Второ становище на Европейския надзорен орган по защита на данните относно прегледа 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)

(2009/C 128/04)

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,

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,

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

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

Контекст

1. На 13 ноември 2007 г. Европейската комисия прие предложение за изменение, наред с други, на Директивата относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, обикновено наричана Директива за правото на неприкосновеност на личния живот и електронни комуникации [1] (оттук-нататък „предложение“ или „предложение на Комисията“). На 10 април 2008 г. ЕНОЗД прие становище относно предложението на Комисията, в което предостави препоръки за подобряване на предложението, за да се гарантира, че предложените промени ще осигурят възможно най-добра защита на правото на неприкосновеност на личния живот и лични данни на лицата („Първо становище на ЕНОЗД“) [2].

2. ЕНОЗД приветства предложеното от Комисията създаване на система за задължително уведомяване за нарушения на сигурността, което изисква компаниите да уведомяват лицата, ако личните им данни са били изложени на риск. Освен това, ЕНОЗД приветства новата разпоредба, позволяваща на юридически лица (напр. потребителски асоциации и доставчици на интернет услуги) да предприемат съдебни действия срещу разпространители на нежелани съобщения с цел по-нататъшно укрепване на съществуващите инструменти за борба с нежеланите съобщения.

3. По време на парламентарните обсъждания, предшестващи първото четене в Европейския парламент, ЕНОЗД предложи допълнителни съвети чрез оповестяването на бележки по определени въпроси, посочени в докладите, изготвени от комисиите на Европейския парламент, в чиято компетентност е преразглеждането на Директивите за универсалната услуга [3] и на Директивата за правото на неприкосновеност на личния живот и електронните комуникации („Бележки“) [4]. В бележките бяха разгледани основно въпроси, свързани с обработката на данни за трафик и закрилата на правата върху интелектуалната собственост.

4. На 24 септември 2008 г. Европейският парламент (ЕП) прие законодателна резолюция относно Директивата за правото на неприкосновеност на личния живот и електронни комуникации („първо четене“) [5]. ЕНОЗД оцени

[1] Преразглеждането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации е част от един по-широк процес на преразглеждане, целящ създаването на орган на ЕС за далекосъобщенията, преразглеждане на директиви 2002/21/ЕО, 2002/19/ЕО, 2002/20/ЕО, 2002/22/ЕО и 2002/58/ЕО, и е-разглеждане на Регламент (ЕО) № 2006/2004 (по-нататък съвкупно „преразглеждане на пакета за телекомуникации“).

[2] Становище от 10 април 2008 г. относно предложението 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 (Директива за правото на неприкосновеност на личния живот и електронни комуникации), ОВ C 181, 18.7.2008 г., стр. 1.

[3] Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги (Директива за универсалната услуга), ОВ L 108, 24.4.2002 г., стр. 51.

[4] Бележки на ЕНОЗД по определени въпроси, посочени в доклада на комисията по вътрешния пазар и защита на потребителите на Европейския парламент относно преразглеждането на Директива 2002/22/ЕО (универсална услуга) и Директива 2002/58/ЕО (право на неприкосновеност на личния живот и електронни комуникации, 2 септември 2008 г. Може да се намери на интернет адрес: www.edps.europa.eu

[5] Законодателна резолюция на Европейския парламент от 24 септември 2008 г. относно предложението 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, 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 (COM(2007) 698 — C6-0420/2007 — 2007/0248(COD).

положително няколко от измененията на ЕП, които бяха приети след посочените по-горе становище и бележки на ЕНОЗД. Сред важните промени беше включването на доставчици на услуги на информационното общество (т.е. компании, опериращи в интернет) в обхвата на задължението за уведомяване за нарушения на сигурността. ЕНОЗД приветства и изменението, позволяващо на юридически и физически лица да подават иск за нарушение на разпоредба на Директивата за неприкосновеност на личния живот и електронни комуникации (а не само за нарушение на разпоредбите относно нежеланите съобщения, както беше първоначално посочено в предложението на Комисията). Първото четене в Европейския парламент беше последвано от приемането от Комисията на изменено предложение относно директивата за неприкосновеност на личния живот и електронни комуникации (по-нататък „изменено предложение“) ([6]).

5. На 27 ноември 2008 г. Съветът постигна политическо споразумение за преразглеждане на правилата за пакета за телекомуникациите, включително Директивата за неприкосновеност на личния живот и електронни комуникации, което ще приеме вид на обща позиция на Съвета („обща позиция“) ([7]). В съответствие с член 251, параграф 2 от Договора за създаване на Европейската общност ЕП ще бъде нотифициран за общата позиция, което може да доведе до предложение за изменения от страна на ЕП.

Общи бележки по позицията на Съвета

6. Съветът измени съществени елементи от текста на предложението и не прие много от приетите от ЕП изменения. Макар общата позиция определено да съдържа положителни елементи, като цяло ЕНОЗД е загрижен от съдържащото се в нея, по-специално тъй като общата позиция не включва някои от положителните изменения, предложени от ЕП, измененото предложение или становищата на ЕНОЗД и на европейските органи по защита на данните, оповестени чрез работна група „Член 29“ ([8]).

7. Тъкмо обратното, в редица случаи разпоредби в измененото предложение и измененията на ЕП, осигуряващи гаранции на гражданите, са заличени или значително отслабени. Вследствие, предлаганото на лицата ниво на защита в общата позиция е значително отслабено. Поради тези причини ЕНОЗД сега издава второ становище с надеждата, че в хода на придвижване на Директивата за неприкосновеност на личния живот и електронни комуникации в законодателния процес, ще бъдат приети нови изменения, които ще възстановят гаранциите за защита на данните.

8. Настоящото второ становище разглежда някои основни поводи за безпокойство и не повтаря вече направените в първото становище на ЕНОЗД или в бележките коментари, които остават в сила. По-конкретно, настоящото становище разглежда следните въпроси:

— разпоредбите относно уведомяване за нарушения на сигурността,

— обхватът на приложение на Директивата за неприкосновеност на личния живот и електронни комуникации спрямо частни и публично достъпни частни мрежи,

— обработката на данни за трафик за целите на сигурността,

— възможността юридически лица да предприемат правни действия при нарушения на Директивата за неприкосновеност на личния живот и електронни комуникации.

9. При разглеждането на посочените по-горе въпроси в настоящото становище се прави анализ на общата позиция на Съвета, която се сравнява с първото четене в ЕП и измененото предложение на Комисията. Становището съдържа препоръки, целящи рационализиране на разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации и гарантиращи, че тя и занапред ще защитава адекватно правото на неприкосновеност на личния живот и личните данни на лицата.

II. **РАЗПОРЕДБИТЕ ОТНОСНО УВЕДОМЯВАНЕ ЗА НАРУШЕНИЯ НА СИГУРНОСТТА**

10. ЕНОЗД подкрепя приемането на система за задължително уведомяване за нарушения на сигурността, съгласно която органите и лицата ще бъдат уведомявани, ако личните им данни са били изложени на риск ([9]). Уведомяването за нарушения на сигурността може да помогне на лицата да предприемат необходимите стъпки за смекчаване на евентуалните вреди, породени от излагането на риск. Освен това, задължението за изпращане на уведомяване за нарушения на сигурността ще насърчи компаниите да подобрят сигурността на данните и ще засили отчетността им по отношение на личните данни, за които носят отговорност.

11. Измененото предложение на Комисията, първото четене в Европейския парламент и общата позиция на Съвета представляват три различни подхода към уведомяването за нарушения на сигурността, които понастоящем са предмет на разглеждане. Всеки от трите подхода има положителни страни. При все това ЕНОЗД счита, че във всеки от подходите могат да се внесат подобрения и съветва при обмислянето на последните стъпки към приемане на системата за нарушения на сигурността да се вземат предвид направените по-долу препоръки.

([6]) Изменено 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, 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, 6.11.2008 г., COM (2008) 723 окончателен.

([7]) На разположение на публичния уебсайт на Съвета.

([8]) Становище 2/2008 относно преразглеждането на Директива 2002/58/ЕО относно правото на неприкосновеност на личния живот и електронни комуникации, което може да се намери на уебсайта на работна група „Член 29“.

([9]) Използваната в настоящото становище формулировка „изложени на риск“ означава пробив в личните данни, възникнал в резултат на случайно или незаконно унищожаване, загуба, промяна, неупълномощено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

12. В анализа на трите системи за уведомяване за нарушения на сигурността трябва да се обсъдят пет основни въпроса: *i)* определението за нарушение на сигурността; *ii)* образуванията, обхванати от задължението за уведомяване („обхванати образувания“); *iii)* стандартът, който задейства задължението за уведомяване; *iv)* установяване на образуването, което преценява дали определено нарушение на сигурността отговаря на стандарта или не, и *v)* получатели на уведомяването.

Преглед на подходите на Комисията, Съвета и ЕП

13. Европейският парламент, Комисията и Съветът приеха различни подходи за уведомяване за нарушения на сигурността. По време на първото четене в ЕП бяха направени промени в изложената в предложението на Комисията първоначална система за уведомяване за нарушения на сигурността ([10]). Съгласно подхода на ЕП задължението за уведомяване се прилага не само спрямо доставчици на обществено достъпни електронни съобщителни услуги, но и по отношение на доставчици на услуги на информационното общество („ДОДЕСУ“ и „ДУИО“). Освен това, съгласно въпросния подход националният регулаторен орган или компетентните органи (съвместно „органите“) трябва да бъдат уведомявани за всяко нарушаване на личните данни. Ако органите установят, че нарушението е *сериозно*, те ще изискват ДОДЕСУ и ДУИО да уведомят засегнатото лице без забавяне. В случай на нарушения, които представляват неминуема и пряка опасност, ДОДЕСУ и ДУИО уведомяват лицата, преди да уведомят органите, и не изчакват регулаторно решение. Изключение от задължението за уведомяване на потребителите обхваща образувания, които могат да удостоверят пред органите, че *„са използвани подходящи технически мерки за защита“*, които правят данните неразбираеми за лице, което няма право на достъп до тях.

14. Съгласно подхода на Съвета, уведомяване трябва да се изпрати както на абонатите, така и на органите, но само в случаите, когато *обхванатото образувание* счита, че нарушението представлява *сериозен риск* за неприкосновеността на личния живот на абоната (т.е. кражба или фалшифициране на самоличност, физическа вреда, значително накърняване на достойнството или репутацията).

15. Измененото предложение на Комисията запазва въведеното от ЕП задължение за уведомяване на органите за всяко нарушение. Същевременно, за разлика от подхода на ЕП, измененото предложение съдържа изключение от изискването за уведомяване на засегнатите лица, когато ДОДЕСУ доказва пред компетентния орган, че *i)* *„има малка вероятност“* да възникне вреда (напр. икономически загуби, социални вреди или кражба на самоличност) вследствие на нарушението или *ii)* са предприети *„подходящи технологични мерки за защита“* на засегнатите от нарушението данни. Така, подходът на Комисията включва основан на щетите анализ във връзка с индивидуалното уведомяване.

16. Важно е да се отбележи, че съгласно подходите на ЕП ([11]) и Комисията в крайна сметка тъкмо *органите* отговарят за това да се определи дали нарушението е сериозно или има вероятност да причини вреди. За сравнение, в подхода на Съвета решението се взема от *засегнатите образувания*.

17. Както подходът на Комисията, така и този на Съвета се прилагат само спрямо ДОДЕСУ, а не, както в подхода на ЕП, спрямо ДУИО.

Определението за нарушение на сигурността

18. ЕНОЗД отбелязва с радост, че трите законодателни предложения съдържат едно и също определение за уведомяването за нарушения на сигурността, което е описано като *„нарушение на сигурността, водещо до случайното или незаконно унищожаване, загуба, промяна, неупълномощено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин [...]“* ([12]).

19. Както е посочено по-долу, това определение се приветства, доколкото то е достатъчно широко, за да обхване повечето ситуации, които биха могли да дадат основания за уведомяване за нарушения на сигурността.

20. На първо място, определението включва случаи на *неупълномощен достъп* до лични данни на трета страна, като например незаконното проникване в сървър, съдържащ лични данни, и извличането на тази информация.

21. На второ място, това определение включва и ситуации на загуба или разкриване на лични данни при все още недоказан неупълномощен достъп. Това включва ситуации като евентуална загуба на лични данни (напр. CD-ROM, устройства за съхранение на данни с USB интерфейс и други преносими устройства), или превръщането им в обществено достояние от редовни потребители (файлове с данни на служители, които са непреднамерено и временно на разположение в публично достъпна област чрез интернет). Тъй като често ще липсват доказателства, че тези данни могат или не, в определен момент, да бъдат достъпни за неупълномощени трети страни или използвани от тях, уместно е тези случаи да бъдат включени в обхвата на определението. ЕНОЗД следователно препоръчва да се запази това определение. Освен това ЕНОЗД препоръчва определението за нарушение на сигурността да се включи в член 2 от Директивата за неприкосновеност на личния живот и електронни комуникации, тъй като това би било в съответствие с общата структура на директивата и би внесло по-голяма яснота.

([10]) По-конкретно този въпрос е разгледан в изменения 187, 124—127, както и 27, 21 и 32 на ЕП.

([11]) Освен в случай на неминуема и пряка опасност, когато обхванатите образувания трябва първо да уведомят потребителите.

([12]) Член 2, буква и) от общата позиция и измененото предложение и член 3.3 от първото четене в ЕП.

Образувания, които следва да бъдат обхванати от задължението за уведомяване

22. Съгласно подхода на ЕП задължението за уведомяване се прилага спрямо ДОДЕСУ и ДУИО. Същевременно, в системите на Съвета и Комисията само ДОДЕСУ като телекомуникационни компании и доставчици на достъп до интернет ще бъдат задължени да уведомяват лицата, когато са пострадали от нарушения на сигурността, които водят до излагане на личните данни на риск. Други сектори на дейност, например банки онлайн, търговци на дребно онлайн, онлайн доставчици на здравни услуги и други не са обхванати от това задължение. Поради посочените по-долу причини ЕНОЗД счита, че в контекста на публичните политики от решаващо значение е да се гарантира, че изискването за уведомяване обхваща и услугите на информационното общество, сред които търговска дейност онлайн, банки онлайн, онлайн доставчици на здравни услуги и други.

23. На първо място ЕНОЗД отбелязва, че макар и телекомуникационните компании несъмнено да са обект на нарушения на сигурността, които изискват задължение за уведомяване, същото важи и за други видове компании/доставчици. Вероятността търговците на дребно онлайн, банките онлайн, аптеките онлайн да бъдат, подобно на телекомуникационните компании, обект на нарушения на сигурността, е също толкова, ако не и по-голяма. Следователно съображенията относно риска не подкрепят ограничаване на обхвата на изискването за уведомяване за нарушение до ДОДЕСУ. Опитът на други държави е нагледен пример за необходимостта от по-широк подход. Така например в САЩ почти всички щати (понастоящем повече от 40) са приели закони за уведомяване за нарушения на сигурността, които имат по-широк обхват на приложение и включват не само ДОДЕСУ, но и всяко образувание, което разполага с необходимите лични данни.

24. На второ място, макар че нарушение на видовете лични данни, редовно обработвани от ДОДЕСУ, несъмнено може да окаже въздействие върху неприкосновеността на личния живот на лицето, същото, ако не в още по-голяма степен, важи за видовете лична информация, обработвана от ДУИО. Несъмнено, банки и други финансови институции може да разполагат със строго поверителна информация (напр. подробности за банкова сметка), чието разкриване може да позволи използване за кражба на самоличност. Освен това, разкриването от онлайн доставчици на здравни услуги на чувствителна информация, свързана със здравето, може да нанесе особени вреди на лицето. Ето защо, видовете лични данни, които могат да бъдат изложени на риск, също изискват по-широко приложение на уведомяването за нарушения на сигурността, което би включвало най-малкото ДУИО.

25. Бяха повдигнати някои правни въпроси срещу разширяването на обхвата на приложението на този член, т.е. обхванатите от това изискване образувания. По-специално фактът, че обхватът като цяло на Директивата за неприкосновеност на личния живот и електронни комуникации засяга само ДОДЕСУ беше изтъкнат като пречка за прилагането на задължението за уведомяване и към ДУИО.

26. Във връзка с това ЕНОЗД би желал да припомни, че: *i)* Няма никакви правни пречки в някои разпоредби на директивата да се включат и други участници освен ДОДЕСУ. Законодателят на Общността разполага с пълни правомощия в това отношение. *ii)* В сегашната Директива за неприкосновеност на личния живот и електронни комуникации има други прецеденти на прилагане спрямо образувания, различни от ДОДЕСУ.

27. Така например член 13 се прилага не само към ДОДЕСУ, но и към всяка компания, която разпраща нежелани съобщения, като изисква предварително съгласие за това. Освен това, член 5, параграф 3 от Директивата за неприкосновеност на личния живот и електронни комуникации, който, *inter alia*, забранява съхраняването на информация, като бисквитки в крайното устройство на потребителя, е обвързващо не само за ДОДЕСУ, но и за всеки, който се опитва да съхранява информация или да получи достъп до информация, съхранявана в крайни устройства на лицата. Освен това, в рамките на сегашния законодателен процес Комисията дори предложи обхватът на член 5, параграф 3 да се разшири, когато подобни технологии (бисквитки/софтуер за наблюдение) се доставят не само чрез електронни съобщителни системи, но и чрез всякакви други възможни средства (разпространение чрез сваляне от интернет или чрез външен носител за съхранение на данни, като например CD-ROM, устройства за съхранение с USB интерфейс, устройства с флаш памет и т.н.). Всички тези елементи са положителни и следва да бъдат запазени, но те съставляват и подходящи прецеденти за настоящото обсъждане относно обхвата.

28. Освен това, в сегашния законодателен процес Комисията, ЕП и евентуално Съветът предлагат нов член 6.6, параграф а), разгледан по-долу, който се прилага спрямо образувания, различни от ДОДЕСУ.

29. Най-накрая, като се имат предвид общите положителни елементи, произтичащи от задължението за уведомяване за нарушения на сигурността, много вероятно е гражданите да очакват тези ползи, когато личните им данни са били изложени на риск, не само от ДОДЕСУ, но и от ДУИО. Очакванията на гражданите може да не бъдат изпълнени, ако те например не бъдат уведомени, когато онлайн банка е изгубила информация за тяхната банкова сметка.

30. Накратко, ЕНОЗД е убеден, че ползите от уведомяването за нарушения на сигурността ще станат реални в пълна степен, само ако приложното поле на обхванатите образувания включва както ДОДЕСУ, така и ДУИО.

Стандарт, предизвикващ уведомяване

31. По отношение на факторите, предизвикващи уведомяване, както е пояснено по-долу, ЕНОЗД счита, че стандартът *„има вероятност да причини вреди“* в измененото предложение е най-подходящият сред трите предложени стандарта. Същевременно е важно да се гарантира, че понятието „вреди“ е достатъчно широко, за да обхване всички случаи на отрицателни последици за неприкосновеността на личния живот или други законни интереси на лицата. В противен случай би било за предпочитане да се създаде нов стандарт, според който уведомяването да е задължително *„ако има вероятност нарушението да предизвика неблагоприятни последици за лицата“*.

32. Както беше посочено в предишния раздел, условията, при които лицата трябва да бъдат уведомявани (наричани „задействащ фактор“ или „стандарт“), се различават в подходите на ЕП, Комисията и Съвета. Очевидно, обемът на уведомяванията, които лицата ще получават, зависи до голяма степен от „задействащия фактор“ или определения стандарт за уведомяване.

33. В подходите на Съвета и Комисията уведомяване трябва да се извърши, ако нарушението представлява *„сериозно нарушение на неприкосновеността на личния живот на абоната“* (Съветът) и ако *„в резултат на нарушението има вероятност от вреди за интересите на потребителя“* (Комисията). В подхода на ЕП задействащият фактор за уведомяване на лицата е *„сериозност на нарушението“* (т.е. уведомяване на лицата е необходимо, ако нарушението се счита за *„сериозно“*). Под този праг уведомяване не е необходимо ([13]).

34. ЕНОЗД осъзнава, че ако личните данни са били изложени на риск, може да се твърди, че лицата, на които принадлежат тези данни, при всички положения имат право да знаят за това. Същевременно е напълно справедливо да се помисли дали това решение е подходящо в контекста на други интереси и съображения.

35. Беше посочено, че задължението за уведомяване във всички случаи, когато лични данни са били изложени на риск, иначе казано без ограничения, може да доведе до свръхуведомяване и „умора от уведомяване“, което от своя страна да предизвика понижена чувствителност (десенсибилизация). Както е посочено по-долу, ЕНОЗД се отнася предпазливо към този аргумент; същевременно би искал да подчертае загрижеността си от свръхуведомяването като евентуален признак на широкоразпространено неизпълнение на практики в областта на информационната сигурност.

36. Както беше посочено по-горе, ЕНОЗД съзнава възможните неблагоприятни последици от свръхуведомяването и би желал да спомогне за това приетата правна рамка по отношение на уведомяването за нарушения на сигурността да не води до такъв резултат. Честото уведомяване на лицата при нарушения, дори тогава, когато няма неблагоприятни последици, вреди или бедствено положение, може да доведе до подкопаване на една от основните цели на уведомяването, тъй като по ирония лицата може да пренебрегнат уведомяването в тези случаи, когато всъщност може да е необходимо да вземат мерки за собствената си защита. Ето защо е важно да се постигне необходимото равновесие при изпращането на значимо уведомяване, тъй като липсата на реакция от лицата по отношение на полученото уведомяване значително намалява ефективността на системите за уведомяване.

37. За да се приеме подходящ стандарт, който няма да доведе до свръхуведомяване, освен обмислянето на задействащ фактор за уведомяване трябва да бъдат взети предвид други фактори и по-специално определението за нарушение на сигурността и информацията, обхваната от задължението за уведомяване. Във връзка с това ЕНОЗД отбелязва, че според трите предложени подхода обемът на уведомяванията може да бъде висок в контекста на широкото определение за нарушения на сигурността, обсъдено по-горе. Това безпокойство от свръхуведомяване допълнително се засилва от факта, че определението за нарушение на сигурността обхваща всички видове лични данни. Макар ЕНОЗД да счита този подход за правилния (неограничаване на видовете лични данни, подлежащи на уведомяване) за разлика от други подходи като например законите на САЩ, където изискванията са съсредоточени върху чувствителността на информацията, все пак този фактор трябва да се вземе предвид.

38. Във връзка с казаното по-горе и като се вземат съвкупно предвид различните променливи, ЕНОЗД счита, че е целесъобразно да се предвиди праг или стандарт, под който уведомяването не е задължително.

39. И двата предложени стандарта, т.е. че нарушението представлява „сериозен *риск за неприкосновеността на личния живот*“ или че *„има вероятност да нанесе вреди“* очевидно включват например социални или свързани с репутацията вреди и икономически загуби. Така например тези стандарти ще разглеждат случаи на излагане на кражба на самоличност чрез разпространението на непублични идентификатори като паспортни номера, както и разкриването на информация, свързана с личния живот на лицето. ЕНОЗД приветства този подход. ЕНОЗД е убеден, че ползите от уведомяването за нарушения на сигурността няма да се реализират напълно, ако системата за уведомяване обхваща само нарушенията, водещи до икономически вреди.

([13]) Вж. бележка под линия 11 относно изключението от това правило.

40. От двата предложени стандарта ЕНОЗД отдава предпочитание на стандарта на Комисията „*има вероятност да причини вреди*“, тъй като той би осигурил по-подходящо ниво на защита на лицата. Много по-вероятно е нарушенията да изискват уведомяване, ако „*има вероятност да причинят вреди*“ на неприкосновеността на личния живот на лицата, отколкото ако крият „*сериозен риск*“ от такива вреди. Ето защо включването в обхвата единствено на нарушения, представляващи сериозен риск за неприкосновеността на личния живот на лицето, би ограничило значително броя на нарушенията, за които трябва да се извърши уведомяване. Включването в обхвата единствено на такива нарушения би предоставило на ДОДЕСУ и на ДУИО извънредна свобода на преценка дали е необходимо уведомяване, доколкото така би било много по-лесно те да оправдаят заключение, че няма „*сериозен риск*“ от вреди, отколкото че „*няма вероятност да причини вреди*“. Макар че свръхуведомяването със сигурност трябва да се избягва, при преценката трябва да се вземе предвид защитата на интересите на лицата по отношение на неприкосновеността на личния им живот и те следва да бъдат защитени поне тогава, когато има вероятност нарушението да им причини вреди. Освен това, понятието „*има вероятност*“ ще бъде по-ефективно на практика както за обхванатите образувания, така и за компетентните органи, тъй като налага обективно оценяване на случая и свързаните с него обстоятелства.

41. Също така нарушения, свързани с личните данни, могат да причинят вреди, на които е трудно да се даде количествено изражение и които могат да бъдат различни. Всъщност, разкриването на един и същ вид данни може да причини, в зависимост от конкретните обстоятелства, значителни вреди на едно лице и помалки на друго. Стандарт, който изисква вредите да са материални, значителни или сериозни, не би бил подходящ. Подходът на Съвета например, който изисква нарушението да засяга *сериозно* неприкосновеността на личния живот, би осигурил неадекватна защита на лицата, доколкото такъв стандарт изисква последиците за неприкосновеността на личния живот да са „сериозни“ Това дава възможност и за субективно оценяване.

42. Въпреки че, както беше посочено по-горе, формулировката „*има вероятност да причини вреди*“ изглежда подходящ стандарт за уведомяване за нарушения на сигурността, ЕНОЗД остава загрижен, че тя може и да не изчерпва всички случаи, изискващи лицата да бъдат уведомени, т.е. всички случаи, в които има вероятност от отрицателни последици за неприкосновеността на личния живот и други законни права на лицата. Поради тази причина би могло да се помисли за стандарт, които изисква уведомяване, „*ако има вероятност нарушението да предизвика неблагоприятни последици за лицата*“.

43. Този алтернативен стандарт има и допълнителното преимущество, че е в съответствие със законодателството на ЕС в областта на защитата на данните. Всъщност, в Директивата относно защитата на данните често се говори за неблагоприятни последици за правата и свободите на субектите на данни. Така например член 18 и съображение 49, които разглеждат задължението операциите по обработката на данни да се регистрират при органите по защита на данните, позволяват на държавите-членки да се освобождават от това задължение в случаи, когато „*обработването не би могло да накърнява правата и свободите на съответните физически лица*“. Подобна формулировка е използвана в член 16.6 от общата позиция, за да се даде възможност на юридически лица да завеждат искове срещу разпространители на нежелани съобщения.

44. Освен това, като се вземе предвид посоченото по-горе, следва да се очаква обхванатите образувания и особено органите, отговарящи за прилагането на законодателството в областта на защитата на данните, да познават по-добре посочения по-горе стандарт и така по-лесно да преценяват дали определено нарушение отговаря на установения стандарт.

Образувание, което определя дали нарушение на сигурността отговаря или не на стандарта

45. В подхода на ЕП (освен в случаи на неминуема опасност) и измененото предложение на Комисията органите на държавите-членки определят дали нарушение на сигурността отговаря или не на стандарта, който задейства задължението за уведомяване на засегнатите лица.

46. ЕНОЗД смята, че участието на орган е важно, за да се определи дали изискванията на един стандарт са изпълнени, доколкото този орган е до известна степен гарант за правилното прилагане на закона. Такава система може да предотврати неподходящото оценяване от компаниите на едно нарушение като безвредно/несериозно и последващото избягване на уведомяване, когато в действителност такова уведомяване е необходимо.

47. От друга страна ЕНОЗД е загрижен, че режим, изискващ от органите да правят оценка, може да се окаже непрактичен и трудно приложим или на практика да доведе до обратен резултат. По този начин може дори да доведе до намаляване на гаранциите, свързани със защитата на данните на лицата.

48. Всъщност, при такъв подход съществува вероятност органите по защита на данните да бъдат затрупани с уведомявания за нарушения на сигурността и може да срещнат сериозни трудности при извършването на необходимото оценяване. Важно е да се помни, че за да се прецени дали едно нарушение отговаря на стандарта, на органите трябва да се предостави достатъчно вътрешна информация, често от комплексно техническо естество, която те трябва да обработят много бързо. Като се има предвид трудността на оценката и фактът, че някои органи разполагат с ограничени средства, ЕНОЗД се опасява, че органите много трудно ще могат да спазят това задължение и могат да прибягнат до средства, предназначени за други важни приоритети. Освен това, подобна система може да обремени ненужно органите; всъщност, ако решат, че нарушението не е сериозно, и въпреки това на лицата бъдат нанесени вреди, органите може евентуално да бъдат държани отговорни.

49. Посочената по-горе трудност допълнително се подсилва, ако се вземе предвид, че времето е определящо за свеждането до минимум на рисковете, произтичащи от нарушения на сигурността. Освен ако органите не съумеят да направят оценката в много кратки срокове, допълнителното време, необходимо за тази оценка, може да увеличи вредите за засегнатите лица. Следователно, тази допълнителна стъпка, която цели да осигури по-голяма защита на лицата, може, напротив, да доведе до по-ниска защита, отколкото основаните на пряко уведомяване системи.

50. Поради посочените по-горе причини ЕНОЗД смята, че би било за предпочитане да се създаде система, при която съответните образувания да преценяват дали нарушението отговаря на стандарта или не, както е предвидено в подхода на Съвета.

51. Същевременно, за да се избегне риска от евентуални злоупотреби, например на образувания, които отказват да извършат уведомяване в случаи, при които то очевидно е необходимо, от решаващо значение е да се включат определени гаранции, които са посочени по-долу.

52. На първо място, задължението обхванати образувания да определят дали трябва да извършат уведомяване трябва, разбира се, да бъде придружено от друго задължение, налагащо задължителното уведомяване на органите за всички нарушения, които отговарят на необходимия стандарт. В тези случаи засегнатите образувания следва да бъдат задължени да уведомяват органите за нарушението, за основанията за своето решение относно уведомяването и за съдържанието на извършеното уведомяване.

53. На второ място, органите трябва да получат същинска надзорна функция. При упражняването на тази функция органите трябва да имат възможност, но не задължението, да разследват обстоятелствата, свързани с нарушението, и да изискват подходящи действия за коригиране ([14]). Тук следва да се включва не само уведомяването на лица (когато то все още не е извършено), но и възможността да се налага задължение за предприемане на действия, които да предотвратят бъдещи нарушения. В това отношение органите следва да получат ефективни правомощия и средства, както и нужната свобода на действие да решават в кои случаи да предприемат действия за уведомяване за нарушения на сигурността. С други думи, това би позволило на органите да подхождат избирателно и да извършват разследвания например на наистина вредни нарушения на сигурността, като удостоверяват и прилагат съответствие с изискванията на закона.

54. За да се постигне това, освен правомощията, признати съгласно Директивата за неприкосновеност на личния живот и електронни комуникации, като например член 15.а.3 и Директивата за защита на данните, ЕНОЗД препоръчва да се вмъкне следната формулировка: „*Ако засегнатият абонат или лице още не е уведомено, компетентният национален орган, след като е преценил естеството на нарушението, може да изисква от ДОДЕСУ и ДУИО да направят това*“.

55. Освен това ЕНОЗД препоръчва ЕП и Съветът да потвърдят предложеното от ЕП задължение (изменение 122, член 4.1.а) на образувания да извършват оценка на риска и идентифициране на своите системи и личните данни, които възнамеряват да обработват. Въз основа на това задължение образуванията изготвят адаптирано и точно определение на мерките за сигурност, които ще бъдат прилагани в техния случай и които следва да бъдат на разположение на органите. Ако възникне нарушение на сигурността, това задължение ще улесни обхванатите образувания — и в крайна сметка и органите в тяхната надзорна функция — да определят дали излагането на риск на тази информация може да има неблагоприятни последици или да причини вреди на лицата.

56. На трето място, задължението на обхванатите образувания да определят дали трябва да уведомят лицата трябва да се съпътства от задължение за провеждане на подробно и изчерпателно вътрешно проследяване (одитна следа), което описва всички възникнали нарушения и съответното уведомяване, както и мерките, предприети за избягване на бъдещи нарушения. Тази вътрешна одитна следа трябва да бъде на разположение на органите за преглед и евентуално разследване. Така органите ще могат да изпълняват надзорната си функция. Това може да се постигне чрез приемането на формулировка в следния смисъл: „*ДОДЕСУ и ДУИО водят и поддържат подробен регистър, в който се описват всички нарушения на сигурността, свързаната с това техническа информация и предприетите действия за коригиране. В регистъра е описано и всяко уведомяване на засегнати абонати или лица и на компетентните национални органи, включително датата и съдържанието. Регистърът се предоставя на компетентния национален орган при поискване.*“

57. Разбира се, за да се гарантира последователност при прилагането на този стандарт, както и на други аспекти на рамката за нарушения на сигурността, като например формата и процедурите за уведомяване, би било целесъобразно Комисията да приеме технически мерки за прилагане, след консултации с ЕНОЗД, работна група „Член 29“ и съответните заинтересовани страни.

([14]) Член 15а.3 отчита тези надзорни правомощия, като установява, че „*Държавите-членки гарантират, че компетентните национални органи и, когато е целесъобразно, други национални органи, разполагат с всички необходими правомощия и ресурси за разследване, включително възможността да получават всякаква подходяща информация, от която биха имали нужда за наблюдение и изпълнение на националните разпоредби, приети в съответствие с настоящата директива.*“

Получатели на уведомяването

58. Що се отнася до уведомяването ЕНОЗД предпочита формулировката на ЕП и Комисията пред тази на Съвета. Всъщност, ЕП е заменил формулировката „абонати“ с „ползватели“. Комисията използва „абонати“ и „засегнато лице“. Във формулировката на ЕП и на Комисията като получатели на уведомяването са включени не само настоящите, но и бившите абонати, както и трети страни, като например ползватели, които осъществяват връзка с някои обхванати образувания, без да са техни абонати. ЕНОЗД приветства този подход и призовава ЕП и Съвета да го запазят.

59. Същевременно ЕНОЗД отбелязва някои несъответствия във формулировките в първото четене в ЕП, които следва да бъдат коригирани. Така например в повечето, но не във всички случаи формулировката „абонати“ е заменена с „ползватели“, в други случаи с „потребители“. Това следва да се хармонизира.

III. **ОБХВАТ НА ПРИЛОЖЕНИЕ НА ДИРЕКТИВАТА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЕЛЕКТРОННИ КОМУНИКАЦИИ: ПУБЛИЧНИ И ЧАСТНИ МРЕЖИ**

60. Член 3.1 от сегашната Директива за неприкосновеност на личния живот и електронни комуникации установява образуванията, които са основно засегнати от директивата, т.е. тези, които обработват данни „*във връзка с*“ предоставянето на публично достъпни електронно комуникационни услуги в публични комуникационни мрежи (назовани по-горе ДОДЕСУ) ([15]). Примерите за ДОДЕСУ включват предоставяне на достъп до интернет, пренос на информация чрез електронни мрежи, мобилни и телефонни връзки и др.

61. ЕП прие изменение 121, което изменя член 3 от първоначалното предложение на Комисията, съгласно който обхватът на приложение на Директивата за неприкосновеност на личния живот и електронни комуникации е разширен, за да се включи „*обработката на лични данни във връзка с предоставянето на публично достъпни електронно комуникационни услуги в публични и частни комуникационни мрежи и публично достъпни частни мрежи в Общността, [...]*“ (член 3.1 от Директивата за неприкосновеност на личния живот и електронни комуникации). За съжаление, Съветът и Комисията не можаха да приемат това изменение и съответно не включиха този подход в общата позиция и измененото предложение.

Приложение на Директивата за неприкосновеност на личния живот и електронни комуникации спрямо публично достъпни частни мрежи

62. Поради посочените по-долу основания и за да спомогне за постигането на консенсус, ЕНОЗД предлага да се запази същността на изменение 121. Освен това ЕНОЗД предлага да се включи изменение, доуточняващо видовете услуги, които ще включва разширеният обхват.

63. Частни мрежи често се използват за предоставяне на електронни комуникационни услуги, като например достъп до интернет на неопределен, потенциално голям брой лица. Такъв е например случаят с достъп до интернет в интернет-кафенета, както и на места с безжичен достъп в хотели, ресторанти, летища, влакове и други публични места, където такива услуги често се предоставят като допълнение към други услуги (напитки, настаняване и пр.)

64. В горепосочените примери комуникационна услуга, напр. достъп до интернет, става публично достъпна не чрез публична мрежа, а по-скоро чрез частна, т.е. частно управлявана мрежа. Освен това, въпреки че в горните случаи комуникационната услуга се предоставя на обществеността, тъй като използваната мрежа е частна, а не публична, *може да се твърди*, че предоставянето на тези услуги не е обхванато в цялата Директива за неприкосновеност на личния живот и електронни комуникации или най-малкото в някои нейни членове ([16]). В резултат основните права на лицата, гарантирани от Директивата за неприкосновеност на личния живот и електронни комуникации, в тези случаи не са защитени и възниква неравностойна правна ситуация за ползватели, които имат достъп до същите услуги за достъп до интернет чрез публични телекомуникационни средства, спрямо онези, които имат достъп до тях чрез частни мрежи. И това въпреки факта, че във всички тези случаи съществува същата степен на риск за неприкосновеността на личния живот и личните данни на лицата, както когато за услугата се използват публични мрежи. Накратко, изглежда няма *основание*, което съгласно Директивата да оправдава различното третиране на комуникационни услуги, предоставяни чрез частна мрежа, спрямо тези, предоставяни чрез публична мрежа.

65. Ето защо ЕНОЗД би подкрепил изменение като изменение 121 на ЕП, съгласно което Директивата за неприкосновеност на личния живот и електронни комуникации ще се прилага и при обработката на лични данни във връзка с предоставянето на публично достъпни електронно комуникационни услуги в *частни* комуникационни мрежи.

66. ЕНОЗД обаче отчита, че тази формулировка би могла да има непредвидими и евентуално и нежелани последици. Всъщност, самото упоменаване на частни мрежи би могло да се тълкува като обхващащо положения, които

([15]) „Настоящата директива се прилага при обработката на лични данни във връзка с предоставянето на публично достъпни електронни комуникационни услуги в публични комуникационни мрежи в Общността“.

([16]) *Напротив*, би могло да се твърди, че тъй като комуникационната услуга е публично достъпна, дори ако мрежата е частна, предоставянето на такива услуги е обхванато от съществуващата правна рамка въпреки факта, че мрежата е частна. Така например във Франция работодатели, предоставящи на служителите си достъп до интернет, се разглеждат като доставчици на интернет, които предлагат достъп до интернет на търговска основа. Това тълкуване не е широко възприето.

директивата очевидно няма за цел да обхваща. Така например, би могло да се твърди, че буквалното или стриктно тълкуване на тази формулировка би могло да включи в обхвата на директивата собственици на жилища с безжичен достъп ([17]) , които дават възможност на всекиго в техния обхват (обикновено жилището) да осъществява връзка; макар че изменение 121 няма такава цел. За да се избегне такъв резултат, ЕНОЗД предлага изменение 121 да се перифразира, като включи в обхвата на приложение на Директивата за неприкосновеност на личния живот и електронни комуникации „*обработката на лични данни във връзка с предоставянето на публично достъпни електронно комуникационни услуги в публични или публично достъпни частни комуникационни мрежи в Общността,...*“

67. Така ще бъде по-ясно, че само частни мрежи, които са публично достъпни, ще бъдат обхванати от Директивата за неприкосновеност на личния живот и електронни комуникации. Чрез прилагане на разпоредбите на Директивата за неприкосновеност *само* към *публично достъпни частни мрежи* (а не към всички частни мрежи) се въвежда ограничение, така че директивата обхваща само комуникационните услуги, предоставяни в частни мрежи, които умишлено са направени публично *достъпни*. Тази формулировка допълнително подчертава, че *наличността* на частната мрежа *за членове на широката общественост* е основният фактор при определянето дали директивата ще обхваща (освен предоставянето на публично достъпни комуникационни услуги). С други думи, независимо от това дали е публична или частна, ако мрежата умишлено е направена публично достъпна, за да предоставя публична комуникационна услуга, като например достъп до интернет, дори тази услуга да допълва друга (напр. настаняване в хотел), този вид услуга/ мрежа ще бъде обхванатата от Директивата за неприкосновеност на личния живот и електронни комуникации.

68. ЕНОЗД отбелязва, че подкрепеният по-горе подход, според който разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации се прилагат спрямо *публично достъпни частни мрежи*, съответства на приетите в няколко държави-членки подходи, където органите вече са включили такива услуги, както и услугите, предоставяни в чисто частни мрежи, в обхвата на приложение на националните разпоредби за изпълнение на Директивата за неприкосновеност на личния живот и електронни комуникации ([18]).

69. За по-голяма правна сигурност по отношение на образуванията, включени в новия обхват, може би ще е полезно в Директивата за неприкосновеност на личния живот да се включи изменение, което дава определение за „публично достъпни частни мрежи“ и което би могло да гласи, както следва: „*публично достъпна частна мрежа означава частно управлявана мрежа, до която членове на широката общественост имат неограничен достъп, независимо дали чрез заплащане или заедно с други услуги или предложения, при приемане на приложимите договорености и условия.*“

70. На практика горният подход би означавал, че ще бъдат включени частни мрежи в хотели и други учреждения, които предоставят достъп до интернет на широката общественост чрез частна мрежа. Обратно, предоставянето на комуникационни услуги в чисто частни мрежи, където услугата е сведена до група определени лица, няма да бъде включено в обхвата. Ето защо виртуални частни мрежи например, както и жилища на потребители, оборудвани с безжичен достъп, няма да бъдат обхванати от директивата. Няма да бъдат обхванати и услуги, предоставени чрез чисто корпоративни мрежи.

Частни мрежи в обхвата на приложение на Директивата за неприкосновеност на личния живот и електронни комуникации

71. Изключването на частни мрежи *сами по себе си*, както е посочено по-горе, следва да се счита за *междинна* мярка, която да подлежи на по-нататъшно обсъждане. Всъщност, като се имат предвид от една страна последиците за неприкосновеността на личния живот от изключването на чисто частните мрежи като такива и от друга фактът, че се засягат голям брой хора, които обикновено осъществяват достъп до интернет чрез корпоративни мрежи, в бъдеще може да се наложи преразглеждане. Поради тази причина и за да допринесе за дебата по този въпрос, ЕНОЗД препоръчва в Директивата за неприкосновеност на личния живот и електронни комуникации да се включи съображение, според което Комисията ще проведе публични консултации относно прилагането на Директивата към всички частни мрежи, със съдействието на ЕНОЗД, органите по защита на данните и други заинтересовани страни. Освен това, в съображението би могло да се уточни, че в резултат на публичните консултации Комисията следва да изготви подходящо предложение за разширяване или ограничаване на видовете образувания, които следва да бъдат обхванати от директивата.

72. Освен посоченото по-горе, различните членове от Директивата за неприкосновеност на личния живот и електронни комуникации следва да бъдат съответно изменени, така че във всички оперативни разпоредби освен публичните мрежи изрично да се посочват публично достъпните частни мрежи.

IV. **ОБРАБОТКА НА ДАННИ ЗА ТРАФИК ЗА ЦЕЛИТЕ НА СИГУРНОСТТА**

73. В хода на законодателния процес, свързан с преразглеждането на Директивата за неприкосновеност на личния живот и електронни комуникации, компаниите, предоставящи услуги в областта на сигурността, заявиха, че е необходимо в директивата да бъде въведена разпоредба, узаконяваща събирането на данни за трафик за гарантиране на ефективна сигурност онлайн.

([17]) Обикновено локална мрежа (LANs).
([18]) Вж. бележка под линия 16.

74. Вследствие, ЕП вмъкна изменение 181, с което се създава нов член 6.6., буква а), изрично упълномощаващ обработката на лични данни за целите на сигурността: „*Без да се засяга съответствието с разпоредбите, различни от член 7 от Директива 95/46/ЕО и член 5 от настоящата директива, данните за трафик могат да бъдат обработвани за целите на законните интереси на контролиращия данните орган с цел прилагане на технически мерки за гарантиране на мрежовата и информационната сигурност, както е определено в член 4, буква в) от Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за създаване на Европейска агенция за мрежова и информационна сигурност, на публична електронна съобщителна услуга, публична или частна електронна съобщителна мрежа, информационна обществена услуга или свързано крайно и електронно съобщително оборудване, с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице. Такава обработка трябва да бъде строго ограничена до необходимото за целите на сигурността*“.

75. В измененото предложение на Комисията това изменение принципно беше възприето, но отпадна основна формулировка, целяща да гарантира, че останалите разпоредби на директивата трябва да бъдат спазвани при отстраняването на формулировката, която гласи „*Без да се засяга [...].. на настоящата директива*“). Съветът прие преработен вариант, който представляваше още една стъпка към размиване на важните защити и балансиране на интересите, залегнали в изменение 181, чрез приемането на формулировка, която гласи следното: „*Данните за трафик могат да се обработват до степента, строго необходима за гарантирането [...] на мрежовата и информационна сигурност, посочена в член 4, буква в) от Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за създаване на Европейската агенция за мрежова и информационна сигурност.*“

76. Както е пояснено по-долу, член 6.6, буква а) е излишен и крие опасност от злоупотреби, особено ако бъде приет във вид, който не включва важните гаранции, клаузи, спазващи други разпоредби на директивата, и балансирането на интереси. Ето защо ЕНОЗД препоръчва този член да се отхвърли или поне да се направи необходимото всеки един член относно този въпрос да включва видовете гаранции, съдържащи се в изменение 181 на ЕП.

Правни основания за обработката на данни за трафик, приложими към електронни комуникационни услуги и други администратори на лични данни, съгласно сегашното законодателство за защита на данните

77. Степента, в която ДОДЕСУ могат да обработват законно данни за трафик, е уредена по член 6 от Директивата за неприкосновеност на личния живот и електронни комуникации, който ограничава обработката на данни за трафик до определен брой цели, като изготвяне на сметка, взаимна връзка и търговия. Тази обработка може да се извърши само при определени условия, като например съгласие на лицето в случай на търговия. Освен това, други администратори на данни като ДУИО могат да обработват данни за трафик по член 7 от Директивата за защита на данните, който установява, че администраторите на лични данни могат да обработват лични данни при спазване на най-малко едно от посочените правни основания, наричани още правни съображения.

78. Пример за такова правно основание е член 7, буква а) от Директивата за защита на данните, който изисква съгласието на субекта на данните. Така например, ако онлайн търговец на дребно желае да обработва данни за трафик с цел изпращане на реклами или търговски материали, той трябва да получи съгласието на лицето. Друго правно основание, посочено в член 7, допуска, в определени случаи, обработката на данни за трафик за целите на сигурността например от компании в сферата на сигурността, които предлагат услуги, свързани със сигурността. Това се основава на член 7, буква е), който установява, че администраторите на лични данни могат да обработват лични данни, ако това е „*необходимо за целите на законните интереси, преследвани от администратора или от трето лице или лица, на които се разкриват данните, с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице.*“. Директивата за защита на данните не уточнява случаите, в които обработката на лични данни отговаря на това изискване. Вместо това, решенията се вземат от администраторите на лични данни за всеки отделен случай, често със съгласието на националните органи по защита на данните и други органи.

79. Следва да се обмисли взаимодействието между член 7 от Директивата за защита на данните и предложения член 6.6, буква а) от Директивата за неприкосновеност на личния живот и електронни комуникации. Предложеният член 6.6, буква а) уточнява обстоятелствата, при които посочените по-горе изисквания в член 7, буква е) ще бъдат изпълнени. Всъщност, като упълномощава обработката на данни за трафик с цел гарантиране на сигурността на мрежата и информацията, член 6.6, буква а) допуска такава обработка за целите на законните интереси, преследвани от администратора на лични данни.

80. Както е обяснено по-долу, ЕНОЗД смята, че предложеният член 6.6, буква а) не е нито необходим, нито полезен. Всъщност, по принцип, от правна гледна точка е ненужно да се установява дали определен вид дейност, свързана с обработката на данни за трафик, в този случай обработката на данни за целите на сигурността, отговаря или не на изискванията в член 7, буква е) от Директивата за защита на данните, в който случай може да е необходимо съгласието на лицето по силата на член 7, буква а). Както вече беше отбелязано, тази оценка обикновено се прави от администраторите на лични данни, т.е. компании на ниво изпълнение, след консултации с органите по защита на данните, и при необходимост съдилищата. По принцип ЕНОЗД смята, че в определени случаи законната обработка

на данни за трафик за целите на сигурността, която е извършена, без да се застрашават основни права и свободи на лицата, вероятно ще отговаря на изискванията на член 7, буква е) от Директивата за защита на данните и следователно може да бъде извършена. Освен това, в Директивата за защита на данните и в Директивата за неприкосновеност на личния живот и електронни комуникации няма друг случай на обособяване или предоставяне на специално третиране за определени дейности, свързани с обработката на данни, които биха задоволили изискванията на член 7, буква е), а и няма изразена необходимост за такова изключение. Напротив, както беше отбелязано по-горе, при много обстоятелства този вид дейност очевидно се вмества добре в сегашния текст. Следователно, правна разпоредба, потвърждаваща тази оценка, по принцип е ненужна.

Вариантите на член 6.6, буква а) на ЕП, Съвета и Комисията

81. Както е обяснено, макар и ненужно, по-горе, важно е да се подчертае, че изменение 181 във вида, приет от Европейския парламент, беше все пак формулирано до известна степен, вземайки предвид принципите за неприкосновеност на личния живот и защитата на данните, залегнали в законодателството в областта на защитата на данните. Изменение 181 на ЕП би могло да разгледа още по-задълбочено интересите, свързани със защитата на данните и неприкосновеността на личния живот, чрез добавянето например на формулировката „в специфични случаи“, за да се гарантира избирателното прилагане на този член, или чрез включването на конкретен период на съхранение.

82. Изменение 181 съдържа някои положителни елементи. То потвърждава, че обработката следва да спазва всички останали принципи за защита на данните, приложими към обработката на лични данни („*Без да се засяга... съответствието с разпоредбите [...] на Директива 95/46/ЕО и [...] на настоящата директива*“). Освен това, въпреки че изменение 181 допуска обработката на данни за трафик за целите на сигурността, то установява равновесие между интересите на образуването, обработващо данни за трафик, и тези на лицата, чиито данни се обработват, така че подобна обработка на данни може да се извърши, само ако интересите, свързани с основните права и свободи на лицата, имат преимущество пред тези на образуването, обработващо данните („*с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице*“). Това изискване е съществено дотолкова, доколкото допуска обработката на данни за трафик в специфични случаи; то обаче не позволява образувание да обработва данни за трафик на едро.

83. Преработеният вариант на Съвета на изменението съдържа положителни елементи, като например запазването на формулировката „*строго необходимо*“, която подчертава ограничения обхват на приложение на този член. Във варианта на Съвета обаче са премахнати посочените по-горе гаранции, свързани със защитата на данните и неприкосновеността на личния живот. Макар по принцип да се прилагат общи разпоредби за защита на данните, независимо дали се прави конкретно позоваване във всеки отделен случай, вариантът на Съвета на член 6.6, буква а) може все пак да се тълкува като предоставящ пълни правомощия за вземане на решения за обработка на данни за трафик, без да се спазват гаранциите за защита на данните и неприкосновеност на личния живот, които се прилагат при всяка обработка на данни за трафик. Следователно може да се твърди, че данни за трафик могат да се събират, съхраняват и използват за по-нататъшни цели, без да е необходимо да се спазват принципите за защита на данните и специфични задължения, които иначе се прилагат спрямо отговорните страни, като например принципа за качество или задължението за справедлива и законна обработка и изискването да се пази поверителността и сигурността на данните. Освен това, тъй като липсва позоваване на приложимите принципи за защита на данните, които налагат срок за съхранение на информацията, или на специфичен срок в самия член, вариантът на Съвета може да се тълкува като позволяващ събирането и обработката на данни за трафик за целите на сигурността за неопределен период.

84. В допълнение, чрез стремежа към разширяване на формулировките Съветът отслаби на определени места в текста защитите, свързани с неприкосновеността на личния живот. Така например позоваването на „законните интереси на администратора на лични данни“ беше премахнато, което повдига въпроси във връзка с видовете образувания, които биха могли да се възползват от това изключение. От решаващо значение е да се избегне допускането на възможността ползвател или юридическо лице да се възползва от това изменение.

85. Скорошният опит в ЕП и Съвета показва, че е трудно да се определят посредством закона размерът и условията, съгласно които обработката на данни за целите на сигурността може да бъде законно извършена. Малко вероятно е съществуващ или бъдещ член да премахне очевидните рискове от прекалено широко прилагане на изключението по причини, различни от свързаните със сигурността, или от образувания, които не би следвало да могат да се възползват от изключението. Това не означава, че подобна обработка не може да се извърши в никой случай. Но по-добра оценка на това дали и до каква степен би могла да се извърши обработка може да бъде направена на ниво изпълнение. Образувания, които желаят да участват в такава обработка, следва да обсъдят обхвата и условията с органите по защита на данните и евентуално с работна група „Член 29“. Друга възможност е в Директивата за неприкосновеност на личния живот и електронни комуникации да се включи член, допускащ обработката на данни за трафик за целите на сигурността след изрично упълномощаване от органите по защита на данните.

86. Като се вземат предвид от една страна рисковете, които крие член 6.6, буква а) за основното право на лицата на защита на данните и неприкосновеността на личния живот, а от друга страна и фактът, че, както се посочва в настоящото становище, от правна гледна точка този член е ненужен, ЕНОЗД стигна до заключението, че най-добрият изход би било пълното заличаване на предложения член 6.6, буква а).

87. Ако въпреки препоръката на ЕНОЗД бъде приет текст в смисъла на някой от настоящите варианти на член 6.6 буква а), той при всяко положение следва да съдържа обсъдените по-горе гаранции за защита на данните. Той следва да бъде и подобаващо интегриран в съществуващата структура на член 6, за предпочитане като нов параграф 2а.

V. **ВЪЗМОЖНОСТТА ЮРИДИЧЕСКИ ЛИЦА ДА ПРЕДПРИЕМАТ ПРАВНИ ДЕЙСТВИЯ ПРИ НАРУШЕНИЯ НА ДИРЕКТИВАТА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЕЛЕКТРОННИ КОМУНИКАЦИИ**

88. ЕП прие изменение 133, което дава възможност на доставчиците на достъп до интернет и други юридически лица като потребителски асоциации да завеждат дела за нарушения на която и да е разпоредба на Директивата за неприкосновеност на личния живот и електронни комуникации ([19]). За съжаление, нито Комисията, нито Съветът приеха това изменение. ЕНОЗД счита това изменение за много положително и препоръчва то да бъде запазено.

89. За да се разбере значението на това изменение, трябва да се осъзнае, че в областта на неприкосновеността на личния живот и защитата на данните нанесените на лице вреди, индивидуално погледнати, обикновено не са достатъчни сами по себе си, за да може това лице да предяви иск в съда. Обикновено лицата не отиват сами в съда заради това, че са получили нежелани съобщения или заради погрешно включване на името им в директория. Това изменение би позволило на потребителски асоциации и профсъюзи, представляващи интересите на потребителите, да предявяват иск от тяхно име на колективно ниво в съда. Освен това е вероятно по-голямото разнообразие от механизми за прилагане да доведе до по-голямо спазване и следователно да способства за ефективно прилагане на разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации.

90. В правната рамка на някои държави-членки съществуват прецеденти, в които вече е предвидена възможността за колективна правна защита, за да могат потребители или заинтересовани групи да търсят обезщетение от страната, причинила вреди.

91. Освен това, законодателството на някои държави-членки в областта на конкуренцията ([20]) , дава право на потребители, заинтересовани групи (освен *засегнатия конкурент*) да заведат дело срещу образуването, извършило нарушението. *Основанието* за този подход е, че е вероятно компании, действащи в нарушение на законодателството за конкуренцията, да се облагодетелстват, тъй като потребители, претърпели само леки вреди, по правило не са склонни да заведат дело. Това основание може да се прилага *mutantis mutandi* в областта на защитата на данните и неприкосновеността на личния живот.

92. По-важното, както беше посочено по-горе, е, че предоставянето на право на юридически лица като потребителски асоциации и ДОДЕСУ да завеждат дела укрепва позицията на потребителите и съдейства за цялостното спазване на законодателството в областта на защитата на данните. Ако извършващите нарушения компании са изправени пред по-голям риск да бъдат съдени, те вероятно ще инвестират повече в спазването на законодателството в областта на защитата на данните, което в дългосрочен план увеличава степента на защита на неприкосновеността на личния живот и на потребителите. Предвид всички тези основания ЕНОЗД призовава ЕП и Съвета да приемат разпоредба, позволяваща на юридически образувания да предявяват иск за нарушения на която и да е от разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации.

VI. **ЗАКЛЮЧЕНИЕ**

93. Общата позиция на Съвета, първото четене в ЕП и измененото предложение на Комисията съдържат, в различна степен, положителни елементи, които биха послужили за увеличаване степента на защита на неприкосновеността на личния живот на лицата и техните лични данни.

94. Същевременно ЕНОЗД смята, че има място за подобрения, по-специално по отношение на Общата позиция на Съвета, в която за съжаление не са запазени някои от измененията на ЕП, целящи да гарантират адекватната защита на неприкосновеността на личния живот на лицата и техните лични данни. ЕНОЗД призовава ЕП и Съвета да възстановят гаранциите, свързани с неприкосновеността на личния живот, залегнали в първото четене в ЕП.

95. Освен това, ЕНОЗД смята за целесъобразно да се рационализират някои от разпоредбите на директивата. Това важи с особена сила за разпоредбите относно нарушения на сигурността, тъй като ЕНОЗД смята, че максималните ползи от уведомяването при нарушение ще бъдат най-добре постигнати, ако от самото начало има адекватна правна рамка. Най-сетне, ЕНОЗД смята за целесъобразно да се подобри и уточни формулировката на някои от разпоредбите на директивата.

96. Във връзка с посоченото по-горе, ЕНОЗД призовава ЕП и Съвета да положат повече усилия за подобряване и уточняване на някои от разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации, като същевременно възстановят приетите на първо четене в ЕП изменения, целящи да гарантират подходящо ниво на защита на неприкосновеността на личния живот и данните. За целта точки 97, 98, 99 и 100 по-долу представят накратко най-важните въпроси и правят някои препоръки и предложения по текста. ЕНОЗД призовава всички участващи страни да ги вземат предвид в хода на придвижването на Директивата за неприкосновеност на личния живот и електронни комуникации за окончателно приемане.

Нарушения на сигурността

97. Европейският парламент, Комисията и Съветът приеха различни подходи за уведомяване за нарушения на сигурността. Между трите модела има разлики по отношение, *inter alia,* на обхванатите от задължението образувания, на стандарта и фактора, задействащ уведомяването, субектите на данни, които могат да бъдат уведомявани и т.н. Необходимо е ЕП и Съветът да положат максимални усилия и да представят стабилна правна рамка за нарушения на сигурността. За целта ЕП и Съветът следва:

([19]) Член 13.6 от първото четене в ЕП.

([20]) Вж. например , § 8 UWG — Закон на Германия относно нелоялната конкуренция.

— *Да запазят* определението за нарушение на сигурността в текстовете на ЕП, Съвета и Комисията, тъй като то е достатъчно широко, за да обхване повечето ситуации, които биха могли да дадат основания за уведомяване за нарушения на сигурността.

— По отношение на образуванията, които ще бъдат обхванати от предложеното изискване за уведомяване, *да се включат* доставчиците на услуги на информационното общество. Вероятността търговци на дребно онлайн, банки онлайн, аптеки онлайн да бъдат обект на нарушения на сигурността по подобие на телекомуникационните компании, е също толкова, ако не и поголяма. Гражданите ще очакват да бъдат уведомявани, не само когато доставчиците на достъп до интернет пострадат от нарушения на сигурността, но и особено ако това се случи с техните банки онлайн или аптеки онлайн.

— По отношение на факторите, предизвикващи уведомяване, стандартът „*има вероятност да причини вреди*“ в измененото предложение е подходящ и осигурява добро функциониране на системата. Същевременно е важно да се гарантира, че „вреди“ е достатъчно широко понятие, за да обхване всички случаи на отрицателни последици за неприкосновеността на личния живот или други законни интереси на лицата. В противен случай би било за предпочитане да се създаде нов стандарт, според който уведомяването да е задължително „*ако има вероятност нарушението да предизвика неблагоприятни последици за лицата*“. Подходът на Съвета, според който нарушението трябва да засяга *сериозно* неприкосновеността на личния живот, би предложил неадекватна защита на лицата, доколкото такъв стандарт изисква последиците за неприкосновеността на личния живот да са „сериозни“. Това дава възможност и за субективно оценяване.

— Макар участието на орган с цел определяне дали засегнато образувание трябва да уведоми лицата определено да има положителни страни, то може да се окаже непрактично и трудно приложимо, а и да отнеме средства, предназначени за други важни приоритети. ЕНОЗД се опасява, че ако органите не успеят да реагират изключително бързо, подобна система може дори да намали защитата на лицата и да обремени ненужно органите. Ето защо, като цяло, ЕНОЗД съветва *да се създаде* система, която да оставя на засегнатите образувания преценката за това дали трябва да извършат уведомяване.

— За да позволят на органите да упражняват надзор върху оценките на обхванатите образувания дали да уведомяват, *да въведат* следните гаранции:

  — *Да гарантират*, че тези образувания са длъжни да уведомяват органите за всички нарушения, които отговарят на установения стандарт.

  — *Да предоставят* на органите надзорна функция, която им позволява да подхождат избирателно с цел ефективност. За постигане на посоченото погоре, да вмъкнат следната формулировка: „*Ако засегнатият абонат или лице още не е уведомено, компетентният национален орган, след като е преценил естеството на нарушението, може да изисква от ДОДЕСУ и ДУИО да направят това*“.

  — *Да приемат* нова разпоредба, която изисква образуванията да водят подробна и изчерпателна история на вътрешния одит (одитна следа). Това би могло да се постигне чрез приемането на следната формулировка: „*ДОДЕСУ и ДУИО поддържат подробен регистър, в който се описват всички нарушения на сигурността, свързаната с това техническа информация и предприетите действия за коригиране. В регистъра е описано и всяко уведомяване на засегнати абонати или лица, и на компетентните национални органи, включително датата и съдържанието. Регистърът се предоставя на компетентния национален орган при поискване.*“

— За да се гарантира последователност при прилагането на рамката за нарушения на сигурността, *да предоставят* на Комисията възможността да приеме технически мерки за прилагане, след предварителни консултации с ЕНОЗД, работна група „Член 29“ и други заинтересовани страни.

— По отношение на лицата, които трябва да бъдат уведомявани, *да използват* формулировката на Комисията или ЕП „засегнати лица“ или „засегнати ползватели“, тъй като тя включва всички лица, чиито лични данни са били изложени на риск.

Публично достъпни частни мрежи

98. Комуникационните услуги често се правят публично достъпни не чрез публични мрежи, а чрез частно управлявани мрежи (напр. места с безжичен достъп в хотели, летища), които, може да се твърди, не са включени в обхвата на директивата. ЕП прие изменение 121 (член 3), което разширява обхвата на приложение на директивата, като включва публични и частни комуникационни мрежи, както и публично достъпни частни мрежи. В това отношение ЕП и Съветът следва:

— *Да запазят* същността на изменение 121, но *да* го *преформулират*, за да включат в обхвата на Директивата за неприкосновеност на личния живот и електронни комуникации единствено „*обработката на лични данни във връзка с предоставянето на публично достъпни електронно комуникационни услуги в публични или публично достъпни частни комуникационни мрежи в Общността*“. Мрежите, които са изцяло частно управлявани (за разлика от публично достъпни частни мрежи) няма да бъдат изрично обхванати.

— *Да изменят* съответно всички оперативни разпоредби, за да се упоменат изрично публично достъпните частни мрежи освен публичните мрежи.

— *Да включат* изменение, което определя *„публично достъпна частна мрежа означава частно управлявана мрежа, до която членове на широката общественост имат неограничен достъп, независимо дали чрез заплащане или заедно с други услуги или предложения, при приемане на приложимите договорености и условия“*. Това ще гарантира по-голяма правна сигурност по отношение на включените в новия обхват образувания.

— *Да приемат* ново съображение, съгласно което Комисията ще проведе публични консултации относно прилагането на Директивата за неприкосновеност на личния живот и електронни комуникации спрямо всички частни мрежи, с принос от ЕНОЗД, работна група „Член 29“ и други заинтересовани страни. Да уточнят, че в резултат на публичните консултации Комисията следва да изготви подходящо предложение за разширяване или ограничаване на видовете образувания, които следва да бъдат обхванати от Директивата за неприкосновеност на личния живот и електронни комуникации.

Обработка на данни за трафик за целите на сигурността

99. ЕП прие на първо четене изменение 181 (член 6.6, буква а), което разрешава обработката на данни за трафик за целите на сигурността. В общата позиция на Съвета беше приет нов вариант, който размi някои от гаранциите, свързани с неприкосновеността на личния живот. В това отношение ЕНОЗД препоръчва ЕП и Съветът:

— *Да отхвърлят* напълно този член, защото той е ненужен и ако бъде използван за злоупотреби, може излишно да застраши защитата на данните и неприкосновеността на личния живот на лицата.

— Или, ако бъде приет вариант на сегашния текст на член 6.6, буква а), *да се включат* гаранциите за защита на данните, разгледани в настоящото становище (сходни с тези в изменението на ЕП).

Действия при нарушения на Директивата за неприкосновеност на личния живот и електронни комуникации

100. Европейският парламент прие изменение 133 (член 13.6), което позволява на юридически лица да завеждат дела при нарушения на която и да е от разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации. За съжаление Съветът не запази това изменение. Съветът и ЕП следва:

— *Да одобрят* разпоредбата, позволяваща на юридически лица, като потребителски асоциации и профсъюзи, да завеждат дела за нарушения на която и да е от разпоредбите на Директивата (не само за нарушение на разпоредбите относно нежелани съобщения, както е в настоящия подход в общата позиция и измененото предложение). По-голямото разнообразие от механизми за прилагане ще доведе до по-голямо спазване и ефективно прилагане на разпоредбите на Директивата за неприкосновеност на личния живот и електронни комуникации като цяло.

Посрещане на предизвикателството

101. По отношение на всички посочени по-горе въпроси ЕП и Съветът трябва да посрещнат предизвикателството да изготвят подходящи правила и разпоредби, които са работещи, функционални и зачитат правата на лицата на неприкосновеност на личния живот и защита на данните. ЕНОЗД изразява надежда, че участниците ще положат максимални усилия за посрещане на това предизвикателство и че настоящото становище ще допринесе в това начинание.

Съставено в Брюксел на 9 януари 2009 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните