа до информация. Ако това поведение стане обичайна практика и потребителите не разполагат с познатия цялостен достъп (или е твърде скъп) до интернет, това би застрашило достъпа до информация и способността на потребителите да изпращат и получават съдържанието, което искат, като използват приложенията или услугите, избрани от тях. Този проблем може да бъде избегнат чрез правно задължителен принцип относно неутралността на интернет.

17. Това насочва ЕНОЗД към последиците върху защитата на данните и неприкосновеността на личния живот при участие на доставчиците на интернет услуги в управлението на трафика. По-специално:

— Когато доставчиците на интернет услуги обработват данни за трафика с единствена цел да насочат информационния поток от изпращача към получателя, те обикновено извършват ограничена обработка на лични данни ([11]). По същия начин както пощенските служби обработват информацията, която се намира върху плика на писмото, така и доставчиците на интернет услуги обработват информацията, която е необходима, за да се насочи съобщението към получателя. Това не противоречи на правните изисквания за защитата на данните, неприкосновеността на личния живот и поверителността на съобщенията.

— Когато обаче доставчиците на интернет услуги проверяват съобщителните данни с оглед на диференцирането на всеки информационен поток и прилагането на специфични политики, които могат да бъдат неблагоприятни за лицата, последиците са по-значими. В зависимост от обстоятелствата при всеки отделен случай и от вида на извършения анали, обработката може да предизвика сериозна загриженост относно неприкосновеността на личния живот и личните данни на физическите лица. Това става по-ясно, когато политиките за управление разкриват съдържанието на интернет съобщенията на физическите лица, включително изпратени и получени електронни писма, посетени уебсайтове, изтеглени или качени файлове и т.н.

III. **ПРЕГЛЕД НА ПРАВНАТА РАМКА НА ЕС ОТНОСНО НЕУТРАЛНИЯ ХАРАКТЕР НА ИНТЕРНЕТ И БЪДЕЩОТО РАЗВИТИЕ НА ПОЛИТИКАТА**

III.1. **Правната рамка накратко**

18. До 2009 г. законодателните инструменти на ЕС не съдържаха разпоредби, които изрично да забраняват на доставчиците на интернет услуги да участват във филтриране, блокиране или начисляване на допълнителни разходи на абонатите за достъп до услугите. В същото време тези инструменти не съдържаха разпоредби, които изрично да признават тази практика. До известна степен това беше ситуация на несигурност.

19. Пакетът за далекосъобщенията от 2009 г. промени това, като включи разпоредби в полза на отворения характер на интернет. Например член 8, параграф 4 относно общата регулаторна рамка за електронните съобщителни мрежи и услуги („Рамкова директива“) установява задължение за регулаторните органи да насърчават възможността крайните ползватели да имат достъп до съдържание, приложения или услуги по техен избор ([12]). Тази разпоредба се прилага към мрежата като цяло, а не на равнище отделни доставчици. В неотдавнашния проект за заключения на Съвета също беше подчертана необходимостта от запазване на отворения характер на интернет ([13]).

([11]) Това изключва операции, насочени към повишаване на сигурността на мрежата и засичане на вреден трафик, а също и операции необходими за изготвяне на абонатни сметки и взаимно свързване. Това също така изключва задължения, произтичащи от директивата за запазване на данни, Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 13.4.2006 г., стр. 54). („Директива за запазване на данните“).

([12]) Директива 2002/21/ЕО от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги, изменена с Директива 2009/140/ЕО и Регламент (ЕО) № 544/2009 (ОВ L 337, 18.12.2009 г., стр. 37).

([13]) Вж. точка 3, буква д), в която Съветът признава: „Необходимостта от поддържане на отворения характер на интернет, като се гарантира, че той ще продължи да осигурява висококачествени услуги в рамка, при която се насърчават и спазват основни права като свободата на словото и на стопанската инициатива“ и точка 8, буква г), в която държавите-членки се приканват да „поддържат отворения и неутрален характер на интернет като цел на своята политика“.

20. Директивата за универсалната услуга ([14]) съдържа повече конкретни задължения. В членове 20 и 21 се определят изискванията за прозрачност по отношение на ограниченията на достъпа до и/или използването на услуги и приложения. С нея също така се изискват минимални нива на качеството на услугата.

21. В съображение 28 от директивата за изменение на Директивата за универсалната услуга и Директивата за правото на неприкосновеност на личния живот и електронни комуникации ([15]), по отношение на практики на доставчиците на интернет услуги, водещи до проверка на съобщенията на физическите лица, се подчертава, че „в зависимост от използваната технология и вида ограничение такова ограничение може да изисква съгласие на ползвателя съгласно Директивата за правото на неприкосновеност на личния живот и електронни комуникации“. Така в съображение 28 се напомня за необходимостта от съгласие в съответствие с член 5, параграф 1 от Директива за правото на неприкосновеност на личния живот и електронни комуникации за всяко ограничение, основаващо се на контрол върху общуването в интернет. В раздел IV по-долу допълнително се анализира прилагането на член 5, параграф 1 и цялостната правна рамка за защита на данните и правото на неприкосновеност на личния живот.

22. В заключение, член 22, параграф 3 от Директивата за универсалната услуга понастоящем дава право на националните регулаторни органи да налагат на доставчиците на интернет услуги, ако е необходимо, минимални изисквания за качеството на услугите, с цел да се предотврати влошаването на услугите и затрудняването или забавянето на трафика в обществените мрежи.

23. Горепосоченото означава, че на равнище ЕС има широк интерес към отворен интернет (виж член 8, параграф 4 от Рамковата директива). Тази цел на политика, която се прилага към мрежата като цяло обаче не е пряко свързана със забрани или задължения на индивидуални доставчици на интернет услуги. С други думи доставчик на интернет услуги може да участва в политики за управление на трафика, с които може да се забранява достъп до определени приложения, при условия че крайните потребители са надлежно информирани и са изразили свободно, конкретно и недвусмислено своето съгласие.

24. Тази ситуация може да бъде различна в зависимост от държавите-членки. В някои държави-членки доставчиците на интернет услуги могат да участват при определени условия в политики за управление на трафика, например за да блокират приложения като VoIP (като част от по-евтин абонамент за интернет), при условие че лицата са дали своето свободно изразено, конкретно и недвусмислено информирано съгласие. Други държави-членки са избрали да утвърдят принципа на неутралност на интернет. Например през юли 2011 г. Нидерландският парламент прие закон, с който общо се забранява на доставчиците да затрудняват или забавят приложения или услуги по интернет (като например VoIP), освен ако това не е необходимо, за да се сведат до минимум последиците от претоварване, по причини, свързани с целостта и сигурността, за борба срещу нежеланите съобщения или съгласно съдебно нареждане ([16]).

III.2. **Съобщение относно неутралния характер на интернет**

25. В съобщението относно неутралния характер на интернет ([17]) Европейската комисия заключи, че ситуацията по отношение на неутралността на интернет изисква наблюдение и допълнителен анализ. Нейната политика беше наречена „политика на изчакване“ преди да бъдат обмислени допълнителни регулаторни стъпки.

([14]) Директива 2002/22/ЕО, както е изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г., която изменя Директива 2002/22/ЕС относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите. (ОВ L 337, 18.12.2009 г., стр. 11). Срв. също член 1, параграф 3, който гласи, че с директивата нито се вменява задължение за условия, нито се забраняват условия, които да бъдат поставяни от доставчиците на интернет услуги за ограничаване на достъпа на крайните ползватели до и/или ползването на услуги и приложения, когато това е разрешено съгласно националното законодателство и в съответствие със законодателството на Общността, но от тях се изисква да предоставят информация за такива условия.

([15]) Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите.

([16]) Оригиналът на нидерландското изменение може да бъде намерен на адрес: https://zoek.officielebekendmakingen.nl/kst-32549-A.html Причините представени от пресата за такъв вариант на политика, не се отнасят до съображения, свързани със защитата на данните и неприкосновеността на личния живот, а по скоро до причини, свързани с това да се гарантира, че потребителите не са лишени от или не им се предлага ограничен достъп до информация. Изглежда че въпросите, свързани с достъпа до информация, са мотивите за това изменение.

([17]) Виж бележка под линия на стр. 4.

26. В съобщението на Комисията се признава, че всички мерки и допълнителни регулаторни стъпки ще бъдат обект на по-задълбочена оценка във връзка с аспектите, свързани със защитата на данните и неприкосновеността на личния живот. В проекта за заключения на Съвета също бяха отчетени належащите въпроси относно защитата на данните и неприкосновеността на личния живот ([18]).

27. Въпросът, на който трябва да бъде направена оценка с оглед на защитата на данните и неприкосновеността на личния живот е дали политиката на изчакване е достатъчна. Въпреки че в рамката за защитата на данните и неприкосновеността на личния живот за момента се предвиждат някои предпазни мерки, особено чрез принципа на поверителност на съобщенията, явно е необходимо да се наблюдава отблизо нивото на съответствие и публикуване на насоки относно няколко аспекта, които не са съвсем ясни. Освен това някои идеи трябва да бъдат доразвити, например тази как рамката може да бъде изяснена и допълнително подобрена с оглед на технологичните разработки. Ако наблюдението показва, че пазарът се развива към масивна, протичаща в реално време проверка на съобщения и поражда въпроси, свързани със съответствието с рамката, ще са необходими правни мерки. Конкретни предложения относно това ще бъдат направени в раздел VI.

IV. **ТЕХНИЧЕСКА ИНФОРМАЦИЯ И ПОСЛЕДИЦИ, СВЪРЗАНИ С НЕПРИКОСНОВЕНОСТТА НА ЛИЧНИЯ ЖИВОТ И ЗАЩИТАТА НА ДАННИТЕ**

28. Преди да се навлезе по-дълбоко в темата е важно да е наличен по-добър поглед върху техниките за проверка, които доставчиците на интернет услуги могат да използват, за да участват в управлението на трафика, и как това би повлияло върху принципа на неутралност на интернет. Последиците върху неприкосновеността на личния живот и защитата на данните от такива техники се различават значително в зависимост от това коя/кои техника/и е или са използвани. Техническата информация е необходима, за да се разбере и прилага правилно правната рамка относно защитата на данните, описана в раздел V. Все пак следва да се отбележи, че това е постоянно променяща се и сложна област. Следователно описанието по-долу няма за цел да е изчерпателно и напълно актуализирано, а само да предостави техническата информация, която е крайно необходима за разбирането на правните съображения.

IV.1. **Предаване на информация чрез интернет: основите**

29. Когато потребител предава съобщение чрез интернет, предаваната информация се разделя на пакети. Тези пакети се предават по интернет от изпращача до получателя. Всеки пакет ще включва наред с други неща и информация за източника и посоката. Освен това доставчиците на интернет услуги могат да включат тези пакети в допълнителни слоеве и протоколи ([19]), които ще бъдат използвани за управлението на различни потоци от трафик в рамките на мрежата на доставчика на интернет услуги.

30. Да се върнем пак към аналогията с пощенското писмо, използването на протокол за мрежови пренос е равносилно на поставянето на съдържанието на пощенско писмо в плик, с адрес на получателя, който трябва да се прочете от пощенските служби, след което те да го доставят. Пощенските служби могат да използват допълнителни протоколи в своите вътрешни транзити за управление на всички пликове, които трябва да бъдат предадени, като целта е всеки плик да достигне получателя, написан първоначално от изпращача. Като се използва тази аналогия, всеки пакет е съставен от две части, *полезен товар на IP пакета* който включва съдържанието на съобщението и ще бъде еквивалент на писмото. Той съдържа информация, предназначена единствено за получателя. Втората част от пакета е *заглавната част на IP пакета*, която включва наред с други неща и адреса на получателя и изпращача, и ще бъде еквивалент на плика. Заглавната част на IP пакета позволява доставчиците на интернет услуги и други посредници да насочват полезния товар от адреса на източника към адреса на получателя.

31. Доставчиците на интернет услуги и други посредници гарантират, че IP пакетите пътуват по мрежата чрез възли, които разчитат информацията от заглавната част на IP пакета, сравняват я с маршрутните таблици, след което ги препращат към следващия възел по пътя към получателя. Този процес се извършва в

([18]) Виж точка 4, буква д) в която Съветът отбелязва: „Съществуването на някои опасения, изразени главно от потребителите и органите за защита на данните, по отношение на защитата на личните данни“.

([19]) Както е описано в раздел IV.2, такива протоколи кодират информацията, която се предава изцяло по съгласуван начин, така че лицата, участващи в съобщаването, да могат да се разбират помежду си, например HTTP, FTP и т.н.

рамките на мрежата, като се използва подходът „максимални усилия за по-малко памет“, тъй като всички пакети, които пристигат към даден възел, се обработват по един и същи начин. След като бъдат препратени към следващия възел, не е необходимо в рутера да се запазва по-нататъшна информация ([20]).

IV.2. **Техники за провеждане на проверка**

32. Както става ясно от горепосоченото, доставчиците на интернет услуги „прочитат“ заглавните части на IP пакетите с цел да ги насочат към потребителя. Въпреки това, както е посочено по-горе, анализът на трафика (включително заглавните части на IP пакетите и полезния товар на IP пакетите) може да бъде извършен за други цели и с други видове технологии. Новите тенденции например могат да включват забавяне на някои приложения, използвани от потребителите, като например P2P, или като алтернатива — увеличаване на скоростта на трафика за някои услуги, като например видео по заявка за привилегировани абонати. Въпреки че посредством всички техники за провеждане на проверка *технически* се извършва проверка на пакетите с интернет данни, те включват различни нива на намеса Има две основни категории техники за провеждане на проверка. Едната се основава единствено на заглавната част на IP пакета, другата също и върху полезния товар на IP пакета.

Основана на информация за заглавната част на IP пакета. Проверката на заглавната част на IP пакета разкрива някои области, които могат да позволят на доставчиците на интернет услуги да прилагат редица специфични политики за управление на трафика. С тези техники, които се основават единствено на проверката на заглавната част на IP пакетите, по принцип се обработват данни, които са предназначени за информация за посоката, за различни цели (т.е. диференциране на трафика). Поглеждайки IP адреса на източника, доставчикът на интернет услуги може да го свърже с конкретен абонат и да приложи някои специфични политики, например насочване на пакета през по-бърза или по-бавна връзка. Поглеждайки IP адреса на получателя, доставчикът на интернет услуги също може да приложи специфични политики, например блокиране или филтриране на достъпа до определени уебсайтове.

Основана на по-задълбочена проверка. Задълбочената проверка на пакетите с интернет данни позволява на доставчиците на интернет услуги да имат достъп до информация, адресирана единствено до получателя на съобщението. Ако се върнем отново към примера с пощенските услуги, този подход е еквивалентен на отваряне на плика и прочитане на съдържанието на писмото, за да се извърши анализ на съдържанието на съобщението (включено в IP пакетите), с цел да се приложи специфична мрежова политика. Има различни начини за извършване на проверката, всеки от тях поражда различни заплахи за субектите на данни.

— *Задълбочена проверка на пакетите с интернет данни, основана на анализ на протоколи и статистически записи*. В допълнение към IP протокола, чиято цел е да направи възможно предаването на данни по интернет, има допълнителни протоколи, които кодират информацията, която се предава по съгласуван начин (транспорт, сесия, представяне и приложение и т.н). Целта на тези протоколи е да гарантират, че лицата, участващи в съобщаването, могат да се разбират помежду си. Например има някои протоколи, които са свързани с уеб-браузинг ([21]), други са за прехвърляне на файлове ([22]) и т.н. Следователно техниките за провеждане на проверка, основани на проверка на протоколи и комбинирани със статистически анализ, целят откриване на конкретни модели или отпечатъци, които определят кои протоколи са налице ([23]). Тези техники за провеждане на инспекции позволяват на доставчиците на интернет услуги да разбират вида на съобщението (електронна поща, уеб-браузинг, качване на файлове) и в някои случаи да определят използваната услуга или приложение, както в случая с VoIP съобщенията, където използваните протоколи са много специфични за определен доставчик или доставчик на услуги. Самото познаване на вида на съобщението може да позволи на доставчиците на интернет услуги да прилагат съответните политики за управление на трафика, например да блокират уеб трафика. Това може да бъде и първата стъпка за позволяване на доставчиците на интернет услуги да извършват допълнителни анализи, които могат да изискват пълен достъп до метаданните и съдържанието на съобщението.

([20]) Независимо от това в мрежовото оборудване за интернет се използват протоколи за маршрутизация, които ще регистрират дейност, ще обработват статистика за трафика и ще обменят информация с друго мрежово оборудване, за да насочват IP пакетите, като използват най-ефективния маршрут. Например когато една връзка е претоварена или разрушена и рутерът получава тази информация, той ще актуализира своята маршрутна таблица с алтернативен вариант, който не използва тази връзка. Заслужава да се отбележи и събирането и обработването, което в някои случаи може да се извърши за целите на фактурирането или дори в съответствие с изискванията на Директивата за запазване на данните.

([21]) HTTP — Протокол за прехвърляне на хипертекст — или HTML — Език за маркиране на хипертекст.

([22]) FTP — Протокол за прехвърляне на файлове.

([23]) Има различни начини за определяне на използваните протоколи. Възможно е например, за да се определят портовете, използвани за създаване на съобщението, да се търси в специфични области във вътрешни протоколи. Статистическата характеристика на информационния поток също може да бъде загатната от анализа на някои от специфичните полета, корелация на протоколите, използвани едновременно между два IP адреса.

— *Задълбочена проверка на пакетите с интернет данни, основана на анализ на съдържанието на съобщението*. В заключение е възможно да се извърши проверка на метаданните ([24]) и на самото съдържание на съобщението. Тази техника се състои в прихващане на всички IP пакети, които са част от първоначалния информационен поток, така че оригиналното съдържание на съобщението да може да бъде възстановено напълно и да бъде анализирано. Така например за откриване на вредно или незаконно съдържание като вируси, детска порнография и т.н. е необходимо да се възстанови самото съобщение, за да може да бъде анализирано. Трябва да се отбележи, че понякога заинтересованите лица могат да кодират изцяло съобщението и тази практика ще затрудни доставчиците на интернет услуги да извършат анализ на съдържанието на съобщението.

IV.3. **Последици върху неприкосновеността на личния живот и защитата на данните**

33. Техниките за провеждане на проверка, основаващи се на заглавните части на IP пакетите и по-специално тези, базирани на проверката на пакетите с интернет данни, включват наблюдение и филтриране на тези данни и водят до значителни последици по отношение на неприкосновеността на личния живот и защитата на данните. Те също могат да бъдат в противоречие с правото на поверителност на съобщенията

34. Внимателното разглеждане на съобщенията на физическите лица само по себе си има сериозни последици върху неприкосновеността на личния живот и защитата на данните. И все пак проблемът е по-всеобхватен, тъй като в зависимост от целите, преследвани с наблюдението и прихващането на съобщенията, последиците върху неприкосновеността на личния живот могат да бъдат още по-големи. Например има разлика в това просто да се направи проверка на съобщенията и да се гарантира, че системата работи добре, и в това да се извършва проверка на съобщенията, за да се прилагат политики, които биха оказали влияние върху физическите лица. Когато с политиките в областта на трафика и избора може да се цели единствено избягване на претоварването на мрежата, тогава обикновено няма големи последици върху неприкосновеността на личния живот на физическите лица. С политиките за управление на трафика обаче може да се цели блокиране на някакво информационно съдържание или да оказване на влияние върху съобщенията, например чрез поведенческа реклама. В тези случаи последиците са по-сериозни. Безпокойството се увеличава, ако човек осъзнае, че този тип информация се събира не за малки групи от хора, а по-скоро за всички клиенти на доставчиците на интернет услуги въз основа на една обща база ([25]). Ако всички доставчици на интернет услуги възприемат техниките за филтриране, това би довело до едно всеобщо наблюдение на използването на интернет. Освен това, ако вниманието бъде съсредоточено си върху вида на обработваната информация, е очевидно, че рисковете за неприкосновеността на личния живот са големи, тъй като голяма част от събраната информация е вероятно да е много чувствителна и след събирането ще е достъпна за доставчиците на интернет услуги и за тези, които търсят информация от тях. Освен това информацията може да бъде и много ценна в търговско отношение. Само по себе си това създава висок риск от изместване на функции, когато първоначалните цели лесно могат да се развият в търговски или други форми на експлоатация на събраната информация.

35. Правилното прилагане на техниките за наблюдение, проверка и филтриране трябва да се извършва в съответствие с приложимите предпазни мерки за защита на данните и неприкосновеността на личния живот, които установяват границите за това какво може да се направи и при какви обстоятелства. Следва преглед на приложимите предпазни мерки съгласно текущата правна рамка на ЕС за защита на данните и неприкосновеност на личния живот.

V. **ПРИЛАГАНЕ НА ПРАВНАТА РАМКА НА ЕС ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЗАЩИТА НА ДАННИТЕ**

36. Рамката на ЕС за защита на данните е технологично неутрална; поради това ѝ качество за нея не се регулират специфични техники за провеждане на проверка като горепосочените. С Директивата за правото на неприкосновеност на личния живот и електронни комуникации се регулират неприкосновеността на личния живот при предоставянето на електронни съобщителни услуги в обществените мрежи

([24]) Всеки протокол има някои специфични области в заглавната си част, които предоставят допълнителна неофициална информация за предаденото съобщение. Следователно съдържанието на тези области може да се приема за метаданните на съобщението. Пример за тези области може да бъде номера на използвания порт, който, ако е 80, е много вероятно видът на съобщението да е уеб-браузинг.

([25]) Разбира се възможностите за проследяване не са присъщи единствено за доставчиците на интернет. Мрежови доставчици на реклами също имат такава възможност чрез използване на бисквитките на трети страни за проследяване на потребители в уебсайтове. Виж например последните академични статии, които показват, че Google присъства на 97 от 100-те най-добри уебсайта, което означава, че Google може да проследява потребители, които не са избрали бисквитките на трети страни, докато са разглеждали тези популярни уебсайтове. Вж.: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan и Hoofnagle, Chris Jay, Флаш бисквитки и Неприкосновеност на личния живот II: Сега с HTML5 и ETag Respawning (29 юли 2011 г.) (Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning). Налична на адрес SSRN: http://ssrn.com/abstract=1898390. Проследяването на потребители чрез бисквитките на трети страни е разгледано от Работната група по член 29. Вж. становище 2/2010 относно поведенческите реклами онлайн, прието на 22 юни 2010 г. (WP 171).

(обикновено достъп до интернет и телефония) ([26]), а с Директивата за защита на личните данни се регулира обработката на данни като цяло. Разгледана общо, в тази правна рамка се определят различни задължения, приложими за доставчиците на интернет услуги, които обработват и наблюдават трафика и съобщителните данни.

V.1. **Правни основания за обработка на данни за трафика и за съдържанието**

37. Съгласно законодателството за защита на данните обработката на лични данни, например в този случай обработката на данни за трафика и съобщителни данни, изисква подходящо правно основание. В допълнение към това общо изискване в някои случаи могат да се прилагат специфични изисквания.

38. В конкретния случай видът на личните данни, обработвани от доставчиците на интернет услуги, се отнася до данните за трафика и съдържанието на съобщенията. И съдържанието на съобщенията, и данните за трафика са защитени от правото на поверителност на съобщенията, което е гарантирано от член 8 от ЕКПЧ и членове 7 и 8 от Хартата. По-специално в член 5, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, озаглавен „конфиденциалност на комуникациите“ се изисква държавите-членки да гарантират конфиденциалност на съобщенията и свързания трафик на данни през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги. В същото време член 5, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда, че обработката на данни за трафика и съдържанието от доставчиците на интернет услуги, може да бъде позволена при определени условия със съгласието на потребителите. Това е направено чрез определяне на забрана за „слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители, без съгласието на заинтересованите потребители, с изключение на законно упълномощени да извършват това в съответствие с член 15, параграф 1“. Тази теза е доразвита по-долу.

39. В допълнение към съгласието на заинтересованите потребители Директивата за правото на неприкосновеност на личния живот и електронни комуникации предвижда други основания, които могат да легитимират обработката на данни за трафика и съобщителни данни от доставчиците на интернет услуги. Съответните правни основания за обработката в този случай са: i) предоставяне на услугата; ii) гарантиране на сигурността на услугата, и iii) свеждане до минимум на претоварването. Други възможни правни основания за легитимиране на политиките за управление, основаващи се на данни за трафика или съобщителни данни са разгледани по-долу iv).

i) Правни основания за предоставяне на услугата

40. Както е видно от раздел IV, доставчиците на интернет услуги обработват информацията върху заглавните част на IP пакетите за цели, включващи насочване на всеки IP пакет към неговия получател. С член 6, параграф 1 и член 6, параграф 2 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се позволява обработка на данните за трафика за целите на пренасяне на съобщение. По този начин доставчиците на интернет услуги могат да обработват информацията, която е необходима за предоставяне на услугата.

ii) Правни основания за гарантиране на сигурността на услугата

41. Съгласно член 4 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации всеки доставчик на интернет услуги е задължен да вземе подходящи технически и организационни мерки, за да гарантира сигурността на своите услуги. Практиката за филтриране на вируси може да включва обработката на заглавните части на IP пакетите и полезния товар на IP пакетите. Като се има предвид, че в член 4 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се изисква доставчиците на интернет услуги да гарантират сигурността на мрежата, тази разпоредба легитимира техниките за провеждане на проверка, основани на заглавни части на IP пакетите и на съдържание, с което се цели стриктното постигане на тази цел. На практика това означава, че в границите, определени от принципа на пропорционалност (виж раздел V.3), доставчиците на интернет услуги могат да участват в наблюдение и филтриране на съобщителни данни за борба с вирусите и като цяло да гарантират сигурността на мрежата ([27]).

([26]) Съображение 10 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации гласи: „В сектора за електронни комуникации се прилага Директива 95/46/ЕО, по-специално по всички въпроси, засягащи защита на основни права и свободи, които не са специално обхванати от разпоредбите на настоящата директива, включително задълженията на администратора и правата на лицата“. По отношение на съгласието на съответното физическо лице от значение е също така и съображение 17: „За целите на настоящата директива съгласието на потребителя или абоната, независимо дали последният е физическо или юридическо лице, трябва да има същото значение, както данните-обект на съгласие, както са определени и допълнително уточнени в Директива 95/46/ЕО“.

([27]) Становище 2/2006 на Работната група по член 29 относно въпроси за неприкосновеността на личния живот, свързани с предоставянето на услуги за скрининг на електронна поща, прието на 21 февруари 2006 г. (WP 118). В това становище работната група счита, че използването на филтри за целите на член 4, може да бъде съвместимо с член 5 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

iii) Правни основания за свеждане до минимум на ефекта от претоварване

42. *Обосновката* за това правно основание може да бъде намерена в съображение 22 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, в което се разяснява забраната от член 5, параграф 1 да се съхраняват съобщения. Това не забранява автоматичното, междинното и временното съхранение на тази информация, доколкото това се прави единствено с цел осъществяване на предаване и не продължава за по-дълъг период от необходимия за предаване и за целите на управление на трафика, а поверителния характер на съобщенията остава гарантиран.

43. Ако има претоварване, възниква въпросът дали доставчиците на интернет услуги могат да обмислят произволно да понижават или забавят трафика или просто да забавят съобщенията, които не са чувствителни спрямо фактора време, например P2P или трафика на електронна поща, което позволява например гласовият трафик да стане с приемливо качество.

44. Предвид цялостния обществен интерес за гарантиране на използваема съобщителна мрежа, доставчиците на интернет услуги могат да твърдят, че даването на предимство или ограничаването на трафика за справяне с претоварването е законна мярка, която е необходима за предоставяне на адекватна услуга. Това означава, че в тези случаи и за тази цел ще има общо законово основание за обработката на лични данни и няма да е необходимо изричното съгласие на потребителите.

45. В същото време възможността за подобна намеса не е неограничена. Ако доставчиците на интернет услуги трябва да проверяват съобщенията с оглед на поверителността и да прилагат стриктно принципа на пропорционалност, за постигането на тази цел те трябва да използват метода с най-малка намеса, който е достъпен (като се избягва задълбочената проверка на пакетите с интернет данни) и трябва да го прилагат толкова дълго, колкото е необходимо за разрешаване на проблема с претоварването.

iv) Правни основания за обработката на данни за други цели

46. Доставчиците на интернет услуги могат също така да искат да проверяват данните за трафика и съдържанието и за други цели, например за предлагане на целеви абонаменти (напр. абонамент, при който се ограничава достъпът до P2P, или абонамент, при който се увеличава скоростта за определени приложения). Проверката и по-нататъшната употреба на данни за трафика и съобщителни данни за цели, различни от тези по предоставяне на услугата или гарантиране на нейната сигурност и липсата на претоварване, са разрешени само при строго определени условия, в съответствие с правната рамка.

47. Правната рамка е главно член 5, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, с който се изисква съгласие от потребителите за слушане, записване, съхранение или участие в други видове подслушване или наблюдение на съобщения и на свързаните данни за трафика. На практика това означава, че съгласието на потребителите, участващи в съобщаването е необходимо, за да се легитимира обработката както на данните за трафика, така и на съобщителните данни съгласно член 5, параграф 1.

48. Както бе обяснено по-горе, прилагането на техники за проверка и филтриране се основава или на заглавните части на IP пакетите, които представляват данни за трафика, или на задълбочена проверка на пакетите с интернет данни, която също включва полезния товар на IP пакетите, представляващи съобщителни данни. Следователно по принцип прилагането на такива техники за цели, различни от предоставянето на услугата или сигурността, би било забранено, освен ако обработката не е позволена от правно основание, като например съгласието (член 5, параграф 1). Пример за прилагането на член 5, параграф 1 е в случаите, когато доставчик на интернет услуги реши да предложи на клиентите намалена тарифа за достъп до интернет в замяна на получаване на поведенческа реклама, като използва задълбочена проверка на пакетите с интернет данни и следователно съобщителни данни, за да го постигне. Следователно съгласно член 5, параграф 1 в действителност е необходимо конкретно и информирано съгласие.

49. Освен това с член 6 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, озаглавен „данни за трафик“ се предоставят определени правила, приложими специално за данните за трафика. По-специално в него се предвижда възможността доставчиците на интернет данни да

обработват данни за трафика въз основа на съгласието на потребителите да получават услуги с добавена стойност ([28]). С тази разпоредба се определят изискванията за съгласие, предвидени в член 5, параграф 1, когато са засегнати данните за трафика.

50. На практика невинаги е лесно да се установи в кои случаи е необходимо съгласие и в кои случаи сигурността на мрежата може да легитимира обработката, по-специално ако целите на техниките за проверка са две (например избягване на претоварването и предоставяне на услуги с добавена стойност). Следва да се подчертае, че съгласието не може да се счита за лесен и систематичен начин за постигане на съответствие с принципите за защита на данни.

51. Опитът относно прилагането на рамката и по-специално относно различните аспекти, описани по-горе, е малък. Това е област, в която допълнителните насоки, доразвити в раздел VI, са от съществено значение. Освен това има допълнителни свързани аспекти по отношение на получаването на съгласие, които също изискват специално внимание. Те са описани по-долу.

V.2. **Въпроси, свързани с предоставянето на информирано съгласие като правно основание**

52. Съгласието, което се изисква по силата на членове 5 и 6 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации има същото значение, както данните-обект на съгласие, както са определени и допълнително уточнени в Директива 95/46/ЕО ([29]). В съответствие с член 2, буква з) от Директивата за защита на личните данни „съгласие на съответното физическо лице означава „всяко свободно изразено, конкретно и информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него“. Неотдавна в становище 15/2011 относно съгласието на Работната група по член 29 бяха разгледани ролята на съгласието и изискванията за неговата валидност ([30]).

53. Следователно доставчиците на интернет услуги, които изискват съгласие за участие в проверка и филтриране на данни за трафика и съдържанието, трябва да гарантират, че съгласието е свободно изразено и конкретно, и то трябва да представлява цялостно информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него. В съображение 17 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации отново се потвърждава, че „(…) Съгласие може да бъде дадено по всеки подходящ начин, позволяващ свободно да се посочи специфичен и уведомителен знак за желанията на потребителя, включително чрез отбелязване в графа, при посещение на интернет страница“. По-долу следват няколко практически примера за това какво означава в този контекст съгласието да бъде свободно изразено, конкретно и информирано.

Съгласие: Свободно изразено, конкретно и информирано указание за волята на съответното физическо лице

54. *Свободно изразено съгласие.* Потребителите не трябва да страдат от ограничения, свързващи съгласието с абонамент за интернет, който те искат да сключат.

55. Съгласието на физическите лица не би било свободно изразено, ако то трябва да бъде дадено за наблюдение на техните съобщителни данни, с цел те да получат достъп до съобщителни услуги. Това би било още по-вярно, ако *всички* доставчици на даден пазар участват в управлението на трафика за цели, които се простират отвъд сигурността на мрежата. Единствената друга възможност е изобщо да не се абонират за интернет услуги. Предвид факта, че интернет е станал много важен инструмент както за

([28]) Съображение 18 от директивата съдържа списък, който илюстрира услугите с добавена стойност. Не е ясно дали услугите, за които се прилагат политиките за управление на трафика, може да се тълкуват като част от списъка. Политики за управление на трафика, целящи да дадат приоритет на определено съдържание, могат да бъдат възприемани, като осигуряващи качество на услугата. Например управление на трафика, което води просто до обработката на заглавните части на IP пакетите и има за цел предлагане на услуги за игри на цени с надбавки, при които на личния трафик за игри на потребителите е даден приоритет чрез мрежата, могат да бъдат разглеждани като услуги с добавена стойност. От друга страна не е много ясно дали управлението на трафика с цел ограничаване на някои видове трафик, например понижаването на P2P трафика, може да се счита за такова.

([29]) Виж съображение 17 и член 2, буква е) от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

([30]) Прието на 13 юли 2011 г. (WP 187).

работа, така и за развлекателни цели, липсата на абонамент за интернет услуги не представлява валидна алтернатива. Резултатът би довел до това лицата да нямат реален избор, т.е. те няма да могат да изразят свободно съгласието си ([31]).

56. ЕНОЗД счита, че съществува ясна необходимост Комисията и националните органи да наблюдават пазара, по-специално за да се установи дали този вариант — т.е. доставчиците да свързват телекомуникационни услуги с наблюдението на съобщенията — става общоприет. Доставчиците следва да предложат алтернативни услуги, включително абонамент за интернет, който не подлежи на управление на трафика, без да се налагат по-високи разходи за лицата.

57. *Конкретно съгласие*. Поради необходимостта съгласието да бъде конкретно, в този случай се изисква доставчиците на интернет услуги да поискат съгласие за наблюдение на трафика и съобщителни данни по един ясен и характерен начин. Съгласно Работната група по член 29 „… за да бъде конкретно, съгласието трябва да бъде разбираемо: то трябва да се отнася ясно и точно за обхвата и последиците от обработката на данните и не може да се прилага за един отворен набор от дейности по обработка. С други думи това означава, че контекстът, в който се прилага съгласието, е ограничен.“ Има вероятност конкретното съгласие да не бъде получено, ако съгласието за проверката на данните за трафика и съобщителните данни е „обвързано“ с общото съгласие за абониране за услугата. Вместо това спецификата поражда необходимост от използването на целеви средства за получаване на съгласието, като формуляр за конкретно съгласие или отделна графа, ясно предназначени за целите на наблюдението (а не информацията да бъде включена в общите условия на договора и да се изисква подписване на договора в този му вид).

58. *Информирано съгласие*. За да бъде валидно едно съгласие, то трябва да бъде информирано. Нуждата от осигуряване на адекватна предварителна информация произтича не само от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, но и от членове 20 и 21 от Директивата за универсалната услуга, изменена с Директива 2009/136/ЕО ([32]). Нуждата от информация и съгласие е изрично потвърдена в съображение 28 от Директива 2009/136/ЕО: „ползвателите следва във всички случаи да са напълно осведомени относно всякакви ограничения върху използването на електронни съобщителни услуги, наложени от доставчика на услуги и/или на мрежи. Такава информация следва, по избор на доставчика, да посочва конкретно вида на съответното съдържание, приложение или услуга, индивидуалните приложения или услуги, или и двете“. След това, то уточнява, че: „В зависимост от използваната технология и вида ограничение такива ограничения може да изискват съгласие на ползвателя съгласно Директива 2002/58/ЕО“.

59. Като се има предвид сложността на тези техники за наблюдение, предоставянето на смислена предварителна информация е едно от главните предизвикателства за получаване на валидно съгласие. Потребителите трябва да бъдат информирани по начин, който им позволява да разбират как се използва информацията, която се обработва и въздействието върху опита на потребителя, както и нивото на посегателство върху неприкосновеността на личния живот, свързано с тези техники.

60. Това означава, че не само информацията трябва да бъде ясна и разбираема за средния потребител, но и че тя се представя на лицата директно по видим начин, така че да не могат да я пренебрегнат.

61. *Указания за волята*. Съгласно приложимата правна рамка за съгласието също се изисква утвърдително действие от страна на потребителя, за да изрази своето съгласие. Мълчаливото съгласие не отговаря на този стандарт. Това също потвърждава необходимостта да се използват специфични средства за получаване на съгласие, което позволява на доставчиците на интернет услуги да извършват проверка на трафика и на съобщителните данни в контекста на прилагането на политиките за управление на трафика. В неотдавнашното си становище относно съгласието Работната група по член 29 подчерта необходимостта от детайлност при получаване на съгласието с оглед на различните елементи, от които се състои обработката на данни.

([31]) Подобен е случаят PNR, при който се разисква дали съгласието на пътниците за прехвърляне на информация за резервациите им на органите на САЩ е валидно. Работната група счита, че съгласието на пътниците не е свободно изразено, тъй като авиокомпаниите са задължени да изпращат данните преди излитането на самолетите и следователно пътниците нямат реален избор, ако искат да ползват въздухоплавателни услуги; Становище 6/2002 на Работната група по член 29 относно предаването на информация от списъка на пътниците и други данни от авиокомпаниите на органите на САЩ.

([32]) Директива 2009/136/ЕО от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги (вж. бележка под линия 15).

62. Могат да се намерят доводи, че ако лицата, участващи в съобщаването, не желаят доставчиците на интернет услуги да имат достъп до него, за да прилагат политиките за управление на трафика, те винаги могат да кодират съобщението. От практическа гледна точка този подход може да счита за полезен, въпреки че изисква известни усилия и технически познания и не може да се счита за подобен на свободно изразеното, конкретното и информираното съгласие. Също така използването на техники за кодиране не запазва напълно поверителността на съобщението, тъй като доставчикът на интернет услуги ще има достъп поне до информацията от заглавната част на IP пакета, за да насочва съобщението, и ще бъде в позицията да прилага статистически анализ.

63. Съгласно член 5, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации трябва да бъде получено съгласие от заинтересованите потребителите. В много случаи потребителят ще бъде същевременно и абонатът, което позволява съгласието да бъде дадено в момента на сключване на абонамента за телекомуникационни услуги. В други случаи, включително тези, в които участват повече от едно лице, съгласието на заинтересованите потребители ще трябва да бъде получено поотделно. Това би породило практически въпроси, както е обяснено по-долу.

Съгласие на всички заинтересовани потребители

64. В член 5, параграф 1 се предвижда съгласието на потребителя да легитимира обработката. *Всички потребители*, участващи в съобщаването, трябва да дадат своето съгласие. *Обосновката* на това твърдение е, че съобщаването обикновено засяга поне две лица (изпращача и получателя). Например, ако доставчик на интернет услуги сканира полезните товари на IP пакетите, които се отнасят за електронна поща, те проверяват информацията, която се отнася както за изпращача, така и за получателя на електронната поща.

65. Когато се извършва наблюдение и прихващане на трафика и на съобщенията (напр. някакъв уеб трафик), за доставчиците на интернет услуги може да е достатъчно да получат съгласието на потребителя, който е и абонатът. Това е така, защото в този случай (посетен уебсайт) другото лице, участващо в съобщаването, може да не се разглежда като „заинтересован потребител“ ([33]). Ситуацията обаче може да се усложни още повече, когато такова наблюдение включва проверка на съдържанието на електронната поща и по този начин на личната информация на изпращача и получателя на писмото, които е възможно да нямат договорни отношения с един и същи доставчик на интернет. Наистина в този случай доставчикът на интернет услуги ще обработва лични данни (име, електронна поща и потенциално чувствителни данни за съдържанието) на лица, които не са потребители. От практическа гледна точка получаването на съгласие от такива лица може да бъде доста по-трудно, тъй като следва да се направи въз основа на всеки отделен случай, а не по повод сключването на договор за телекомуникационни услуги. Не би било реалистично да се предполага, че съгласието на абонатите е дадено от името на други потребители, какъвто често може да бъде случаят с частните домакинства.

66. В този контекст ЕНОЗД счита, че доставчиците на интернет услуги трябва да спазват съществуващите правни изисквания и да прилагат политики, които не включват наблюдение и проверка на информация. Това е още по-важно по отношение на съобщителните услуги, които включват трето лице, което не е в състояние да даде съгласието си за наблюдение, по-специално по отношение на изпратените и получените електронни писма (това не се прилага, когато целта се основава на съображения за сигурност).

67. В същото време следва да се отбележи, че националното законодателство, в което се прилага член 5, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, невинаги може да бъде задоволително по този въпрос и като цяло изглежда, че в този контекст има по-скоро необходимост от по-добри насоки относно изискванията на Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Поради това ЕНОЗД приканва Комисията да бъде по-активна в това отношение и да предприеме инициатива, при която биха могли да бъдат извлечени ползи от информацията от надзорните органи, събрани в Работната група по член 29, както и от други заинтересовани страни. Ако е необходимо, случаят следва да бъде отнесен пред Съда с цел да се постигне пълна яснота относно смисъла и последствията от член 5, параграф 1.

([33]) Въпреки онези случаи, при които уеб трафикът включва предаване на лична информация, като например снимки за индентификация на физически лица, публикувани на уебсайт. Обработката на такава информация изисква правно основание, но не би била обхванатa от член 5, параграф 1, тъй като лицата не са „заинтересовани потребители“.

V.3. **Пропорционалност — принцип за намаляване на количеството данни**

68. В член 6, буква в) от Директивата за защитата на личните данни се определя принципът на пропорционалност ([34]), който се прилага по отношение на доставчиците на интернет услуги, тъй като, когато участват в наблюдение и филтриране, те се явяват администратори на данни по смисъла на тази директива.

69. Съгласно този принцип личните данни могат да бъдат обработвани само ако те са „адекватни, релевантни, и да не са прекомерни по отношение на целите, за които се събират и/или обработват допълнително“. Прилагането на този принцип води до необходимостта да се направи оценка на това дали средствата, използвани за обработката на данните, и видът на използваните личнит данни са подходящи и има вероятност да постигнат целите си. Ако изводът е, че се събират повече данни, отколкото е необходимо, следователно принципът не е спазен.

70. Съответствието на определени видове техники за проверка с принципа на пропорционалност трябва да бъде оценено за всеки отделен случай. Не е възможно да се достигне до заключенията *in abstracto*. Въпреки това е възможно да се посочат различни конкретни аспекти, които следва да бъдат оценени при преценка на съответствието с принципа на пропорционалност.

71. *Размер на обработваната информация*. Наблюдение във възможно най-висока степен на съобщения на клиенти на доставчик на интернет услуги в повечето случаи е прекомерно и незаконно. Фактът, че това може да бъде извършено със средства, които не са видими за лицата, и че има вероятност за тях да е трудно да разберат какво се случва, увеличава въздействието върху неприкосновеността на личния им живот. Доставчиците на интернет услуги следва да оценят кои средства за постигане на желания резултат са с по-малка степен на вмешателство. Например възможно ли е вместо извършването на задълбочена проверка на пакетите с интернет данни желания резултат да се постигне чрез наблюдение на заглавните части на IP пакетите? Дори при използването на задълбочена проверка на пакетите с интернет данни е възможно необходимата информация да бъде получена само от идентификацията на определени протоколи. Прилагането на предпазни мерки за защита на данните, включително псевдоанонимност, също може да бъде от значение. Резултатът от оценката трябва да потвърди, че обработката на данни е пропорционална.

72. *Резултат от обработката (пряко свързан с целите)*. Пропорционалност може да липсва в случаите, когато доставчиците на интернет услуги използват политиките за управление на трафика, с изключение на достъпа до определени услуги, без да позволяват предоставяне на потребителите на справедлив дял от получените ползи в замяна.

73. Важно е да се припомни, че принципът на пропорционалност продължава да се прилага дори и ако други задължителни правни изисквания са изпълнени, включително и ако например доставчик на интернет услуги е получил съгласие от лицата да участват в наблюдение на съдържанието. Това означава, че обработката на данните, извършена чрез наблюдение на съдържанието, все още може да бъде незаконна, ако нарушава подчертания основен принцип на пропорционалност.

V.4. **Мерки за сигурност и организационни мерки**

74. С член 4 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации се изисква доставчиците на интернет услуги да вземат технически и организационни мерки, за да гарантират: i) че до личните данни има достъп единствено упълномощен персонал и той е за законни цели; ii) защитата на личните данни от случайна или неправомерна обработка, и iii) прилагане на политиката за сигурност по отношение на обработката на лични данни. С него също така на националните компетентни органи се позволява да извършват одити по отношение на тези мерки.

75. Освен това съгласно член 4, параграфи 3 и 2 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации доставчиците на интернет услуги са задължени и да уведомят съответните национални компетентни органи в случай на нарушаване на данните, както и лицата, които са засегнати, в случай че това оповестяване може да има неблагоприятни последици за тях.

76. Обработката на лична информация, включена в съобщенията с цел да се прилагат политиките за управление на трафика, може да даде на доставчиците на интернет услуги достъп до данни, които са дори по-чувствителни от данните за трафика.

([34]) Както беше посочено по-горе, Директивата за защита на личните данни се прилага за всички въпроси относно защитата на основните права и свободи, които не са специално обхванати от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

77. Следователно политиките за сигурност, разработени от доставчиците на интернет услуги, следва да включват специфични предпазни мерки, за да се гарантира, че взетите мерките са адекватни по отношение на тези рискове. В същото време националните компетентни органи, които извършват одит на мерките, следва да бъдат особено взискателни. В заключение следва да се гарантира, че са въведени ефективни процедури за уведомяване, за да се информират субектите на данни, чиято информация е компрометирана и които поради това може да са неблагоприятно засегнати.

VI. **ПРЕДЛОЖЕНИЯ ЗА ПОЛИТИКА И ЗАКОНОДАТЕЛНИ МЕРКИ**

78. Техниките за проверка, основаващи се на данни за трафика и проверка на полезния товар на IP пакетите, т.е. съдържанието на съобщенията, могат да разкрият дейности на потребителите в интернет: посетени уебсайтове и дейности, свързани с тези сайтове, използване на P2P приложения, свалени файлове, изпратени и получени електронни писма, от кого, по каква тема и при какви условия и т.н. Доставчиците на интернет услуги могат да използват тази информация, за да дадат приоритет на някои видове съобщения пред други, като например видео по заявка. Възможно е да искат да я използват за откриване на вируси или създаване на профили с цел обслужване на поведенческа реклама. Тези действия накърняват правото на поверителност на съобщенията.

79. В зависимост от използваните техники и спецификата на случая последиците върху неприкосновеността на личния живот ще се увеличат. Колкото по-задълбочени са прихващането и анализът на събраната информация, толкова по-голямо е противоречието с принципа на поверителност на съобщенията. Ключови елементи за определяне на степента на намеса в личния живот и личните данни на физическите лица са също и целите, за които се провежда наблюдението, и прилаганите предпазни мерки за защита на данните. Блокирането и наблюдението за целите на борбата със зловредния софтуер, заедно със строгите ограничения относно съхранението и използването на проверявани данни, не могат да бъдат сравнявани със ситуации, при които информацията се натрупва за създаване на индивидуални профили с цел обслужване на поведенческа реклама.

80. По принцип ЕНОЗД счита, че ако съществуващата рамка на ЕС за неприкосновеност на личния живот и защита на данните бъде тълкувана, прилагана и изпълнявана правилно, би била подходяща да гарантира, че правото на поверителност се спазва и че защитата на неприкосновеността на личния живот и защитата на данните на физическите лица като цяло не е изложена на опасност ([35]). Доставчиците на интернет услуги не следва да използват такива механизми освен ако не прилагат по подходящ начин правната рамка. По-специално съответните елементи от рамката, която доставчиците на интернет услуги следва да имат предвид и да спазват, включват следното:

— Доставчиците на интернет услуги могат да прилагат политики за управление на трафика, предназначени да осигуряват сигурност на услугата, доставяне на услугата, включително ограничаване на претоварването съгласно членове 4 и 6 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

— Доставчиците на интернет услуги се нуждаят от друго конкретно правно основание и вероятно от съгласието на потребителите, за да прилагат политики за управление на трафика, които водят до обработка на данните за трафика и/или на съобщителните данни за цели, различни от горепосочените. Например информираното съгласие на потребителите е необходимо за наблюдение и филтриране на съобщенията на физическите лица за целите на ограничаване (или разрешаване) на достъпа до определени приложения и услуги, като например P2P или VoIP.

— Съгласието може да бъде свободно изразено, изрично и информирано. То следва да се укаже чрез утвърдително действие. Тези изисквания поставят силен акцент върху необходимостта да се активизират усилията, за да се гарантира, че физическите лица са надлежно информирани по пряк, разбираем и конкретен начин, така че да могат да оценят последиците от практиките и в крайна сметка да вземат информирано решение. Предвид сложността на тези техники, предоставянето на смислена предварителна информация на потребителите е едно от основните предизвикателства за получаване на валидно съгласие. Освен това не следва да има неблагоприятни последици (включително финансови разходи) за потребители, които не са дали съгласие за наблюдение.

([35]) Това не засяга необходимостта от промени в законодателството, основаващи се на други съображения, по-специално в контекста на общия преглед на законодателната рамка на ЕС за защита на данните, с цел да се подобри ефективността ѝ с оглед на новите технологии и глобализацията.

— Принципът на пропорционалност има решаващо значение, когато доставчиците на интернет услуги участват в политиките за управление на трафика, независимо от правното основание за обработката и целта: доставяне на услуга, избягване на претоварване или предоставяне на целеви абонаменти със или без достъп до определени услуги или приложения. Този принцип ограничава възможността на доставчиците на интернет услуги да участват в наблюдение на съдържанието на съобщения на физически лица, което води до прекомерна обработка на информация или произтичащи ползи единствено за доставчиците на интернет услуги. Какво може да се направи от доставчиците на интернет услуги от логистична гледна точка ще зависи от нивото на навлизане на техниките, желаните резултати (за които те могат да натрупат ползи) и приложените специфични предпазни мерки за неприкосновеност на личния живот и защита на данните. Преди внедряването на техниките за проверка доставчиците на интернет услуги трябва да участват в оценка на съвместимостта им с принципа на пропорционалност.

81. Въпреки че понастоящем законодателната рамка включва съответните условия и предпазни мерки, необходимо е да се обърне особено внимание на това дали доставчиците на интернет услуги ефективно спазват законодателните изисквания, дали предоставят необходимата информация за потребителите, за да направят смислен избор и дали спазват принципа на пропорционалност. На национално равнище органите, компетентни за горепосоченото, включват от една страна националните телекомуникационни органи, а от друга — националните органи за защита на данните. На равнище ЕС съответните органи на равнище ЕС включват ОЕРЕС. Възможно е ЕНОЗД също да играе роля в този контекст.

82. В допълнение към наблюдението на настоящото ниво на съответствие и предвид сравнително новите възможности на масивната, протичаща в реално време проверка на съобщенията, някои аспекти, свързани с прилагането на рамката, които бяха разгледани в настоящото становище, изискват допълнителен, по-задълбочен анализ и разясняване. Насоките, които са особено значими за няколко области, включват:

— Определяне на законни практики за проверка, за да се гарантира непрекъснатост на трафика, без да се изисква съгласие на потребителя, както например при борбата срещу спама. В допълнение към вмешателството на приложеното наблюдение, аспекти, като например нивото на нарушаване на непрекъснатостта на трафика, които биха били налице, също имат отношение към въпроса.

— Определяне на техниките за проверка, които могат да бъдат използвани за целите на сигурността, които може да не изискват съгласието на потребителите.

— Определяне кога при наблюдението се изисква съгласието на лицето, особено съгласието на всички заинтересовани потребители, и определяне на допустимите технически параметри, за да се гарантира, че техниката за проверка не предполага обработка на данни, която не е пропорционална по отношение на предвиденото ѝ предназначение.

— Освен това в трите горепосочени случая е възможно да са необходими насоки относно прилагането на необходимите предпазни мерки за защита на данните (ограничаване на целите, сигурност и т.н.).

83. Като се има предвид, че компетентностите в тази област са както национални, така и на равнище ЕС, ЕНОЗД счита, че споделянето на гледни точки и опит с цел да се определи хармонизиран подход за горепосоченото е от съществено значение. За да се постигне това, ЕНОЗД предлага да се създаде платформа или експертна група, която следва да обединява представители от националните регулаторни органи — Работната група по член 29, ЕНОЗД и ОЕРЕС. Първата цел на тази платформа би била разработването на насоки поне относно посочени по-горе точки с цел да се гарантират солидни и хармонизирани подходи и равнопоставеност. ЕНОЗД призовава Комисията да организира тази инициатива.

84. Не на последно място, както националните органи, така и техните сродни организации от ЕС, включително ОЕРЕС и Европейската комисия, трябва да обърнат сериозно внимание на пазарното развитие в тази област. С оглед на защитата на данните и неприкосновеността на личния живот един вариант, при който доставчиците на интернет услуги, участващи на рутинна основа в политики за управление на трафика, предлагат абонамент, основан на филтриращ достъп до съдържанието и приложенията, би бил крайно проблематичен. Ако това се случи, ще трябва да бъде въведено законодателство за справяне с тази ситуация.

VII. **ЗАКЛЮЧЕНИЯ**

85. Увеличаването на зависимостта на доставчиците на интернет услуги от наблюдението и техниките за проверка засяга неутралния характер на интернет и поверителността на съобщенията. Това поражда сериозни въпроси, свързани със защитата на неприкосновеността на личния живот и личните данни на потребителите.

86. Въпреки че в съобщението на Комисията относно отвореното и неутрално интернет пространство в Европа накратко се засягат тези въпроси, ЕНОЗД счита, че следва да се направи повече, за да се достигне до една задоволителна политика за бъдещи действия. Следователно с настоящото становище той допринася за продължаващия политически дебат относно неутралния характер на интернет, по-специално относно аспектите, свързани със защитата на данните и неприкосновеността на личния живот.

87. ЕНОЗД счита, че е необходимо националните органи и ОЕРЕС да наблюдават ситуацията на пазара. Това наблюдение трябва да доведе до ясна картина, описваща дали пазарът се развива към масивна, протичаща в реално време проверка на съобщенията, и въпросите, свързани със спазването на правната рамка.

88. Наблюдението на пазара не трябва да се извършва без допълнителен анализ на въздействието на новите практики във връзка със защитата на данните и неприкосновеността на личния живот в интернет. В настоящото становище се очертават някои области, в които разясняването би било от полза. Въпреки че агенциите и органите на ЕС като ОЕРЕС, Работната група по член 29 и ЕНОЗД може би са в състояние да разяснят условията за прилагане на рамката, ЕНОЗД счита, че Комисията е задължена да координира и направлява дебата. Следователно той призовава Комисията да предприеме инициатива, която да включва всички тези заинтересовани страни в платформа или работна група за тази цел. Сред въпросите, които се нуждаят от допълнителен анализ, следва да се разгледат следните точки:

— Определяне на практиките за проверка, които са законни с оглед гарантиране на непрекъснатостта на трафика и които могат да бъдат провеждани за целите на сигурността;

— Определяне кога при наблюдението се изисква съгласието на лицето, особено съгласието на всички заинтересовани потребители, и определяне на допустимите технически параметри, за да се гарантира, че техниката за проверка не предполага обработка на данни, която не е пропорционална по отношение на предвиденото ѝ предназначение.

— Възможно е в горепосочените случаи да са необходими насоки относно прилагането на необходимите предпазни мерки за защита на данните (ограничаване на целите, сигурност и т.н.).

89. В зависимост от тези констатации може да са необходими допълнителни правни мерки. В такъв случай Комисията следва да приеме политически мерки, които имат за цел укрепване на правната рамка и гарантиране на правната сигурност. В новите мерки следва да се разясняват практическите последици от принципа на неутралност на интернет, както вече е направено в някои от държави-членки, и да се гарантира, че потребителите могат да направят реален избор, по-специално като изискват доставчиците на интернет услуги да предлагат ненаблюдавани връзки.

Съставено в Брюксел на 7 октомври 2011 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните