I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА ДАННИТЕ

Становище на Европейския надзорен орган по защита на данните относно предложение за директива на Европейския парламент и на Съвета за изменение, наред с други директиви, на Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации)

(2008/C 181/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

като взе предвид Договора за създаване на Европейската общност, и по-специално член 286 от него,

като взе предвид Хартата на основните права на Европейския съюз, и по-специално член 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 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 [2],

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, и по- специално член 41 от него [3],

като взе предвид искането за становище в съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001, получено на 16 ноември 2007 г. от Европейската комисия,

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

1. На 13 ноември 2007 г. Комисията прие предложение за директива за изменение, наред с други директиви, на Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (наричано оттук-нататък „предложение“ или „предложени изменения“). Обикновено, както и в настоящото становище, позоваването на настоящата версия на Директива 2002/58/ЕО е като „Директива за защитата на личния живот и електронните комуникации“.

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) ОВ L 201, 31.7.2002 г., стр. 37.
([3]) ОВ L 8, 12.1.2001 г., стр. 1.

2. Предложението има за цел да подобри защитата на личния живот и на личните данни в сектора на електронните комуникации. За целта не се прави цялостна преработка на съществуващата Директива за защитата на личния живот и електронните комуникации, а по-скоро се предлагат *ad hoc* изменения към нея, които основно целят да укрепят разпоредбите, свързани със сигурността, и да подобрят механизмите за прилагане.

3. Предложението е част от по-широка реформа на петте директиви на ЕС за телекомуникациите („пакет за телекомуникациите“). В допълнение към предложенията за преразглеждане на пакета за телекомуникациите ([1]) Комисията прие и предложение за регламент за създаване на Европейския орган за пазара на електронни комуникации ([2]).

4. Забележките, съдържащи се в настоящото становище, се ограничават до предложените изменения на Директивата за защитата на личния живот и електронните комуникации, освен ако тези предложени изменения не почиват върху понятия или разпоредби, които се съдържат в предложенията за преразглеждане на пакета за телекомуникациите. Освен това някои бележки, съдържащи се в настоящото становище, се отнасят до разпоредби от Директивата за защитата на личния живот и електронните комуникации, които не са изменени от предложението.

5. Настоящото становище разглежда следните теми: i) обхвата на Директивата за защитата на личния живот и електронните комуникации и, в частност, съответните услуги (предложено изменение на член 3, параграф 1); ii) уведомяването за нарушения на сигурността (предложено изменение за създаване на членове 4, параграф 3 и 4 параграф 4); iii) разпоредбите относно „бисквитки“ (*cookies*), софтуер за наблюдение (*spyware*) и други подобни устройства (предложено изменение на член 5, параграф 3); iv) правните действия, предприемани от доставчиците на електронни съобщителни услуги и от други юридически лица (предложено изменение за създаване на член 13, параграф 6) и v) укрепването на разпоредбите за прилагане (предложено изменение за създаване на член 15а).

Консултация с ЕНОЗД и по-широка обществена консултация

6. Предложението беше изпратено от Комисията на ЕНОЗД на 16 ноември 2007 г. ЕНОЗД разглежда съобщението като искане за провеждане на консултации с институциите и органите на Общността, както е предвидено в член 28, параграф 2 от Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (наричан оттук нататък „Регламент (ЕО) № 45/2001“).

7. Преди приемането на предложението Комисията проведе неформална консултация с ЕНОЗД относно проекта за предложение, което бе приветствано от ЕНОЗД предвид така предоставената му възможност да направи някои предложения по проекта за предложение преди приемането му от Комисията. ЕНОЗД със задоволство отбелязва, че някои от предложените от него идеи са отразени в предложението.

8. Приемането на предложението беше предшествано от широка публична консултация — практика, която ЕНОЗД оценява. Наистина, през юни 2006 г. Комисията организира публична консултация относно своето съобщение за преразглеждане на пакета за телекомуникациите, като разясни своите виждания за ситуацията и представи някои предложения за изменения ([3]). Работна група „Защита на данните/член 29“, чийто член е ЕНОЗД, използва възможността да представи своите виждания по предложените изменения под формата на становище, прието на 26 септември 2006 г. ([4]).

([1]) Предложените изменения на директивите за телекомуникациите са включени в следните предложения: i) Предложение за директива на Европейския парламент и на Съвета за изменение на Директиви 2002/21/ЕО относно общата регулаторна рамка за електронните съобщителни мрежи и услуги, 2002/19/ЕО относно достъпа до електронни съобщителни мрежи и тяхната инфраструктура и взаимосвързаността между тях и 2002/20/ЕО относно разрешението на електронните съобщителни мрежи и услуги, 13 ноември 2007 г., COM(2007) 697 окончателен; ii) Предложение за директива на Европейския парламент и на Съвета 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 в областта на защита на потребителите, 13 ноември 2007 г., COM(2007) 698 окончателен.

([2]) Предложение за регламент на Европейския парламент и на Съвета за създаване на Европейския орган за пазара на електронни комуникации, 13 ноември 2007 г., COM(2007) 699 окончателен.

([3]) Съобщение относно регулаторната рамка на ЕС за електронни съобщителни мрежи и услуги (SEC (2006) 816), прието на 29 юни 2006 г. Съобщението бе допълнено от работен документ на службите на Комисията (COM (206) 334 окончателен).

([4]) Становище 8/2006 относно прегледа на регулаторната рамка на ЕС за електронни съобщителни мрежи и услуги, което разглежда по-специално Директивата за защитата на личния живот и електронните комуникации, прието на 26 септември 2006 г.

Виждания на ЕНОЗД като цяло

9. Като цяло виждания на ЕНОЗД относно предложението са положителни. ЕНОЗД подкрепя напълно целите на Комисията за приемане на предложение, което да подобри защитата на личния живот и на личните данни в сектора на електронните комуникации. ЕНОЗД по-специално приветства приемането на система за задължително уведомяване за нарушения на сигурността (изменение на член 4 от Директивата за защитата на личния живот и електронните комуникации, като се добавят параграфи 3 и 4). В случай на възникване на нарушения по отношение на данните, ползите от уведомяването са безспорни, тъй като чрез него се укрепва отчетността на организациите, и то е фактор, подтикващ компаниите да прилагат строги мерки за сигурност, като позволява да се определят най-надеждните технологии по отношение на защитата на информацията. Освен това, в резултат на уведомяването засегнатите лица могат да предприемат стъпки за защита срещу кражба на самоличност или друг вид злоупотреба с тяхната лична информация.

10. ЕНОЗД приветства и други изменения в предложението, като например възможността юридически лица със законен интерес да предприемат действие срещу лицата, които нарушават някои от разпоредбите на Директивата за защитата на личния живот и електронните комуникации (изменение на член 13, като се добавя параграф 6). Друг положителен аспект е укрепването на правомощията за осъществяване на разследване на националните регулаторни органи, което ще им позволи да преценят дали обработката на данни е извършена в съответствие със законодателството или не, както и да идентифицират нарушителите (добавяне на член 15а, параграф 3). Своевременното възпиране на незаконната обработка на лични данни и на нарушаването на правото на неприкосновеност на личния живот е необходима мярка за защита на правата и свободите на физическите лица. Във връзка с това силно се приветства предложеният член 15а параграф 2, в който се отчита правомощието на националните регулаторни органи да разпореждат прекратяване на нарушенията, тъй като този член ще им позволи незабавно да възпират незаконната обработка на данни.

11. Съдържащият се в предложението подход и по-голямата част от предложените изменения съответстват на виждания, отразени в предишни становища на ЕНОЗД по отношение на бъдещата политика за защита на данните, като например становището относно прилагането на Директивата за защита на личните данни ([1]). Наред с други неща, подходът се основава на виждането, че макар да не са необходими нови принципи за защита на личните данни, е налице необходимост от по-конкретни правила за решаване на въпросите за защита на личните данни, поставяни от новите технологии като интернет, устройствата за радио-честотна идентификация (РЧИ) и др., както и от инструменти, които допринасят за прилагането и ефективното действие на законодателството за защита на личните данни, като например се позволи на юридическите лица да предприемат действия при нарушение на защитата на личните данни и да задължават администраторите да уведомяват за нарушения на сигурността.

12. Независимо от цялостния положителен подход на предложението, ЕНОЗД изразява съжаление, че то не е достатъчно амбициозно. Наистина, с прилагането от 2003 г. на разпоредбите, съдържащи се в Директивата за защитата на личния живот и електронните комуникации, и след внимателен анализ на темата, става видно, че някои от включените в нея разпоредби не са съвсем ясни, като пораждат правна несигурност и проблеми със съответствието. Такъв е случаят, например, със степента, до която полупубличните доставчици на електронни съобщителни услуги са обхванати от Директивата за защитата на личния живот и електронните комуникации. Можехме да се надяваме, че Комисията ще се възползва от прегледа на пакета за телекомуникациите, в частност Директивата за защитата на личния живот и електронните комуникации, за да уреди някои от нерешените проблеми. Освен това, като разглежда нови въпроси като създаването на система за задължително уведомяване за нарушения на сигурността, предложението осигурява само частично решение, като не включва в обхвата на организациите, задължени да уведомяват за подобни нарушения, лицата, които обработват особено чувствителни данни, като например он-лайн банки или доставчици на он-лайн здравни услуги. ЕНОЗД изразява съжаление по отношение на този подход.

13. ЕНОЗД се надява, че в хода на законодателния процес по приемане на предложението законодателят ще вземе предвид бележките и предложенията, съдържащи се в настоящото становище, с цел разрешаване на въпросите, които не са разгледани в предложението на Комисията.

([1]) Становище на Европейския надзорен орган по защита на данните от 25 юли 2007 г. относно Съобщението на Комисията до Европейския парламент и до Съвета относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни (ОВ C 255, 27.10.2007 г., стр. 1).

II. **АНАЛИЗ НА ПРЕДЛОЖЕНИЕТО**

II.1. **Обхват на Директивата за защитата на личния живот и електронните комуникации, по-специално на съответните услуги**

14. Ключов въпрос в настоящата Директива за защитата на личния живот и електронните комуникации е въпросът за нейния обхват на приложение. В предложението се съдържат някои положителни елементи по отношение на определянето и изясняването на обхвата на директивата, по-специално услугите, разгледани в директивата, които са обсъдени по-долу в раздел i). За съжаление предложените изменения не уреждат всички съществуващи проблеми. Както става дума в раздел ii) по-долу, измененията за съжаление не целят разширяване на обхвата на приложение на директивата, така че да включи електронните съобщителни услуги в частните мрежи.

15. В член 3 от Директивата за защитата на личния живот и електронните комуникации се описват услугите, които попадат в нейния обхват, с други думи услугите, за които се прилагат задълженията, посочени в директивата: „*Настоящата директива се прилага при обработката на лични данни във връзка с предоставянето на публично достъпни електронни комуникационни услуги в публични комуникационни мрежи*“.

16. Следователно услугите, обхванати от Директивата за защитата на личния живот и електронните комуникации, са доставчиците на публични електронни съобщителни услуги в публичните мрежи (ДПЕСУПМ). Определението за ДПЕСУПМ се съдържа в член 2, буква в) от рамковата директива ([1]). Определението за публични съобщителни мрежи е дадено в член 2, буква г) от рамковата директива ([2]). Примерите за дейностите на ДПЕСУПМ включват предоставяне на достъп до интернет, пренос на информация чрез електронни мрежи, мобилни и телефонни връзки и др.

i) *Предложено изменение на член 3 от Директивата за защитата на личния живот и електронните комуникации: съответните услуги следва да включват публични съобщителни мрежи, които поддържат устройства за събиране и идентифициране на данни*

17. Предложението изменя член 3 от Директивата за защитата на личния живот и електронните комуникации, като уточнява, че публичните електронни съобщителни мрежи включват „*обществени съобщителни мрежи, които поддържат устройства за събиране и идентифициране на данни*“. В съображение 28 се разяснява, че разработването на приложения, които налагат да се събира информация, включително лични данни, като се използват радио честоти, като например устройствата за РЧИ, трябва да са предмет на Директивата за защитата на личния живот и електронните комуникации, когато са свързани или когато се възползват от публични съобщителни мрежи или услуги.

18. ЕНОЗД смята тази разпоредба за положителна, тъй като в нея се разяснява, че редица приложения за РЧИ попадат в обхвата на Директивата за защитата на личния живот и електронните комуникации, като по този начин се отстранява част от несигурността по тази точка и категорично се елиминират недоразуменията или неправилните тълкувания на закона.

19. Съгласно настоящия член 3 от Директивата за защитата на личния живот и електронните комуникации, някои приложения за РЧИ вече са обхванати от директивата. Това е възможно по ред кумулативни причини. На първо място предвид факта, че приложенията за РЧИ попадат в определението за електронните съобщителни услуги. Второ, предвид това, че са осигурявани по електронна съобщителна мрежа, доколкото приложенията се поддържат от система за пренос, която предава сигнали по

([1]) Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (ОВ L 108, 24.4.2002 г., стр. 33). Рамковата директива очертава границите на това какво следва да се разбира под електронна комуникационна система, а именно: i) „електронна съобщителна услуга“ означава услуга, осигурявана обикновено срещу заплащане, която се състои изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи, включително далекосъобщителни услуги и предавателни услуги в мрежи. ii) услугите, осигуряващи съдържанието, предавано посредством електронни съобщителни мрежи и услуги, се изключват от определението на електронни съобщителни услуги. iii) предоставяне на услуги означава създаването, оперирането, контрола или осигуряването на достъп до мрежа. iv) електронните съобщителни услуги не включват услуги на информационното общество, които са определени в Директивата за електронна търговия като услуга[и], нормално предоставяна[и] срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба на получателя на услугите.

([2]) „Обществена съобщителна мрежа“ означава електронна съобщителна мрежа, използвана изцяло или главно за осигуряване на обществено достъпни електронни съобщителни услуги.

безжичен път. И на последно място, мрежата може да бъде публична и частна. Ако е публична, приложенията за РЧИ ще бъдат счетени за „услуги, разгледани от директивата“ и по този начин попадат в обхвата на приложение на Директивата за защитата на личния живот и електронните комуникации. Все пак предложеното изменение ще отстрани всички оставащи съмнения по въпроса и по този начин ще осигури по-голяма правна сигурност.

20. Разбира се, както бе посочено в предишно становище на ЕНОЗД относно устройствата за РЧИ ([1]), тази разпоредба не изключва евентуалната необходимост да се приемат допълнителни правни инструменти, доколкото това се отнася до РЧИ. Подобни мерки обаче следва да се приемат в друг контекст, а не като част от настоящото предложение.

ii) *Необходимост от включване на електронните съобщителни услуги в частни или получастни мрежи*

21. Макар ЕНОЗД да приветства направеното по-горе разяснение, той изразява съжаление, че предложението не разглежда въпроса с все по-замъглените граници между частните и публичните мрежи. Освен това ЕНОЗД изразява съжаление, че определението за услуги, включено в Директивата за защитата на личния живот и електронните комуникации, не обхваща и частните мрежи. Към настоящия момент член 3, параграф 1 от Директивата за защитата на личния живот и електронните комуникации се прилага единствено за *електронните съобщителни услуги в публичните мрежи*.

22. ЕНОЗД отбелязва тенденцията за все по-голяма смесване на частни и публични услуги. Такъв пример са университетите, където хиляди студенти могат да ползват интернет и e-mail. Възможността подобни полупублични (или получастни) мрежи да нарушат неприкосновеността на личния живот е очевидна и следователно се налага този тип услуги да са подчинени на същите правила, които важат и за изцяло публичните мрежи. Освен това, частните мрежи, като например мрежите на работодатели, осигуряващи на своите служители достъп до интернет, собствениците на хотели или апартаменти, които осигуряват на гостите ползване на телефон и e-mail, както и интернет кафетата, имат отражение върху защитата на личните данни и личния живот на своите потребители, от което следва, че те също трябва да са включени в обхвата на приложение на Директивата за защитата на личния живот и електронните комуникации.

23. В действителност, в практиката на някои държави-членки вече се е наложило прилагането на едни и същи задължения спрямо електронните съобщителни услуги, предоставяни в частни мрежи, и спрямо услугите, осигурявани в публичните мрежи ([2]). Също така, съгласно германското законодателство, становището на органите за защита на данните е, че ако дадена компания разрешава ползването на e-mail за частни нужди, то тя може да бъде възприета като оператор на публични телекомуникационни услуги и по този начин да попадне под действието на разпоредбите на Директивата за защитата на личния живот и електронните комуникации.

24. Накратко, нарастващото значение на смесените (частни/публични) и частни мрежи във всекидневния живот, със съответно нарастващия риск за личните данни и неприкосновеността на личния живот, оправдава необходимостта от прилагането към тези услуги на същия набор от правила, който се прилага и за публичните електронни съобщителни услуги. За тази цел ЕНОЗД смята, че директивата следва да бъде изменена, така че да включи в обхвата си този вид частни услуги; виждане, което се споделя от работна група „член 29“ ([3]).

II.2. **Уведомяване за нарушения на сигурността: изменение на член 4**

25. Член 4 от Директивата за защитата на личния живот и електронните комуникации, като се включват два нови параграфа (3 и 4), които определят задължение за уведомяване за нарушения на сигурността. Наистина, в съответствие с член 4, параграф 3 ДПЕСУПМ са задължени, от една страна, незабавно да уведомяват националните регулаторни органи за всяко нарушение на сигурността, което причинява случайно или неправомерно разрушаване, загуба, изменение, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или другояче обработват във връзка с предоставянето на електронни съобщителни услуги (наричано сборно „компрометиране на данни“); от друга страна ДПЕСУПМ са също така задължени да уведомяват своите клиенти.

([1]) Становище от 20 декември 2007 г. относно съобщението от Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно радиочестотната идентификация в Европа: стъпки към изграждане на политическа рамка COM(2007) 96.

([2]) Така например решението на апелативния съд в Париж по делото „*BNP Paribas* срещу *World Press Online*“, произнесено на 4 февруари 2005 г., гласи, че не съществува разлика между доставчиците на интернет услуги, които осигуряват достъп до интернет на търговска основа, и работодателите, които осигуряват достъп до интернет на своя персонал.

([3]) Становище 8/2006 относно прегледа на регулаторната рамка на ЕС за електронни съобщителни мрежи и услуги, което разглежда по-специално Директивата за защитата на личния живот и електронните комуникации, прието на 26 септември 2006 г.

Ползи от това задължение

26. ЕНОЗД приветства тези разпоредби (член 4 параграф 3 и 4 параграф 4), които въвеждат задължително уведомяване за нарушения на сигурността. Уведомяването за нарушения на сигурността има положителен ефект от гледна точка на защитата на личните данни и на личния живот, и това вече е установено в Съединените щати, където от няколко години има законодателство на държавно равнище относно уведомяването за нарушения.

27. На първо място законодателството относно уведомяването за нарушения засилва отчетността на ДПЕСУПМ по отношение на компрометираната информация. В съответствие с рамката на политиката за защита на личните данни и личния живот, „отчетност“ означава всяка организация да носи отговорност за информацията, която попада под нейните грижи и контрол. Задължението за уведомяване е равносилно на това да се заяви повторно, че от една страна компрометираните данни са били под контрола на ДПЕСУПМ и, от друга, че въпросната организация е отговорна за предприемането на необходимите мерки по отношение на тези данни.

28. На второ място уведомяването за нарушения на сигурността е утвърден фактор за подтикване на организациите, които обработват лични данни, да инвестират в сигурността. Самият факт, че се налага да се направи публично уведомление за нарушения на сигурността, подтиква организациите да прилагат повишени стандарти за сигурност, които защитават личната информация и предотвратяват нарушенията. Освен това уведомяването за подобни нарушения ще помогне за идентифицирането и провеждането на надежден статистически анализ по отношение на най-ефективните решения и механизми за сигурността. Отдавна съществува недостиг на потвърдени данни относно нарушенията на сигурността на информацията и най-подходящите технологии за защита на информацията. Този проблем може да бъде решен посредством задълженията за уведомяване за нарушенията на сигурността, както в случая със законодателството на САЩ относно докладването на нарушения на сигурността, тъй като чрез уведомяването ще се осигури информация за технологиите, които благоприятстват извършването на нарушения ([1]).

29. На последно място, уведомяването за нарушения на сигурността повишава осведомеността на лицата относно възможните рискове, свързани с компрометирането на техните лични данни, което им помага да предприемат необходимите мерки за ограничаване на въздействието на тези рискове. Така например, в случай на компрометиране на банкови данни, лицето, съответно уведомено за това, може да реши да промени своите данни за достъп до банковата си сметка, за да попречи на достъпа на друго лице до тази информация и използването ѝ за неправомерна цел (наричана обикновено „кражба на самоличност“). Най-общо казано, това задължение свежда до минимум вероятността физически лица да станат жертва на кражба на самоличност, като също така помага на жертвата да предприеме необходимите действия за разрешаване на проблемите.

Недостатък на предложеното изменение

30. Макар ЕНОЗД да е удовлетворен от включването на система за уведомяване за нарушения на сигурността в членове 4, параграф 3 и 4, параграф 4, той би приветствал прилагането им в по-широк мащаб, така че да се обхванат доставчиците на услуги на информационното общество. Това би означавало, че законодателството ще обхване и он-лайн банките, он-лайн предприятията, он-лайн доставчиците на здравни услуги и др. ([2]).

31. Основанията за налагане на задължение за уведомяване за нарушения на сигурността спрямо доставчиците на публични електронни съобщителни услуги, т.е. ДПЕСУПМ, са валидни и по отношение на други организации, които също обработват огромно количество лични данни, чието разкриване може да причини особено големи вреди на субектите на тези данни. Това обхваща он-лайн банките, брокерите на данни и други он-лайн доставчици като например тези, които обработват чувствителни данни (тук се включват здравни данни, политически възгледи и др.) Компрометирането на информация, собственост на он-лайн банки и он-лайн предприятия, която може да включва не само номера на банкови сметки, но и данни за кредитни карти, може да доведе до кражба на самоличност, като в този случай е от съществено значение лицата да бъдат уведомени, за да предприемат необходимите мерки. В случая с он-лайн здравните услуги, има вероятност лицата да понесат ако не финансови загуби, то със сигурност вреди, различни от икономическите, когато бъде компрометирана чувствителна информация.

([1]) Вж. доклад „*Икономика на сигурността и вътрешния пазар*“, изготвен от проф. Ross Anderson, Rainer Bцhme, Richard Clayton и Tyler Mooreот по поръчка на ENISA (Европейската агенция за мрежова и информационна сигурност). Докладът се намира на адрес:
http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Доставчиците на услуги на информационното общество са определени в Директивата за електронна търговия като услуга[и], нормално предоставяна[и] срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба на получателя на услугите.

32. Освен това, като се разшири обхватът на това задължение, описаните по-горе ползи, които се очакват в резултат на налагането на това задължение, няма да се ограничат до един сектор на дейност, а именно до доставчиците на публично достъпни електронни съобщителни услуги, а ще включат също така услугите на информационното общество като цяло. Наистина, налагането на подобни задължения за уведомяване спрямо услугите на информационното общество, като например он-лайн банките, не само ще увеличи тяхната отчетност, но също така ще мотивира доставчиците им да укрепят мерките си за сигурност и по този начин да избегнат потенциални нарушения на сигурността в бъдеще.

33. Съществуват и други прецеденти, при които Директивата за защитата на личния живот и електронните комуникации вече се прилага за образувания, различни от ДПЕСУПМ, като например член 5 относно поверителността на съобщенията и член 13 относно нежеланите съобщения (спам). Това потвърждава факта, че в миналото законодателят, съвсем благоразумно, е взел решение за разширяване на обхвата на приложението на някои разпоредби от Директивата за защитата на личния живот и електронните комуникации, тъй като го е счел за целесъобразно и необходимо. ЕНОЗД изразява надежда, че към настоящия момент законодателят няма да се поколебае да възприеме подобен разумен и гъвкав подход и да разшири обхвата на приложението на член 4 с цел да бъдат включени и услугите на информационното общество. За тази цел би било достатъчно в член 4, параграф 3 да се включи позоваване на доставчиците на услугите на информационното общество, както следва: „*В случай на нарушение на сигурността, което води до случайно или …, доставчикът на публично достъпните съобщителни услуги и доставчикът на услугите на информационното общество … уведомяват съответния абонат и националния регулаторен орган за това нарушение*“.

34. ЕНОЗД разглежда това задължение и неговото прилагане спрямо доставчиците на ДПЕСУПМ и на услугите на информационното общество като първа крачка от развитие, което в крайна сметка може да бъде прилагано към всички администратори на данни по принцип.

Специфична правна рамка за нарушения на сигурността, които следва да бъдат уреждани чрез процедурата на комитология

35. Предложението не разглежда редица въпроси, свързани със задължението за предоставяне на уведомление за нарушения на сигурността. Примери на въпроси, които трябва да бъдат разгледани, са обстоятелствата на уведомяване, приложимите формат и процедури. Вместо това член 4, параграф 4 от предложението предвижда тези решения да бъдат приети чрез комитет по комитология ([1]), а именно комитетът по съобщенията, създаден с член 22 от рамковата директива, в съответствие с решение на Съвета от 28 юни 1999 г. По-специално тези мерки ще бъдат приети в съответствие с член 5 от решението на Съвета от 28 юни 1999 г., което въвежда правила за процедурата по регулиране по отношение на „*мерки от общ характер, предназначени да прилагат съществени разпоредби от основни правни инструменти*“.

36. ЕНОЗД не се противопоставя на избора всички тези въпроси да бъдат уреждани от законодателството по прилагане. Приемането на законодателство чрез комитология може да съкрати законодателната процедура. Комитологията също така ще спомогне за постигането на хармонизиране, което следва непременно да бъде поставено за цел.

37. Като се има предвид големият брой въпроси, които ще е необходимо да бъдат уредени в мерките по прилагане, и тяхната уместност, както е подчертано по-долу, изглежда целесъобразно всички те да бъдат уредени чрез един законодателен акт, вместо с подход „на парче“, при който някои от въпросите ще бъдат обект на Директивата за защита на личните данни и електронните комуникации, а други — на законодателството по прилагане. Така че следва да се приветства подходът на Комисията, а именно тези решения да бъдат оставени на законодателството по прилагане, което следва да се приеме след консултация с ЕНОЗД и по възможност с другите заинтересовани страни (вж. точката по-долу).

Въпроси, които ще трябва да бъдат уредени чрез мерките по прилагане

38. Уместният характер на мерките по прилагане се подчертава от наличието на предварителна и в известна степен задълбочена представа за въпросите, които следва да бъдат уредени чрез тези мерки. Наистина, мерките по прилагане могат да определят стандартите, съгласно които трябва да бъде направено уведомяването. Така например те ще уточнят какво представлява нарушение на сигурността, условията, при които трябва да бъде направено уведомяването на физическите лица и на органите, както и срокът за това.

([1]) Законодателни процедури в ЕО, които включват комитети, съставени от представители на правителствата на държавите-членки на равнище държавни служители.

39. ЕНОЗД счита, че Директивата за защитата на личните данни и електронните комуникации и по-специално член 4 не следва да съдържат изключения от задължението за уведомяване. Във връзка с това ЕНОЗД е удовлетворен от подхода на Комисията, съдържащ се в член 4, който включва задължение за уведомяване и не предвижда изключение от него, но дава възможност този и други въпроси да бъдат уредени чрез законодателството по прилагане. Макар ЕНОЗД да е наясно с доводите, които биха обосновали въвеждането на някои изключения от задължението, ЕНОЗД предпочита този и други въпроси да бъдат внимателно разгледани чрез законодателството по прилагане, след старателно и мащабно обсъждане на всички належащи въпроси. Както е посочено по-горе, комплексният характер на въпросите, свързани със задължението за предоставяне на уведомление за нарушенията на сигурността, включително целесъобразният характер на изключенията или ограниченията, налагат това задължение да бъде третирано по уеднаквен начин, т.е. в един законодателен акт, който да урежда изключително този въпрос.

Консултация с ЕНОЗД и необходимост от разширяване на консултацията

40. Като се взема предвид степента, до която мерките за прилагане ще засегнат защитата на личните данни на физическите лица, важно е преди приемането на тези мерки Комисията да проведе подходяща консултация. По тази причина ЕНОЗД приветства член 4, параграф 4 от предложението, в който изрично се посочва, че преди приемането на мерки по прилагане, Комисията ще се консултира с Европейския надзорен орган по защита на данните. Тези мерки не само се отнасят до защитата на личните данни и личния живот на физическите лица, но и имат значително въздействие върху тях. Ето защо е важно да се проведе консултация с ЕНОЗД, съгласно член 41 от Регламент (ЕО) № 45/2001.

41. Освен консултация с ЕНОЗД, целесъобразно би било да се включи разпоредба, според която проектът за мерки по прилагане ще е обект на публична консултация, с оглед получаване на съвет и насърчаване на обмена на най-добри практики по тези въпроси. По този начин не само промишлеността, но и други заинтересовани страни, включително други органи за защита на данните и работна група „член 29“ ще се сдобият с подходящ канал за представяне на техните становища. Необходимостта от публична консултация се засилва от факта, че процедурата за приемане на законодателство е комитологията, при която Европейският парламент има ограничена намеса.

42. ЕНОЗД отбелязва, че член 4, параграф 4 от предложението предвижда Комисията да се консултира също така с Органа за пазара на електронни съобщения преди приемането на правила за прилагане. Във връзка с това ЕНОЗД се изразява в подкрепа на принципа за консултация с Органа за пазара на електронни съобщения като депозитар на опита и знанията на ENISA по отношение на въпроси, свързани с мрежите и информационното общество. До създаването на Орган за пазара на електронни съобщения би било целесъобразно в предложеното изменение (член 4, параграф 4) да се предвиди като временно решение консултация с ENISA.

II.3. **Разпоредба относно „бисквитки“ (*cookies*), софтуер за наблюдение (*spyware*) и други подобни устройства: изменение на член 5, параграф 3**

43. Член 5, параграф 3 от Директивата за защитата на личния живот и електронните комуникации разглежда въпроса за технологиите, които разрешават достъпа до информация и съхранението на информация в терминалното оборудване на потребителите посредством електронни съобщителни мрежи. Пример за прилагането на член 5, параграф 3 е използването на „бисквитки“ (*cookies*) ([1]). Други примери включват използването на технологии, като например *spyware* (програми за скрито наблюдение) и троянски коне (програми, скрити в съобщения или в друг наглед безвреден софтуер). Целта на тези технологии и цели се различава в голяма степен, тъй като, докато някои са напълно безвредни или дори полезни за потребителя, други са безспорно вредни и носещи заплаха.

([1]) „Бисквитките“ (*cookies*) се поставят от доставчиците на услуги на информационното общество (уебсайтове) в терминалното оборудване на потребителите за различни цели, включително за разпознаване на посетителя, когато той посети отново даден сайт. На практика, когато на даден интернет потребител се изпраща „бисквитка“ чрез уебсайт, компютърът на потребителя получава уникален номер (т.е. компютърът, който е получил „бисквитки“ от уебсайт А, става „притежател на компютър с бисквитка 111“). Уебсайтът съхранява този номер като референция. Ако потребителят на компютъра, който е получил „бисквитка“ 111, не изтрие файла с „бисквитката“, следващият път, когато посети същия уебсайт, този сайт ще е в състояние да идентифицира компютъра като притежателя на „бисквитка“ 111. По този начин уебсайтът стига до естественото заключение, че е бил посещаван и преди. Механизмът, позволяващ на даден уебсайт да разпознае съответния компютър като повторен посетител, е елементарен. Когато посещаващият компютър притежава „бисквитки“, като например „бисквитка“ 111, и посещава сайта, който при предишно посещение е създал „бисквитката“, той ще провери твърдия диск на потребителя за файловия номер на „бисквитката“. Ако браузърът на потребителя открие файл с „бисквитка“, който съответства на референтния номер, съхраняван от уебсайта, той уведомява уебсайта, че потребителят притежава „бисквитка“ 111.

44. Член 5, параграф 3 от Директивата за защитата на личния живот и електронните комуникации определя условията, които се прилагат при получаване на достъп до или съхранение на информация на терминалното оборудване на потребителите, при което, наред с други неща, се използват технологиите, споменати по-горе. По-специално, в съответствие с член 5, параграф 3: i) на интернет потребителите трябва да се предоставя ясна и изчерпателна информация в съответствие с Директива 95/46/ЕО, *inter alia* относно целите на обработката; както и ii) на интернет потребителите трябва да бъде разрешено да откажат подобна обработка, т.е. да имат право на освобождаване от обработката на информация, извличана от тяхното терминално оборудване.

Ползи от предложеното изменение

45. Съществуващият член 5, параграф 3 от Директивата за защитата на личния живот и електронните комуникации ограничава обхвата на приложението до ситуации, при които достъпът до информация и съхранението на информация в терминалното оборудване на потребителите се извършват посредством *електронни съобщителни мрежи*. Това включва гореописаната ситуация по отношение на използването на „бисквитки“ (*cookies*), както и други технологии, като софтуер за наблюдение (*spyware*), доставяни посредством електронни съобщителни мрежи. Съвсем не е ясно обаче дали член 5, параграф 3 се прилага в ситуации, при които подобни технологии („бисквитки“/софтуер за наблюдение и други подобни) се разпространяват чрез програма, осигурена на външни носители за съхранение на данни, и са свалени в терминалното оборудване на потребителите. Предвид това, че заплахата за неприкосновеността на личния живот съществува независимо от съобщителния канал, ограничението на член 5, параграф 3 до един единствен съобщителен канал е доста неприятно.

46. Ето защо ЕНОЗД е удовлетворен от изменението на член 5, параграф 3, което разширява обхвата на приложението на член 5, параграф 3, като премахва позоваването на „електронни съобщителни мрежи“. Наистина, измененият вариант на член 5, параграф 3 обхваща както ситуации, при които достъпът до информация и съхранението на информация в терминалното оборудване на потребителите се извършва посредством електронни съобщителни мрежи, така и ситуации, при които се използват други външни носители за съхранение на данни, като компактдискове, CD-ROM, устройства за съхранение с USB интерфейс и др.

Техническо съхранение с цел улесняване на преноса

47. Последното изречение на член 5, параграф 3 от Директивата за защитата на личния живот и електронните комуникации остава непроменено в нейната изменена версия. В съответствие с последното изречение, изискванията на първото изречение от член 5, параграф 3 „… *не пречат на техническото съхранение или достъп с единствена цел осъществяване или улесняване на предаването на съобщение през електронна съобщителна мрежа или само по необходимост, за да се предостави услуга на информационното общество* …“ По този начин задължителните правила на първото изречение от член 5, параграф 3 (необходимостта да се предоставя информация и да се дава възможност за отказ) няма да се прилагат, когато достъпът до терминалното оборудване на потребителя или съхранението на информация е с единствена цел *улесняване* на предаването или само по необходимост, за да се предостави услуга на информационното общество, поискана от потребителя.

48. Директивата не описва в кои случаи достъпът или съхранението на информация има за единствена цел улесняване на предаването или предоставяне на информация. Една ситуация, която безспорно би била обхванатата от това изключение, е осъществяването на интернет връзка. Причината за това е, че за да бъде осъществена интернет връзка, е необходимо да се придобие IP адрес ([1]). Компютърът на крайният потребител ще бъде помолен да разкрие на доставчика на интернет достъп определена информация за себе си, а в замяна доставчикът ще му осигури IP адрес. В този случай информацията, съхранявана в терминалното оборудване на крайния потребител, ще бъде прехвърлена към доставчика на интернет достъп с цел предоставяне на потребителя на достъп до интернет. В този случай доставчикът на интернет достъп е освободен както от задължението да обяви това събиране на информация, така и от това да осигури правото на отказ, доколкото то е необходимо за предоставяне на услугата.

49. Веднъж свързан към интернет, ако потребителят желае достъп до определен уебсайт, той трябва да изпрати искане до сървъра, където се помещава уебсайтът. Последният изпраща отговор, ако знае къде да изпрати информацията, т.е. ако знае IP адреса на потребителя. Предвид начина на съхранение на този адрес, отново се налага уебсайтът, който потребителят желае да посети, да има достъп до информацията на терминалното оборудване на интернет потребителите. Очевидно е, че тази операция също би попаднала в обхвата на изключението. В тези случаи изглежда целесъобразно тя да остане извън обхвата на приложение на изискванията на член 5, параграф 3.

([1]) IP адрес (интернет протокол адрес) е уникален адрес, използван от определени електронни устройства с цел идентифициране и комуникация помежду им в компютърна мрежа, която използва стандарта интернет протокол (IP) — по-просто казано, компютърен адрес. Всяко едно участващо мрежово устройство — в това число рутери, комутатори, компютри, инфраструктурни сървъри (напр. NTP, DNS, DHCP, SNMP, и др.), принтери, интернет факс машини и някои телефони — може да има свой собствен адрес, който е уникален в рамките на конкретната мрежа. Някои IP адреси са предназначени да бъдат уникални в рамките на глобалния интернет, докато други се налага да бъдат уникални единствено в рамките на дадено предприятие.

50. ЕНОЗД счита за целесъобразно да се направи изключение от необходимостта за информиране и предоставяне на възможност за отказ, както е описано по-горе, когато *се налага* техническо съхранение или достъп до терминалното оборудване на потребителя с единствена цел предаване на съобщение по електронна съобщителна мрежа. Същото важи и в случая, когато техническото съхранение или достъпът се налага само по необходимост, за да се предостави услуга на информационното общество. ЕНОЗД обаче не вижда необходимост от задължението за предоставяне на информация и възможност за отказ да се изключи правото на отказ в случаите, когато техническото съхранение или достъп има за цел единствено *улесняване* на предаването на съобщение. Така например, в съответствие с последното изречение от този член, даден субект на данни може да не се възползва от информация и от правото да се противопостави на обработката на данните си, ако „бисквитката“ набере информация за неговите езикови предпочитания или местоположение (напр. Белгия, Китай), тъй като целта на тези „бисквитки“ може да бъде представена като улесняване на предаването на съобщение. ЕНОЗД осъзнава, че на равнище софтуер на практика се дава възможност на субектите на данни да откажат или променят съхранението на „бисквитки“. Това обаче не е подкрепено в достатъчно ясна степен от правна разпоредба, която би дала официално право на субекта на данните да защити правата си в гореописания контекст.

51. За да се избегне подобно развитие, ЕНОЗД предлага да се направи незначително изменение на последната част от член 5, параграф 3, състоящо се в заличаването на думата „улесняване“ от изречението: „… *не пречат на техническото съхранение или достъп с единствена цел осъществяване или улесняване на предаването на съобщение през електронна съобщителна мрежа или само по необходимост, за да се предостави услуга на информационното общество* …“.

II.4. **Правни действия, предприети от ДПЕСУПМ и юридически лица: добавяне на параграф 6 към член 13**

52. Предложеният член 13, параграф 6 предвижда гражданскоправни средства за защита за всяко физическо или юридическо лице със законен интерес, в частност за доставчици на електронни съобщителни услуги, които имат стопански интерес да водят борба с нарушителите на член 13 от Директивата за защитата на личния живот и електронните комуникации. Този член разглежда изпращането на нежелани търговски съобщения.

53. Предложеното изменение ще позволи например на доставчиците на интернет достъп да предприемат действия по отношение на разпространителите на нежелани съобщения заради злоупотреба с техните мрежи, да съдят образувания, фалшифициращи адреси на податели или незаконно проникващи в сървъри с цел използването им като предаватели на нежелани съобщения и пр.

54. Директивата за защитата на личния живот и електронните комуникации остави неяснота по въпроса дали ДПЕСУПМ имат право на действия срещу разпространителите на нежелани съобщения и случаите на ДПЕСУПМ, завели съдебни дела за нарушение на член 13, както е въведен в законодателството на държавите-членки, са единични. ([1]). Като отчита основанието на доставчиците на електронни съобщителни услуги да защитават своите стопански интереси, предложението потвърждава, че директивата за защитата на личния живот и електронните комуникации има за цел не само защита на физическите лица абонати, но също така на доставчиците на електронни съобщителни услуги.

55. ЕНОЗД изразява задоволство, че предложението предоставя възможност на доставчиците на електронни съобщителни услуги, които имат стопански интерес, да завеждат дела срещу разпространителите на нежелани съобщения. Освен при изключителни обстоятелства физическите лица абонати нямат нито паричните средства, нито стимула да предприемат такива съдебни действия. Обратно, доставчиците на интернет достъп и другите ДПЕСУПМ притежават финансовата сила и технологичния капацитет да разследват кампании по разпространяване на нежелани съобщения и да откриват извършителите и е съвсем уместно да имат правото да предявяват съдебни искове срещу разпространителите на нежелани съобщения.

56. ЕНОЗД цени особено предложеното изменение, доколкото то също така би позволило на потребителски асоциации и профсъюзи, представляващи интересите на потребителите, обект на нежелани съобщения, да предявяват искове от тяхно име в съда. Както беше посочено по-горе, вредата, нанесена на един обект на данни, получател на нежелани съобщения, взета сама за себе си, обикновено не е достатъчна за предявяване на иск в съда. Всъщност, ЕНОЗД вече предложи тази мярка по отношение на нарушенията

([1]) Такъв случай е делото Корпорация Microsoft срещу Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

на правото на неприкосновеност на личния живот и защита на данните в най-общ смисъл в своето становище относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни ([1]). ЕНОЗД счита, че предложението би могло да отиде още по-нататък, предлагайки колективни действия, даващи право на групи от граждани колективно да се отнесат до съд по въпроси относно защитата на личните данни. В случая с нежеланите съобщения, когато голям брой лица получават такива съобщения, съществува възможността групи лица да се обединят и да предявят колективен иск срещу разпространителите на нежелани съобщения.

57. ЕНОЗД изразява особено съжаление, че в предложението възможността на юридическите лица да предявяват искове е ограничена до случаи, в които има нарушение на член 13 от директивата, т.е. случаи на нарушение на разпоредбата относно нежелани съобщения чрез електронна поща. Наистина, според предложеното изменение юридическите лица не биха могли да предприемат съдебни действия при нарушение на останалите разпоредби на Директивата за защитата на личния живот и електронните комуникации. Така например, сега действащата разпоредба не позволява на юридическо лице, като потребителска асоциация, да предприеме съдебни действия срещу доставчик на интернет достъп, който е разкрил лични данни на милиони потребители. Привеждането в изпълнение на Директивата за защитата на личния живот и електронните комуникации би се подобрило като цяло, а не само по отношение на определен член, ако разпоредбата на член 13, параграф 6 беше обща, така че да позволи на юридическите лица да предприемат съдебни действия при нарушение на която и да било разпоредба на тази директива.

58. Като решение на този проблем ЕНОЗД предлага обособяването на член 13, параграф 6 в самостоятелен член (член 14). Освен това формулировката на член 13, параграф 6 следва да претърпи леко изменение: Вместо „*съгласно настоящия член*“ тя следва да гласи: „съгласно настоящата директива“.

II.5. **Укрепване на разпоредбите за прилагане: добавяне на член 15а**

59. Директивата за защитата на личния живот и електронните комуникации не съдържа изрични разпоредби за прилагане. Вместо това тя се позовава на раздела за прилагане от Директивата за защита на личните данни ([2]). ЕНОЗД приветства новия член 15а от предложението, който изрично разглежда въпроси за прилагането по тази директива.

60. На първо място ЕНОЗД отбелязва, че една ефективна политика за прилагане в тази област предполага, съгласно изискванията по предлагания член 15а, параграф 3, че националните органи имат правомощия за разследване с цел събиране на необходимата информация. Много често доказателствата за нарушение на разпоредбите на Директивата за защитата на личния живот и електронните комуникации имат електронен характер и могат да бъдат съхранявани на различни компютри и устройства или мрежи. В този смисъл е важно правоприлагащите органи да имат възможността да се получават заповеди за обиск, даващи им правомощия за влизане, претърсване и конфискуване.

61. На второ място ЕНОЗД приветства особено предложеното изменение, т.е. член 15а, параграф 2, съгласно който националните регулаторни органи трябва да имат правомощията да издават съдебни забрани, т.е. преустановяване на нарушенията, както и да разполагат с необходимите правомощия и ресурси за разследване. Националните регулаторни органи, в това число националните органи за защита на данните, следва да имат правомощията да налагат съдебни забрани, възпиращи нарушителите да продължат дейност, която е в нарушение на Директивата за защитата на личния живот и електронните комуникации. Съдебните забрани или правомощието за издаване на заповед за преустановяване на нарушение са полезен инструмент при продължаващи действия в нарушение на правата на лицата. Съдебните забрани ще бъдат много полезни за преустановяване на нарушения на Директивата за защитата на личния живот и електронните комуникации, като например нарушението на член 13 относно нежеланите търговски съобщения, което по своята същност е продължаващо действие.

62. Трето, предложението позволява на Комисията да въвежда технически мерки за прилагане, за да се гарантира ефективно трансгранично сътрудничество при прилагането на националните закони (предложено изменение член 15а, параграф 4). Досегашният опит в сътрудничеството включва споразумението по предложение на Комисията за установяване на обща процедура за уреждане на трансгранични жалби, свързани с нежелани съобщения.

([1]) Становище на Европейския надзорен орган по защита на данните относно Съобщението на Комисията до Европейския парламент и до Съвета относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на личните данни (ОВ C 255, 27.10.2007 г., стр. 1).

([2]) 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.

63. ЕНОЗД смята, че ако законодателството помага на регулаторите да съдействат на съответните органи в други държави, то несъмнено ще съдейства за трансграничното правоприлагане. Следователно е целесъобразно предложението да даде на Комисията възможност да създаде условия за гарантиране на трансгранично сътрудничество, включително процедури за споделяне на информация.

III. ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ

64. ЕНОЗД горещо приветства предложението. Предложените изменения укрепват защитата на личния живот и личните данни на лицата в сектора на електронните комуникации и това се прави ненатрапчиво, без да се създава неоправдана или ненужна тежест за организациите. По-конкретно ЕНОЗД счита, че в по-голямата си част предложените изменения не следва да се изменят, доколкото те изпълняват своята цел. В точка 69 по-долу са изброени измененията, които ЕНОЗД се надява да останат непроменени.

65. Без да се пренебрегва цялостното положително отношение към предложението, ЕНОЗД счита, че някои от измененията следва да бъдат подобрени, за да се гарантира ефективно предоставяне на подходяща защита на личните данни и личния живот на лицата. Това важи особено за разпоредбите относно уведомяването за нарушения на сигурността, както и за тези, уреждащи правните действия, предприемани от доставчиците на електронни съобщителни услуги при нарушение на разпоредбите за нежелани съобщения. В допълнение ЕНОЗД изразява съжаление, че в предложението не са застъпени някои въпроси, които не са подобаващо уредени в сегашната Директива за защитата на личния живот и електронните комуникации, като така се пропуска възможността чрез настоящото преразглеждане да се уредят нерешените въпроси.

66. За разрешаването на двата проблема, т.е. въпроси, които не са подобаващо разгледани в предложението или такива, които изобщо не са застъпени, в настоящото становище се правят няколко предложения. Точки 67 и 68 обобщават проблемите и предлагат специфична формулировка. ЕНОЗД призовава законодателя да ги вземе предвид в хода на придвижването на предложението през законодателния процес.

67. Съдържащите се в предложението изменения, във връзка с които ЕНОЗД горещо се застъпва за изменение, са, както следва:

i) **Уведомяване при нарушение на сигурността**: съгласно формулировката предложеното изменение, добавящо *член 4, параграф 4*, се прилага за доставчиците на електронни съобщителни услуги (доставчици на интернет достъп, оператори на мрежи), които за задължени да уведомяват националните регулаторни органи и клиентите си при нарушение на сигурността. ЕНОЗД напълно подкрепя това задължение. При все това ЕНОЗД счита, че задължението трябва да се отнася и за доставчиците на услуги на информационното общество, които често обработват лична информация от деликатно естество. По този начин он-лайн банките и застрахователите, он-лайн доставчиците на здравни услуги и всяка друга стопанска дейност, осъществявана он-лайн, също ще трябва да спазват това задължение.

За тази цел ЕНОЗД предлага в член 4, параграф 3 да се добави упоменаване на доставчиците на услуги на информационното общество, както следва: „*В случай на нарушение на сигурността … доставчикът на публично достъпни съобщителни услуги и доставчикът на услуги на информационното общество, ще … уведомят засегнатия абонат и националния регулаторен орган за това нарушение*“.

ii) **Правни действия, предприети от ДПЕСУПМ**: съгласно формулировката предложеното изменение, добавящо член 13, параграф 6, предвижда гражданскоправни средства за защита на всяко физическо или юридическо лице, в частност за доставчици на електронни съобщителни услуги, за борба с нарушенията по член 13 от Директивата за защитата на личния живот и електронните комуникации, който урежда въпроса с нежеланите съобщения. ЕНОЗД е удовлетворен от тази разпоредба. Въпреки това ЕНОЗД не вижда основание тази нова способност да бъде ограничена да нарушенията по член 13. ЕНОЗД предлага на юридическите лица да бъде предоставена възможност да предприемат правни действия при нарушение на разпоредбите на Директивата за защитата на личния живот и електронните комуникации.

За постигането му ЕНОЗД предлага обособяването на член 13, параграф 6 в самостоятелен член (член 14). В допълнение формулировката на член 13, параграф 6 следва да претърпи леки изменения: Вместо „съгласно настоящия член“ следва да гласи „съгласно настоящата директива“.

68. Обхватът Директивата за защитата на личния живот и електронните комуникации, който понастоящем е ограничен до доставчиците на публични електронни комуникационни мрежи, е един от бъдещите тревога въпроси, които не са разгледани в предложението. ЕНОЗД счита, че директивата следва да бъде изменена с цел разширяване на обхвата ѝ, за да включи и доставчиците на електронни комуникационни услуги в смесените (частни/публични) и частни мрежи.

69. Измененията, които ЕНОЗД горещо препоръчва да останат непроменени, са, както следва:

i) **Радиочестотна идентификация (РЧИ)**: предложеното изменение на *член 3*, според което електронните комуникационни мрежи включват *„публични комуникационни мрежи, поддържащи събирането на данни и устройства за идентифициране“* е напълно задоволително. Тази разпоредба е много положителна, тъй като внася яснота, че редица приложения на РЧИ трябва да бъдат в съответствие с Директивата за защитата на личния живот и електронните комуникации, като по този начин се премахва известна правна несигурност в това отношение.

ii) **„Бисквитки“/софтуер за наблюдение (*spyware*)**: предложеното изменение на *член 5, параграф 3* заслужава да бъде приветствано, защото по този начин задължението за информиране и предоставяне на правото да не се позволява съхранението на „бисквитки“/софтуер за наблюдение в собственото терминално оборудване ще се прилага и при поставянето на такива устройства посредством външни средства за съхранение на данни като CD-ROM, устройства за съхранение с USB интерфейс. Въпреки това ЕНОЗД предлага в последната част на член 5, параграф 3 да бъде направено незначително изменение, състоящо се в заличаването на думата „улесняване“ от изречението.

iii) **Избор на комитология с консултация с ЕНОЗД и условия/ограничения на задължението за уведомяване**: предложеното изменение за добавяне на член 4, параграф 4 във връзка с уведомяването при нарушение на сигурността оставя на комитологията, след поискване на съвет от ЕНОЗД, решението по комплексни въпроси относно обстоятелствата/формата/процедурите на системата за уведомяване при нарушение на сигурността. ЕНОЗД горещо подкрепя този единен подход. Законодателството относно уведомяването при нарушение на сигурността е отделна област, която трябва да бъде уредена след внимателно обсъждане и анализ.

Свързано с този въпрос е искането на някои заинтересовани страни да се предвидят изключения от задължението за уведомяване при нарушение на сигурността в член 4, параграф 4. ЕНОЗД се противопоставя остро на този подход. ЕНОЗД застъпва позицията, че цялостният въпрос за уведомяването, как да се извършва то, при какви обстоятелства може да бъде съкратено или по някакъв начин ограничено, трябва да бъде анализиран задълбочено след провеждане на съответно разискване.

iv) **Прилагане**: предложеното изменение за добавяне на *член 15а* съдържа много полезни елементи, които трябва да бъдат запазени и които ще допринесат за гарантиране на ефективно спазване, включително укрепването на правомощията за разследване на националните регулаторни органи (член 15а, параграф 3) и предоставянето на правомощия на националните регулаторни органи да издават заповед за преустановяване на нарушенията.

Съставено в Брюксел на 10 април 2008 г.

Peter HUSTINX

Европейски надзорен орган по защита на данните