I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА ДАННИТЕ

Становище на Европейския надзорен орган по защита на данните относно повишаване на доверието в информационното общество чрез насърчаване на защитата на данните и на неприкосновеността на личния живот

(2010/C 280/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

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

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

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година 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 защитата на правото на неприкосновеност 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 ([3]), и по-специално член 41 от него,

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

1. Информационните и комуникационните технологии (ИКТ) предлагат огромни възможности в практически всеки аспект от нашия живот — как работим, играем, общуваме и се образоваме. Те са от решаващо значение за днешната информационна икономика и за обществото като цяло.

2. Европейският съюз е глобална сила в иновационните ИКТ и е решен да остане такава. За посрещането на това предизвикателство Европейската комисия се очаква скоро да приеме нова Европейска програма за цифрово развитие, която комисар Kroes потвърди като свой приоритет ([4]).

3. ЕНОЗД осъзнава ползите от ИКТ и изразява съгласие, че ЕС трябва да положи максимални усилия за насърчаване на тяхното развитие и широкото им приемане. Той също така подкрепя становищата на комисари Kroes и Reding, че физическите лица трябва да заемат централно място в тази нова среда ([5]). Физическите лица трябва да могат да разчитат на способността на ИКТ да запази тяхната информация сигурно и да контролира нейното използване, както и да бъдат уверени, че техните права за неприкосновеност на личния живот и защита на данните ще бъдат спазвани в цифровото пространство. Спазването на тези права е от съществено значение за генериране на доверието на потребителите. А това доверие е решаващо за широкото използване от гражданите на новите услуги ([6]).

([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.

([4]) Отговори на въпросника на Европейския парламент за комисар Neelie Kroes във връзка с изслушванията в ЕП, предшестващи назначението на комисаря.

([5]) Отговори на въпросника на Европейския парламент за комисар Neelie Kroes във връзка с изслушванията в ЕП, предшестващи назначението на комисаря; изказване на комисар Viviane Reding относно „Европейска програма за цифрово развитие за новия цифров потребител“ пред форума на множество заинтересовани страни към Европейската организация на потребителите BEUC „Лична сфера на потребителите и онлайн маркетинг: пазарни тенденции и политически перспективи“, Брюксел, 12 ноември 2009 г.

([6]) Вж. например доклада на RISEPTIS „Доверието в информационното общество“, доклад на консултативния съвет по RISEPTIS (Научни изследвания и иновации относно сигурността, неприкосновеността на личния живот и надеждността в информационното общество). Може да бъде намерен на адрес: http://www.think-trust.eu/general/news-events/riseptis-report.html. Вж. също: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. ЕС притежава силна правна рамка за защита на данните/неприкосновеност на личния живот, чиито принципи остават изцяло валидни в цифровата ера. Това обаче не е основание за самодоволство. В много случаи ИКТ създават причини за загриженост, които не са уредени в съществуващата рамка. Необходимо е следователно да се предприеме нещо, за да се гарантира, че индивидуалните права, залегнали в законодателството на ЕС, продължават да осигуряват ефективна защита в тази нова среда.

5. Настоящото становище обсъжда мерките, които може да бъдат поощрени или предприети от Европейския съюз, с цел да се гарантира защита на личния живот и на данните на лицата в един глобализиран свят, чийто двигател ще бъдат и занапред технологиите. В него се обсъждат законодателни и незаконодателни инструменти.

6. След общ преглед на ИКТ като ново развитие, което създава възможности, но крие и рискове, в становището се обсъжда необходимостта защитата на данните и неприкосновеността на личния живот да бъдат интегрирани на практическо равнище от самото начало на новите информационни и комуникационни технологии (така нареченият по-нататък „принцип за защита на личния живот още при разработването“). За да се осигури спазването на този принцип, в становището се обсъжда необходимостта „принципът за защита на личния живот още при разработването“ да бъде заложен в правната рамка за защита на данните по най-малко два различни начина. Първо, чрез включването му като общ, обвързващ принцип и второ, чрез включването му в конкретни области на ИКТ, създаващи специфични рискове за защита на данните/неприкосновеност на личния живот, които могат да бъдат намалени чрез подходяща техническа архитектура и разработка. Тези области са радиочестотната идентификация (RFID), приложенията на социалната мрежа и приложенията на браузърите. Накрая в становището се предлагат други инструменти и принципи, имащи за цел защита на личния живот и данните на лицата в сектора на ИКТ.

7. При това в становището се изясняват някои въпроси, поставени от работната група по член 29 в нейния принос към обществения обсъждане на бъдещето на неприкосновеността на личния живот ([1]). То се основава освен това на предходни становища на ЕНОЗД, като становището от 25 юли 2007 г. относно прилагането на Директивата за защита на данните, становището от 20 декември 2007 г. относно RFID и неговите две становища относно Директивата за правото на неприкосновеност на личния живот и електронни комуникации ([2]).

II. ИКТ ПРЕДЛАГАТ НОВИ ВЪЗМОЖНОСТИ, НО СЪЗДАВАТ И НОВИ РИСКОВЕ

8. ИКТ могат да бъдат сравнени с други важни открития от миналото, като електричеството. Може би е наистина рано още да бъде оценена историческата им роля, но връзката между ИКТ и икономическия растеж в развитите страни е ясно изразена. ИКТ създадоха заетост, икономически ползи и допринесоха за общото благосъстояние. Въздействието на ИКТ далеч не е само чисто икономическо, тъй като те изиграха важна роля за насърчаване на иновациите и творчеството.

9. Освен това ИКТ преобразиха начина, по който хората работят, общуват и си взаимодействат. Така например хората все повече разчитат на ИКТ за социалните и икономическите взаимодействия. Гражданите могат да използват широка гама от нови приложения на ИКТ, като електронно здравеопазване (eHealth), електронни транспортни услуги (eTransport), електронни услуги на публичните административни органи (eGoverment), както и иновационни интерактивни системи за развлечение и обучение.

10. В светлината на тези ползи всички европейски институции се ангажираха да подкрепят ИКТ като необходим инструмент за подобряване на конкурентоспособността на европейската промишленост и за ускоряване на икономическото възстановяване на Европа. И наистина, през август 2009 г. Комисията прие Доклад за конкурентоспособността на Европа по отношение на цифровите технологии ([3]) и започна публично обсъждане на подходящи бъдещи стратегии за насърчаване развитието на ИКТ. На 7 декември 2009 г. Съветът даде своя принос към това обсъждане под надслов „Стратегия след i2010 — към открито, зелено и компетентно общество на знанието“ ([4]). Европейският парламент прие току-що

([1]) Становище 168 на работната група по член 29 относно бъдещето на неприкосновеността на личния живот, съвместен документ по обсъждането на Европейската комисия на правната рамка за защита основното право на защита на личните данни, прието на 1 декември 2009 г.

([2]) Становище от 25 юли 2007 г. относно Съобщението на Комисията до Европейския парламент и 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; становище от 20 декември 2007 г. относно съобщението на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно радиочестотната идентификация (RFID) в Европа: стъпки към изграждане на политическа рамка (COM(2007) 96), ОВ C 101, 23.4.2008 г., стр. 1; становище от 10 април 2008 г. 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), ОВ C 181, 18.7.2008 г., стр. 1; Второ становище от 9 януари 2009 г. 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.

([3]) Доклад за конкурентоспособността на Европа по отношение на цифровите технологии — основни постижения на стратегията i2010 през периода 2005—2009 г. (SEC(2009) 1060).

([4]) Заключения на Съвета „Стратегия след i2010 — към открито, зелено и компетентно общество на знанието“. (17107/09), приети на 18.12.2009 г.

доклад, имащ за цел да предостави указания на Комисията за определяне на програма за цифрово развитие ([1]).

11. С възможностите и ползите, съпътстващи развитието на ИКТ, идват нови рискове, по-специално за неприкосновеността на личния живот и защитата на личните данни на физическите лица. ИКТ често водят до нарастване (много често по начини, които остават извън погледа на гражданите) на обема на информацията, която се събира, сортира, филтрира, предава или по друг начин се задържа, така че рисковете за тези данни се умножават.

12. Така например чиповете за радиочестотна идентификация (RFID) заместват баркодовете на (някои) потребителски продукти. Чрез подобряване на информационния поток във веригата за доставки (като по този начин се намали необходимостта от „осигурителни“ запаси, дават се по-точни прогнози и пр.), новата система се очаква да бъде от полза както за бизнеса, така и за потребителите. Същевременно това обаче увеличава смущаващата възможност за проследяване за различни цели и от различни субекти посредством лични маркировки.

13. Друг пример са „изчислителните облаци“ и преди всичко доставката на хоствани потребителски и непотребителски приложни услуги по интернет. Към последните спадат от фотобиблиотеки, календари, уебпоща и база данни за потребителите до по-сложни услуги, свързани с търговската дейност. Ползите както за фирмите, така и за гражданите са несъмнени: намаляване на разходите (разходите са вътрешноприсъщи), независимост от местоположението (лесен достъп до информацията навсякъде по света), автоматичност (не са необходими специално отделени ИТ ресурси, актуализации на софтуера) и пр. Същевременно съществуват рискове от проблеми със сигурността и недобронамерени действия и те са съвсем реални. Има също опасност от загуба на достъп и на контрола върху собствените данни.

14. Установено е, че ползите и рисковете вървят ръка за ръка и в други области, използващи ИКТ приложения. Такъв например е случаят с електронното здравеопазване, което може да повиши ефективността, да намали разходите, да увеличи достъпността и общо взето да подобри качеството на здравните услуги. Електронното здравеопазване обаче поставя често въпроса за легитимността на вторичното използване на информацията от него, което изисква внимателен анализ на целите на всяко потенциално вторично използване ([2]). Освен това поради все по-широкото използване на електронните здравни досиета самите системи са преследвани от скандали, разкриващи много случаи на недобронамерени действия с електронните здравни досиета.

15. В заключение, известна степен остатъчен риск вероятно ще се запази, дори след извършване на правилни оценки и прилагане на необходимите мерки. Нереалистично е да се мисли за ситуация с нулев риск. Както се вижда обаче от следващото обсъждане, възможно е и трябва да се прилагат мерки за намаляване на този риск до приемливи равнища.

III. ПРИНЦИПЪТ ЗА ЗАЩИТА НА ЛИЧНИЯ ЖИВОТ ОЩЕ ПРИ РАЗРАБОТВАНЕТО КАТО КЛЮЧОВ ИНСТРУМЕНТ ЗА СЪЗДАВАНЕ НА ЛИЧНО ДОВЕРИЕ В ИКТ

16. Потенциалните ползи от ИКТ могат да бъдат почувствани на практика само ако са в състояние да създадат доверие, с други думи, ако могат да гарантират готовността на потребителя да зависи от ИКТ заради техните характеристики и ползи. Такова доверие ще бъде създадено само ако ИКТ са надеждни, сигурни, под контрола на хората и ако запазването на техните лични данни и неприкосновеността на личния им живот са гарантирани.

17. Широко разпространените рискове и проблеми като показаните по-горе, особено когато водят до злоупотреба или нарушение на личните данни, излагащи на опасност неприкосновеността на личния живот на лицата, има вероятност да застрашат доверието на потребителите в информационното общество. Това може да изложи на сериозна опасност развитието на ИКТ и ползите, които те могат да дадат.

18. Решението на тези рискове за неприкосновеността на личния живот и защитата на данните не може обаче да се състои в премахване, изключване или отказ от използване или от насърчаване на ИКТ. Това не е нито възможно, нито реалистично; то би попречило на гражданите да получат ползите от ИКТ и би ограничило сериозно общите предимства, които може да бъдат спечелени.

19. ЕНОЗД е убеден, че по-положителното решение е разработването и развитието на ИКТ по начин, който зачита неприкосновеността на личния живот и защитата на данните. Ето защо е от решаващо значение неприкосновеността на личния живот и защитата на данните да представляват неразделна част от целия жизнен цикъл на технологията, от най-първия етап на разработването чак до окончателното им разгръщане, използване и разполагаемост. Това обикновено се означава като „принцип за защита на личния живот още при разработването“ (PbD), който е разгледан по-долу.

20. PbD може да доведе до различни мерки в зависимост от конкретния случай на приложение. В някои случаи това може да наложи например заличаване/намаляване на личните данни или предотвратяване на ненужното или нежеланото им обработване. В други случаи принципът на PbD може да бъде свързан с предлагане на инструменти

([1]) Доклад относно определяне на нова програма за цифрово развитие на Европа: от i2010 до digital.eu (2009/2225 (INI)), приет на 18.3.2010 г.

([2]) Например продажбата или използването на здравна информация, събрана за целите на предоставяне на лечение, не могат да бъдат използвани за подбор на сайтове за сателитни клиники, за създаване на амбулаторни хирургични проекти, а всякакви други начини на планиране на бъдещи дейности с финансови последици изисква внимателно проучване.

за повишаване на контрола на лицата върху техните лични данни. Такива мерки трябва да се имат предвид при определянето на стандартни и/или най-добри практики. Те могат освен това да бъдат вградени в архитектурата на системите за информация и комуникация или в структурните организации на субектите, които обработват лични данни.

III.1. **Принципът за защита на личния живот още при разработването, приложим в различни среди, създадени от ИКТ, и тяхното въздействие**

21. Необходимостта от принципа на PbD може да бъде установена в голям брой различни среди, създадени от ИКТ. Секторът на здравеопазването например разчита все повече на ИКТ инфраструктури, които често изискват централизирано съхранение на здравните данни на пациентите. Прилагането на принципа на PbD в сектора на здравеопазването ще изисква оценка на адекватността на различни мерки, като възможност за минимизиране на централно съхраняваните данни и ограничаването им в индекс, използване на инструменти за криптиране, предоставяне на право на достъп само на тези, които трябва да знаят дънните, анонимизиране на данните след като престанат да бъдат необходими и т.н.

22. По подобен начин транспортните системи все повече се снабдяват по подразбиране със съвременни ИКТ приложения, които си взаимодействат с моторното превозно средство и неговата среда за различни цели и функции. Така например автомобилите все по-често се оборудват с нови ИКТ функции (GPS, GSM, мрежа от датчици и пр.), които показват не само тяхното местоположение, но и техническото им състояние в реално време. Тази информация може да бъде използвана например за заместване на съществуващата система за пътни такси с такса, която зависи от ползването на пътя. Прилагането на PbD при разработване на архитектурата на такива системи трябва да позволява обработката и предаването по-нататък на колкото се може по-малък брой лични данни ([1]). В съответствие с този принцип децентрализираните или полудецентрализиланите архитектури, ограничаващи разкриването на данни за местоположението до един централен пункт, са за предпочитане пред централизираните.

23. Горните примери показват, че когато информационните и комуникационните технологии се изграждат в съответствие с принципа на PbD, рисковете за неприкосновеността на личния живот и защитата на данните може да бъдат значително намалени до минимум.

III.2. **Недостатъчно внедряване на ИКТ, прилагащи принципа на PbD**

24. Важен въпрос е дали икономическите оператори, производителите/доставчиците на ИКТ и администраторите на данни са заинтересовани от маркетинга и прилагането на принципа на PbD в ИКТ. В този контекст е важно също да се направи оценка на търсенето на PbD от страна на потребителите.

25. През 2007 г. Комисията публикува съобщение, призоваващо предприятията да използват иновационния си капацитет за създаване и прилагане на PETs като начин за подобряване на защитата на личния живот и личните данни от самото начало на цикъла на разработване ([2]).

26. Към настоящия момент обаче наличните данни показват, че нито производителите на ИКТ, нито администраторите на лични данни (както в частния, така и в публичния сектор) не са успели последователно да прилагат или продават PbD. Излагат се различни основания, в това число липса на икономически стимули или на институционална подкрепа, недостатъчно търсене и т.н. ([3]).

27. Същевременно търсенето от потребителите на PbD е доста слабо. Потребителите на продукти и услуги на ИКТ може да считат надлежно, че техният личен живот и личните им данни са де факто защитени, докато в много случаи това не е така. В някои случаи те просто не са в състояние да предприемат мерките за сигурност, необходими за защита на собствените им лични данни или данните на други лица. Много пъти това е така, защото те не познават напълно, нито дори отчасти, рисковете. Така например младите хора, общо казано, пренебрегват рисковете за неприкосновеността на личния живот, свързани с показване на лична информация в социалните мрежи, и често пренебрегват настройките за неприкосновеност на личния живот. Други потребители пък съзнават рисковете, но може да нямат необходимите технически познания за прилагане на технологиите за защита, като тези за защита на тяхната интернет връзка или за корекция на настройките на браузъра за свеждане до минимум на създаването на профили чрез проследяване на търсенията им в мрежата.

28. Рисковете за защита на личния живот и данните са обаче напълно реални. Ако защитата на личния живот и данните не се вземе предвид още от самото начало, често е много късно и икономически обременително да се коригират системите и много късно да се поправят вече нанесените

([1]) Становище на Европейския надзорен орган по защита на данните от 22 юли 2009 година относно съобщението на Комисията „План за действие за внедряване на интелигентните транспортни системи в Европа“ и придружаващото го предложение за директива на Европейския парламент и на Съвета за установяване на рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и взаимодействие с останалите видове транспорт, което може да бъде намерено на адрес: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_BG.pdf

([2]) Съобщение от 2.5.2007 година COM(2007) 228 окончателен на Комисията до Европейския парламент и Съвета относно насърчаване на защитата на личните данни чрез технологиите за подобряване на защитата на личния живот (PETs).

([3]) Проучване на икономическите ползи от технологиите за подобряване на защитата на личния живот (PETs), jls/2008/D4/036.

щети. Все по-големият брой нарушения на сигурността на данни през последните години онагледява много добре този проблем и засилва необходимостта от защита на личния живот още при разработването.

29. Гореизложеното ясно показва, че производителите и доставчиците на ИКТ технологии, предназначени за обработка на лични данни, трябва, заедно с администраторите на данни, да имат задължението да ги разработват с вградена защита на данните и на личния живот. В много случаи това би означавало те да бъдат проектирани със защита на личния живот по подразбиране.

30. На този фон трябва да обсъдим какви стъпки трябва да бъдат предприети от лицата, вземащи политически решения, за насърчаване на PbD в развитието на ИКТ. На първо място се поставя въпросът дали съществуващата правна рамка за защита на данните съдържа адекватни разпоредби за гарантиране на прилагането на принципа на PbD както от администраторите на данни, така и от производителите/проектантите. Вторият въпрос е какво следва да бъде направено в контекста на Европейската програма за цифрово развитие, за да се гарантира, че секторът на ИКТ ще създава доверие у потребителите.

IV. ЗАЛАГАНЕ НА ПРИНЦИПА ЗА ЗАЩИТА НА ЛИЧНИЯ ЖИВОТ ОЩЕ ПРИ РАЗРАБОТВАНЕТО В ЗАКОНОДАТЕЛНИТЕ АКТОВЕ И ПОЛИТИКИТЕ НА ЕС

IV.1. Настоящата правна рамка за защита на данните и личния живот

31. ЕС има солидна рамка за защита на данните и личния живот, заложена в Директива 95/46/ЕО ([1]), Директива 2002/58/ЕО ([2]) и съдебната практика на Европейския съд по правата на човека ([3]) и Съда на ЕС.

32. Директивата за защита на данните се прилага за „всяка операция или съвкупност от операции, които се извършват … по отношение на личните данни“ (събиране, съхранение, разкриване и т.н.). Тя налага спазване на определени принципи и задължения върху лицата, които обработват лични данни („администраторите на данни“). С нея се въвеждат индивидуални права, като правото на достъп до лична информация. Директивата за правото на неприкосновеност на личния живот и електронни комуникации е посветена специално на защитата на личния живот в сектора на електронните комуникации ([4]).

33. Настоящата директива за защита на данните не съдържа изрично изискване за PbD. Тя обаче включва разпоредби, които непряко, в различни ситуации, може да изискват прилагане на принципа на PbD. По-специално, член 17 изисква администраторите на данните да прилагат подходящи технически и организационни мерки за защита срещу незаконна обработка на данните ([5]). Следователно принципът на PbD е включен по един много общ начин. Освен това разпоредбите на тази директива са насочени главно към администраторите на данни и тяхната обработка на лична информация. Те не изискват изрично информационните и комуникационните технологии да бъдат приведени в съответствие със защитата на личния живот и данните, което налага да бъдат обхванати също проектантите и производителите на ИКТ, включително дейностите, извършвани на етапа на стандартизацията.

34. Директивата за правото на неприкосновеност на личния живот и електронни комуникации е по-ясна. Член 14, параграф 3 предвижда, че „когато се изисква, могат да се приемат мерки, за да се осигури терминалното оборудване да бъде конструирано по начин, който е съвместим с правото на потребителите да защитават и контролират използването на техните лични данни, в съответствие с Директива 1999/5/ЕО и Решение на Съвета 87/95/ЕИО от 22 декември 1986 година, относно стандартизация в областта на информационните технологии и съобщения“. Тази разпоредба обаче не е била никога използвана ([6]).

35. Въпреки че горните разпоредби на двете директиви допринасят за *насърчаването* на принципа за защита на личния живот още при разработването, на практика те не се оказаха достатъчни, за да се *гарантира* залагането на неприкосновеността на личния живот в ИКТ.

36. В резултат на това положение законът не изисква по достатъчно точен начин ИКТ да бъдат разработвани в съответствие с принципа на PbD. Освен това органите по защита на данните нямат достатъчно правомощия, за да гарантират залагането на PbD. Това води до неефективност. Така например органите за защита на данните може да

([1]) Директива 95/46/ЕО на Европейския парламент и на Съвета (наричана по-долу Директива за защита на данните).

([2]) Директива 2002/58/ЕО на Европейския парламент и на Съвета (наричана по-долу: Директива за неприкосновеност при електронните комуникации).

([3]) Тълкуване на основните елементи и условия, изложени в член 8 от Европейската конвенция за защита правата на човека и основните свободи (ECHR) , приета в Рим на 4 ноември 1950 година, както се прилагат в различни случаи.

([4]) Лисабонският договор засили тази защита, като призна зачитането на личния живот и защитата на личните данни като отделни основни права в членове 7 и 8 от Хартата на основните права на ЕС. Хартата на основните права на ЕС стана обвързваща с влизането в сила на Лисабонския договор.

([5]) Член 17 гласи както следва: „Държавите-членки предвиждат, че администраторът трябва да прилага подходящи технически и организационни мерки за защита на личните данни срещу случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп, в частност, когато обработването включва предаване на данните по мрежа, както и срещу всякакви други незаконни форми на обработка“. Съображение 46 го допълва със следния текст: „като имат предвид, че защитата на правата и свободите на съответните лица, по отношение на обработването на лични данни, изисква да бъдат взети съответни технически и организационни мерки, както при разработването на системата за обработка, така и по време на самата обработка, и по-конкретно с цел да се поддържа сигурността и по такъв начин да се предотврати всякаква неразрешена обработка“.

([6]) Комисията съобщи за своите планове да актуализира Директива 1999/5/ЕО към края на 2010 г.

имат правомощия да налагат санкции за оставяне без отговор на искания за достъп, направени от физически лица, и компетенцията да изискват изпълнението на някои мерки за предотвратяване на незаконна обработка на данни. Невинаги обаче е достатъчно ясно дали техните правомощия стигат дотам да изискват системата да бъде разработена по начин, който улеснява правата на лицата за защита на данните ([1]). Например въз основа на съществуващите правни разпоредби не е ясно дали може да се изисква архитектурата на информационната система да бъде проектирана по начин, който да улеснява реакцията на дружествата на искания за достъп, направени от физически лица, така че подобни искания да бъдат обработвани автоматично и по-бързо. Освен това по-късните опити за промяна на технологията, след като тя е била вече разработена или инсталирана, може да доведат до разнородни решения, които не са напълно работещи, освен че са и икономически неизгодни.

37. Според ЕНОЗД, чието становище се споделя с работната група по член 29 ([2]), настоящата правна рамка оставя място за по-ясно изразено утвърждаване на принципа на PbD.

IV.2. **Залагане на различни равнища на принципа за защита на личния живот още при разработването**

38. С оглед на гореизложеното ЕНОЗД препоръчва на Комисията следните подходи на действие:

а) да предложи включването на обща разпоредба относно PbD в правната рамка за защита на данните;

б) да разработи тази обща разпоредба в специфични разпоредби, когато се предлагат специфични правни инструменти в различните сектори. Тези специфични разпоредби могат отсега да бъдат включени в правните инструменти въз основа на член 17 от Директивата за защита на данните (и друго съществуващо законодателство);

в) да включи PbD като ръководен принцип в Европейската програма за цифрово развитие;

г) да въведе PbD като принцип в други инициативи на ЕС (главно незаконодателни).

Обща разпоредба относно PbD

39. ЕНОЗД предлага принципът за защита на личния живот още при разработването да бъде включен недвусмислено и изрично в съществуващата регулаторна рамка за защита на данните. Това ще направи принципа на PbD по-силен, по-ясен и ще наложи ефективното му изпълнение, като освен това ще придаде повече легитимност на правоприлагащите органи да изискват фактическото му прилагане на практика. Това е особено необходимо в светлината на посочените по-горе факти — не само значението на самия принцип като инструмент за засилване на доверието, но и като стимул за заинтересованите страни да прилагат PbD и да повишават гаранциите, предвидени в съществуващата правна рамка.

40. Това предложение се основава на препоръката на работната група по член 29 за въвеждане на принципа за „защита на личния живот още при разработването“ като общ принцип в правната рамка на защита на данните, и по-специално в Директивата за защита на данните. Според работната група по член 29: „Този принцип трябва да бъде обвързващ за проектантите и производителите на технологии, както и за администраторите на данни, чието задължение е да решават какво ИКТ оборудване да бъде придобито и използвано. Те трябва да бъдат задължени да имат предвид технологичната защита на данните още на стадия на планиране на информационно-технологичните производители и системи. Доставчиците на такива системи или услуги, както и администраторите, трябва да покажат, че са взели всички необходими мерки за изпълнението на тези изисквания“.

41. Освен това ЕНОЗД приветства подкрепата от страна на комисар Viviane Reding на принципа за защита на личния живот още при разработването, изказана във връзка с обявеното преразглеждане на Директивата за защита на данните ([3]).

42. Това води до съдържанието на такава разпоредба. На първо място и най-важно е общият принцип за защита на личния живот още при разработването да бъде технологично неутрален. Принципът не трябва да има за цел да регулира технологията, т.е. той не бива да предписва конкретни технически решения. Вместо това той трябва да изисква съществуващите принципи за защита на

([1]) Вж. доклада на службата на комисаря по информационните въпроси на Обединеното кралство под надслов: „Защита на личния живот още при разработването“, публикуван през ноември 2008 г.

([2]) Вж. Становище 168 на работната група по член 29 относно бъдещето на неприкосновеността на личния живот, съвместен документ по обсъждането на Европейската комисия на правната рамка за защита основното право на защита на личните данни, прието на 1 декември 2009 г.

([3]) „Защитата на личния живот още при разработването“ е принцип, който е в интереса както на гражданите, така и на предприятията. Защитата на личния живот още при разработването ще доведе до по-добра защита за лицата, както и до доверие в новите услуги и продукти, което от своя страна ще окаже положително въздействие върху икономиката. Има някои окуражителни примери, но много повече трябва да се направи. Програмно изказване по случай Деня на защита на данните, 28 януари 2010 г., Европейски парламент, Брюксел.

личния живот и данните да бъдат заложени в информационните и комуникационните системи и решения. Това ще позволи на заинтересованите страни, производителите, администраторите на данни и ОЗД да тълкуват значението на принципа във всеки отделен случай. На второ място, спазването на принципа трябва да бъде задължително на различните етапи — от създаването на стандартите и разработването на архитектурата до тяхното прилагане от администратора на лични данни.

Разпоредби в специфичните правни инструменти

43. Настоящите и бъдещите правни инструменти трябва да включват принципа за PbD въз основа на настоящата правна рамка, а след приемането на предложената по-горе обща разпоредба — въз основа на нея. Така например съгласно настоящите инициативи, свързани с интелигентните транспортни системи, Комисията носи конкретна първоначална отговорност при определянето на мерките, инициативите за стандартизация, процедурите и най-добрите практики. При изпълнението на тези задачи принципът за PbD трябва да бъде водещ.

44. ЕНОЗД отбелязва освен това, че принципът за защита на личния живот още при разработването има специфично значение и в областта на свободата, сигурността и правосъдието, както е предвидено в Стокхолмската програма ([1]). В своето становище относно Стокхолмската програма ЕНОЗД подчерта, че архитектурата за обмен на информация трябва да се основава на принципа за „защита на личния живот още при разработването“ ([2]): „По-конкретно това означава, че информационните системи, разработени за цели на обществената сигурност, следва винаги да се изграждат в съответствие с принципа на „защита на личния живот още при проектирането“.“

45. В становището на работната група по член 29 относно бъдещето на неприкосновеността на личния живот ([3]) се настоява с дори още по-точни думи, че в областта на свободата, сигурността и правосъдието — където публичните органи са основните фактори и където мерките за засилване на надзора оказват непосредствено въздействие върху основите права на защита на личния живот и на данните — изискванията за защита на личния живот още при разработването трябва да станат задължителни. Чрез въвеждане на тези изисквания в информационните системи правителствата ще насърчат защитата на личния живот още при разработването и в своето качество на първоначални клиенти.

PbD като ръководен принцип в Европейската програма за цифрово развитие

46. Информационните и комуникационните технологии стават все по-сложни и водят до по-големи рискове за защита на личния живот и данните. Общо взето, цифровизираната информация, достъпът до която е по-лесен и която може по-лесно да бъде копирана и предавана, е изложена на много по-големи рискове от информацията на хартиен носител. С придвижването ни към мрежи от взаимосвързани обекти рисковете ще се увеличават. Колкото по-големи са рисковете за защита на личния живот/данните, толкова по-голямо ще бъде търсенето на засилени предпазни мерки за защита на данните/личния живот. Следователно обосновките за необходимостта от прилагане на PbD са още по-необходими в сектора на ИКТ. Освен това, както беше посочено по-горе, доверието на физическите лица в ИКТ е от основно значение, за да може гражданите да използват широко тези нови услуги, а защитата на личния живот и данните са ключови елементи на такова доверие.

47. Горното подчертава, че стратегията за развитие на ИКТ трябва да потвърждава необходимостта тези услуги да бъдат разработвани с включен в тях елемент на защита на личния живот и данните, т.е. в съответствие с принципа за защита на личния живот още при разработването.

48. Ето защо Европейската програма за цифрово развитие трябва изрично да подкрепи принципа за защита на личния живот още при разработването като необходим елемент за гарантиране на доверието на гражданите в ИКТ и онлайн услугите. Тя трябва да признае, че неприкосновеността на личния живот и доверието вървят ръка за ръка и че принципът за защита на личния живот още при разработването следва да бъде водещ фактор при разработването на един заслужаващ доверие сектор на ИКТ.

PbD като принцип в други инициативи на ЕС

49. Комисията трябва да се ръководи от принципа за защита на личния живот още при разработването при прилагане на политиките, дейностите и инициативите в специфични сектори на ИКТ, включително електронно здравеопазване, електронно възлагане на обществени поръчки, електронно социално осигуряване, електронно обучение и т.н. Много от тези инициативи ще бъдат отделни действия в Европейската програма за цифрово развитие.

50. Това ще рече например, че инициативите, гарантиращи по-ефикасни и по-съвременни приложения за електронната публична администрация, така че гражданите да могат да си взаимодействат с нея, трябва да включват необходимостта те да бъдат разработвани и да работят в съответствие с принципа за защита на личния живот още при разработването. Същото се отнася и до политиките и дейностите на Комисията, насочени към по-бърз интернет, по-добро цифрово съдържание или общо насърчаване на фиксираните и безжичните комуникации и предаването на данни.

([1]) Стокхолмската програма — отворена и сигурна Европа в услуга и за защита на гражданите, приета от Европейския съвет през декември 2009 г.

([2]) Становище от 10 юли 2009 г. относно съобщението на Комисията до Европейския парламент и Съвета „Пространство на свобода, сигурност и правосъдие за гражданите“, ОВ C 276, 17.11.2009 г., стр. 8, съображение 60.

([3]) Становище 168 на Работната група по член 29 относно бъдещето на неприкосновеността на личния живот, съвместен принос към консултациите на Европейската комисия по правната рамка за основното право на защита на личните данни, прието на 1 декември 2009 г.

51. Тук спадат също области, в които Комисията отговаря за широкомащабните ИТ системи като ШИС и ВИС, както и за случаите, при което отговорността на Комисията е сведена до разработването и поддръжката на общата инфраструктура на подобна система, като Европейската информационна система за съдимост (ECRIS).

52. Точното развитие на принципа PbD ще зависи от всеки конкретен сектор и от всяка конкретна ситуация. Така например когато инициативите на Комисията се съпътстват от законодателни предложения в конкретен сектор на ИКТ, в много случаи ще бъде уместно да се включи изрично позоваване на принципа PbD, приложим при разработването на конкретното ИКТ приложение или конкретната ИКТ система. Ако се разработват планове за действие за конкретна област, те трябва да осигуряват систематично прилагане на правната рамка, и по-специално да гарантират, че съответната ИКТ технология е изградена с оглед на принципа за защита на личния живот още при разработването.

53. Що се отнася до изследователската дейност, Седмата рамкова програма и следващите трябва да бъдат използвани като инструмент в помощ на проекти, насочени към анализ на стандарти, ИКТ технологии и архитектура, които служат по-добре на неприкосновеността на личния живот, и по-специално на принципа за защита на личния живот още при разработването. Освен това PbD трябва да бъде необходим елемент и от обсъждането на по-широки ИКТ проекти, имащи за цел обработката на лични данни на физически лица.

Области от специален интерес

54. В някои случаи поради особено големите рискове за неприкосновеността на личния живот и данните на лицата или заради други фактори (нежелание на индустрията да доставя PbD продукти, потребителско търсене и пр.) може да се наложи по-ясно и конкретно определяне на мерките за защита на личния живот още при разработването, които трябва да станат неразделна част от даден тип ИКТ продукт или технология, било в съответни законодателни инструменти, било по друг начин.

55. ЕНОЗД е определил различни области (RFID, приложения за работа в мрежа и браузъри), които според него заслужават на този етап внимателно разглеждане от страна на Комисията на по-практичните мерки, препоръчани по-горе. Тези три области са обсъдени допълнително по-долу.

V. **РАДИОЧЕСТОТНА ИДЕНТИФИКАЦИЯ (RFID)**

56. Радиочестотните приемо-предаватели могат да бъдат прикрепени към предмети, животни и хора. Те могат да се използват за събиране и съхранение на лични данни, като медицински досиета, за проследяване движението на хора или за съставяне на профил на тяхното поведение за различни цели. Това може да се направи без знанието на съответния човек ([1]).

57. Ефективните гаранции относно защитата на данните, неприкосновеността на личния живот и всички свързани с това етични измерения са решаващи за доверието на обществеността в RFID и бъдещия Интернет на нещата. Само тогава технологията ще може да принесе своите многобройни икономически и обществени ползи.

V.1. **Пропуските в правната рамка на приложимата защита на данните**

58. Директивата за защита на данните и Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилагат при събирането на данни, извършвано чрез използване на RFID ([2]). Това изисква, наред с други неща, при работата с използване на RFID да бъдат въведени адекватни предпазни мерки за неприкосновеността на личния живот ([3]).

59. Тази правна рамка обаче не отстранява напълно всички причини за загриженост относно защитата на данните и неприкосновеността на личния живот, породени от тази

([1]) RFID означава радиочестотна идентификация. Основните компоненти на технологията или инфраструктурата на радиочестотната идентификация са *приемо-предавател* (т.е. микрочип), четящо устройство и приложение, свързано с приемо-предавателите и четящите устройства чрез мидълуер (междинен софтуер), и обработка на получените данни. Приемо-предавателят се състои от електронна верига, съхраняваща данни, и антена, която предава данните чрез радиовълни. Четящото устройство има антена и демодулатор, който преобразува постъпващата аналогова информация от радиовръзката в цифрови данни. След това информацията може да бъде изпратена чрез мрежи до бази данни и сървъри, за да бъде обработена с компютър.

([2]) Директивата за правото на неприкосновеност на личния живот и електронни комуникации се позовава на RFID в член 3: „Настоящата директива се прилага при обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Общността, включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация“. Това се допълва от съображение 56: „Технологичният напредък позволява разработването на нови приложения, основани на устройства за събиране на данни и идентификация, които могат да бъдат безконтактни устройства, използващи радиочестоти. Например устройствата за радиочестотна идентификация (RFID) използват радиочестоти за събиране на данни от уникално идентифицирани етикети, които след това могат да се пренасят през съществуващи съобщителни мрежи. Широката употреба на такива технологии може да донесе значителни икономически и социални ползи и поради това може да направи значителен принос към вътрешния пазар, ако такава употреба е приемлива за гражданите. За да се постигне тази цел, е необходимо да се гарантира спазването на всички основни права на хората, включително правото на неприкосновеност на личния живот и защита на данните. Когато такива устройства са свързани към обществено достъпни електронни съобщителни мрежи или използват електронни съобщителни услуги като основна инфраструктура, следва да се прилагат съответните разпоредби на Директива 2002/58/ЕО (Директива за правото на неприкосновеност на личния живот и електронни комуникации), включително тези относно сигурността, данните за трафика и местонахождението и за поверителността“.

([3]) Така например член 17 от Директивата за защита на данните задължава да бъдат прилагани подходящи технически и организационни мерки за защита на личните данни срещу случайно или неправомерно унищожаване или неразрешено разкриване.

технология. Това е така, защото директивите не са достатъчно подробни по отношение на предпазните мерки, които трябва да се прилагат при използване на RFID. Съществуващите правила трябва да бъдат допълнени с допълнителни, които да налагат специални предпазни мерки, като по-специално правят задължително интегрирането на технически решения (принцип за защита на личния живот още при разработването) в технологията на RFID. Това е вярно за приемо-предавателите, съхраняващи лична информация, които трябва да имат команди „kill“ за дезактивиране и използване на криптография, когато съхраняват определени видове лична информация.

V.2. **Саморегулирането като първа стъпка**

60. През март 2007 г. Комисията прие съобщение ([1]), в което, наред с други неща, се признава необходимостта от подробни указания за практическото изпълнение на RFID и целесъобразността от приемане на критерии за разработване, за да се избегнат рисковете за неприкосновеността на личния живот и сигурността.

61. За постигането на тези цели през май 2009 г. Комисията прие препоръка относно спазването на принципите за неприкосновеност на личния живот и защита на данните в приложения, използващи радиочестотна идентификация ([2]). При използване на RFID в търговията на дребно се изисква дезактивиране на приемо-предавателя в точката на продажба, освен ако лицата не са дали съгласието си той да остане активиран. Това е в сила, освен ако оценката на въздействието на защитата на личния живот и на данните не доказва, че приемо-предавателите не представляват вероятна заплаха за защитата на личните данни, като в такъв случай те могат да останат активирани след точката на продажба, освен ако лицата не се откажат от тази опция безплатно.

62. ЕНОЗД е съгласен с подхода на Комисията да използва инструменти за саморегулиране. Както е описано обаче по-долу, възможно е саморегулирането да не даде очакваните резултати; ето защо той приканва Комисията да има готовност за приемането на алтернативни мерки.

V.3. **Проблемни области и възможни допълнителни мерки при неуспех на саморегулирането**

63. ЕНОЗД проявява загриженост, че организациите, използващи RFID в търговията на дребно, може да не вземат предвид възможността приемо-предавателите за RFID да бъдат проследени от нежелани трети страни. Такова проследяване може да разкрие личните данни, съхранявани в приемо-предавателя (ако има такъв), но може също така да даде възможност на трета страна да разпознае дадено лице с течение на времето, просто като използва уникалните идентификатори, съдържащи се в един или няколко приемо-предавателя, носени от физическото лице, в среда, която може да бъде дори извън оперативния периметър на използването на RFID. Той е загрижен освен това, че оператори, използващи RFID, може да се изкушат да разчитат необосновано на изключение и по този начин да оставят приемо-предавателя действащ след пункта за продажба.

64. Ако това се случи, може да се окаже късно да бъдат намалени рисковете за защитата на личните данни и неприкосновеността на личния живот на лицата, които може да са били вече нарушени. Освен това, като се има предвид естеството на саморегулирането, националните правоприлагащи органи може да се окажат в по-слаби позиции, когато искат от организациите, работещи с използване на RFID, да прилагат специфични мерки за защита на личния живот още при разработването.

65. В светлината на гореизложеното ЕНОЗД призовава Комисията да има готовност да предложи законодателни документи, регулиращи основните въпроси на използването на RFID в случай че ефективното прилагане на съществуващата правна рамка не проработи. Оценката на Комисията не трябва да се отлага необосновано, защото отлагането ще изложи гражданите на риск, а ще окаже отрицателно въздействие и върху промишлеността, тъй като правната несигурност е твърде голяма и отстраняването на загнездилите се проблеми ще бъде по всяка вероятност по-трудно и по-скъпоструващо.

66. Сред мерките, които може да се окажат необходими, ЕНОЗД препоръчва прилагане на принципа на предварителното съгласие в точката на продажба, според който всички приемо-предаватели за RFID, прикрепени към потребителските продукти, ще бъдат дезактивирани по подразбиране в точката на продажба. Може да не е необходимо, нито уместно, Комисията да определи конкретната технология, която да се използва. Вместо това законодателството на Съюза трябва да въведе правното задължение да се получи предварително съгласие, като се даде свобода на операторите да решават по какви начини ще бъде изпълнено изискването.

V.4. **Други въпроси, които трябва да бъдат обсъдени: Управление на Интернет на нещата**

67. Информацията, получена от приемо-предавателите за RFID — например информацията за продукта — може да бъде свързана към глобална мрежа на комуникационна инфраструктура. Тя обикновено се нарича „Интернет на нещата“. Възникват въпроси относно защитата на данните/неприкосновеността на личния живот, тъй като предметите от реалния свят може да бъдат идентифицирани от приемо-предавателите за RFID, които наред с информация за продукта може да включват лични данни.

68. Има много открити въпроси за това кой ще управлява съхраняваната информация, свързана с приемо-предавателите. Как ще бъде организирано съхранението? Кой ще има достъп до данните? През юни 2009 г. Комисията прие съобщение относно Интернет на нещата ([3]), в което бяха изрично посочени потенциалните проблеми за защитата на данните и неприкосновеността на личния живот, свързани с това явление.

([1]) Съобщение от Комисията от 15.3.2007 г. до Европейския парламент, Съвета, Икономическия и социален комитет и Комитета на регионите относно радиочестотната идентификация (RFID) в Европа: стъпки към изграждане на политическа рамка, COM(2007) 96 окончателен.

([2]) Препоръка на Комисията от 12.5.2009 година относно спазването на принципите за неприкосновеност на личния живот и защита на данните в приложения, използващи радиочестотна идентификация (C (2009) 3200 окончателен).

([3]) Съобщение от Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Интернет на нещата — план за действие за Европа, 18.6.2009 г., COM(2009) 278 окончателен.

69. ЕНОЗД би желал да подчертае някои от въпросите, поставени от съобщението, които според него заслужават повече внимание с развитието на Интернет на нещата. Първо, необходимостта от децентрализирана архитектура може да помогне за отчетността и приложимостта на правната рамка на ЕС. Второ, трябва да бъдат защитени в максимално възможната степен правата на лицата да не бъдат проследявани. С други думи, трябва да бъде рязко ограничен броят на случаите, когато гражданите биват проследявани чрез приемо-предаватели за RFID без тяхно съгласие. Това съгласие трябва да бъде изрично потвърдено. То е известно най-често като „мълчанието на чиповете“ и правото да бъдем оставени на спокойствие. Накрая, при разработване на Интернет на нещата принципът за защита на личния живот още при разработването трябва да бъде водещ. Това ще изисква например конкретните приложения на RFID, които имат вградени механизми за предоставяне на контрол на потребителите, да бъдат разработвани с настройки по подразбиране за неприкосновеност на личния живот.

70. ЕНОЗД очаква да бъде поискано неговото становище, когато Комисията въвежда мерките, предвидени в съобщението, и по-специално изготвянето на съобщението относно за неприкосновеността на личния живот и доверието в повсеместното информационно общество.

VI. **СОЦИАЛНИТЕ МРЕЖИ И НЕОБХОДИМОСТТА ОТ НАСТРОЙКИ ПО ПОДРАБЗИРАНЕ ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ**

71. Социалните мрежи са „шлагерът на деня“. Оказва се, че те са надминали електронната поща по популярност. Те свързват помежду им хора с подобни интереси и/или дейности. Хората могат да поставят профила си онлайн и да обменят медийни документи, като видеофилми, снимки, музика, както и професионалните си характеристики.

72. Младите хора бързо възприеха работата в социални мрежи и тази тенденция продължава. Средната възраст на потребителите на интернет в Европа намаля през последните няколко години: лицата на 9—10 години се свързват сега няколко пъти седмично; тези на 12 до 14 години влизат в интернет ежедневно, често пъти за един до три часа.

VI.1. **Социалните мрежи и приложимата правна рамка за защита на данните и неприкосновеност на личния живот**

73. Развитието на социалните мрежи даде възможност на потребителите да въвеждат в интернет информация за себе си и за трети страни. Правейки това, според работната група по член 29 ([1]) потребителите на интернет действат като администратори на данни съгласно член 2, буква г) от Директивата за защита на данните по отношение на въвежданите от тях данни ([2]). В повечето случаи обаче тази обработка се квалифицира като домашно изключение в съответствие с член 3, параграф 2 от Директивата. Същевременно доставчиците на социални мрежи се считат за администратори на данни, доколкото предоставят средствата за обработка на потребителски данни и всички основни услуги, свързани с потребителското управление (напр. регистриране и заличаване на потребителски имена).

74. В правно отношение това значи, че потребителите на интернет и доставчиците на социални мрежи споделят отговорността за обработката на лични данни като „администратори на данни“ по смисъла на член 2, буква г) от Директивата, макар и в различна степен и с различен набор от задължения.

75. Следователно потребителите трябва да знаят и да разбират, че като обработват своята лична информация и тази на други хора, те попадат под разпоредбите на законодателството на ЕС относно защитата на данните, което изисква, наред с други неща, да бъде взето информираното съгласие на тези, чиито данни се въвеждат, и предоставяне на засегнатите правото на коригиране, възражение и т.н. Аналогично доставчиците на социални мрежи са длъжни, наред с други неща, да използват подходящи технически и организационни мерки за предотвратяване на неразрешената обработка, като вземат предвид рисковете, свързани с обработката, и естеството на данните. Това на свой ред означава, че доставчиците на социални мрежи трябва да осигурят настройки по подразбиране за неприкосновеност на личния живот, включително такива, които ограничават достъп до профила на контактите на потребителя, избрани от самия него. Настройките трябва да изискват също изричното съгласие на потребителя, преди някой от профилите да стане достъпен за трети страни, като профилите с ограничен достъп не бива да се откриват от вътрешни браузъри.

76. За съжаление има несъответствие между законовите изисквания и фактическото им спазване. Докато в правно отношение потребителите на интернет се разглеждат като администратори на данни и са обвързани от правната рамка на ЕС за защита на данните и неприкосновеност на личния живот, всъщност те често не осъзнават тази своя роля. Общо казано, те не разбират добре, че обработват лични данни и че публикуването на така информация крие рискове за неприкосновеността на личния живот и защитата на данните. Младите хора по-специално изпращат онлайн съдържание, като подценяват последиците за себе си и другите, например във връзка с бъдещото им записване в учебни заведения или при търсене на работа.

([1]) Вж. Становище на работната група по член 29, 163 5/2009, относно работата в социалните мрежи, прието на 12 юни 2009 година.

([2]) „Администратор“ означава физическо или юридическо лице, държавен орган, агенция или друг орган, който сам или съвместно с други определя целите и средствата на обработка на лични данни; когато целите и средствата на обработката се определят от национални или общностни законови или подзаконови разпоредби, администраторът или специфичните критерии за неговото назначаване могат да бъдат определени в националното право или в правото на Общността.

77. Същевременно доставчиците на социални мрежи често избират предварително настройки на базата на откази, като по този начин улесняват разкриването на лична информация. Някои дават достъп до профилите от общи браузъри по подразбиране. Това поставя въпроси дали лицата действително са дали съгласие за разкриване, както и дали социалните мрежи са изпълнили изискванията на член 17 от Директивата (описани по-горе) да използват подходящи технически и организационни мерки за предотвратяване на неразрешената обработка.

VI.2. **Рискове, породени от социалните мрежи, и предложение на мерки за справяне с тях**

78. Горното води до увеличен риск за неприкосновеността на личния живот и защитата на данните на лица. То излага потребителите на интернет и тези, чиито данни са били въведени, на флагрантни нарушения на неприкосновеността на личния им живот и защитата на данните им.

79. При тези обстоятелства въпросът, с който Комисията следва да се занимае, е какво трябва и може да бъде направено за справяне с това положение. Настоящото становище не дава изчерпателен отговор на въпроса, а излага редица предложения за по-нататъшно обсъждане.

Инвестиране в обучението на потребителите на интернет

80. Първото предложение е да се инвестира в обучението на потребителя. Според него институциите на ЕС и националните органи трябва да инвестират в обучението и повишаването на осведомеността относно заплахите, поставени от уебсайтовете на социалните мрежи. Така например ГД „Информационно общество и медии“ работи по Програмата за по-безопасен интернет, която има за цел да даде възможност и да защити децата например чрез дейности за повишаване на осведомеността ([1]). Напоследък институциите на ЕС стартираха кампанията „Помисли, преди да пратиш“, насочена към повишаване на осведомеността за рисковете от обмен на лична информация с непознати лица.

81. ЕНОЗД насърчава Комисията да продължи да подпомага този вид дейности. Но и самите доставчици на социални мрежи трябва да играят активна роля, тъй като те имат правно и социално задължение да обучават потребителите как да използват техните услуги по начин, който да е безопасен и благоприятен за неприкосновеността на личния живот.

82. Както е описано по-горе, при изпращане на информация по социалните мрежи до нея може да бъде предоставен достъп по подразбиране по различни начини. Информацията може например да се направи достъпна за всички, в това число чрез браузъри, които могат да я индексират и така да предоставят преки препратки към нея. От друга страна, информацията може да бъде ограничена до „избрани приятели“ или да остане напълно недостъпна за външни лица. Очевидно разрешителните опции в профила и използваната терминология са различни при отделните уебсайтове.

83. Както е изтъкнато обаче по-горе, много малко потребители на услугите за социални мрежи знаят как да контролират достъпа до въведената от тях информация, да не говорим за промяна на настройките по подразбиране за неприкосновеността на личния живот. Настройките за неприкосновеността на личния живот остават непроменени, тъй като потребителите не съзнават последиците от запазването им или не знаят как да ги променят. Ето защо непроменянето на настройките за неприкосновеност на личния живот не означава в повечето случаи, че лицата са взели информирано решение да приемат обмена на информация. В този контекст е особено важно трети страни, като браузъри, да не получават препратки към отделните профили, като се изхожда от хипотезата, че потребителите са се съгласили по подразбиране (като не са променили настройките за неприкосновеност на личния живот) да дадат неограничен достъп до информацията.

84. Докато обучението на потребителите може да помогне за справяне с тези проблеми, то няма да работи самò по себе си. Както се препоръчва от работната група по член 29 в нейното становище относно социалните мрежи, доставчиците на социални мрежи трябва да предлагат благоприятни за неприкосновеността на личния живот, безплатни настройки по подразбиране. Така потребителите ще осъзнаят по-добре своите действия и ще получат възможност да направят по-добър избор относно това дали и с кого искат да обменят информация.

Роля на саморегулирането

85. Комисията е сключила споразумение с двадесет доставчици на социални мрежи, известно като „Принципи на ЕС за по-безопасна работа в социални мрежи“ ([2]). Целта на споразумението е да бъде повишена безопасността на непълнолетните лица, когато използват уебсайтове за социални мрежи в Европа. Тези принципи включват много от изискванията, следващи от прилагането на правната рамка за защита на данните, описана по-горе. Те включват например изискването да се даде на потребителите чрез инструменти и технология възможността да бъдат сигурни, че контролират използването и разпространението на своята лична информация. Тук е включена и необходимостта да се предоставят настройки по подразбиране за неприкосновеност на личния живот.

86. В началото на януари 2010 г. Комисията публикува констатациите на доклад, оценяващ прилагането на тези принципи ([3]). ЕНОЗД изразява загриженост от изводите на този доклад, че макар да са били предприети някои

([1]) Информация за тази програма може да бъде намерена на адрес: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Принципите могат да бъдат намерени на адрес: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Доклад относно оценката на прилагането на принципите на ЕС за по-безопасна работа в социални мрежи, който може да бъде намерен на адрес: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

стъпки, много други не са. Така например докладът е открил проблеми относно разгласяването на мерките и инструментите, с които разполагат уебсайтовете. Той е установил също така, че по-малко от половината от страните, подписали споразумението, ограничават достъпа на непълнолетни само до техните приятели.

Необходимост от задължителни настройки за неприкосновеност на личния живот по подразбиране

87. При това положение основният въпрос е дали са необходими допълнителни политически мерки, за да се гарантира, че социалните мрежи настройват услугите си за неприкосновеност на личния живот по подразбиране. Този проблем беше поставен от предишния комисар по въпросите на информационното общество Viviane Reding, която изтъкна, че може да се наложат законодателни мерки ([1]). В същия дух Европейският икономически и социален комитет заяви, че паралелни саморегулационни стандарти за минимална защита трябва да бъдат наложени със закон ([2]).

88. Както е посочено по-горе, задължението на доставчиците на социални мрежи да прилагат по подразбиране настройки за неприкосновеност на личния живот следва непосредствено от член 17 от Директивата за защита на данните ([3]), който задължава администраторите на данни да вземат подходящи технически и организационни мерки („както при разработването на системата за обработка, така и по време на самата обработка“) с цел да се поддържа сигурността и да се предотврати неразрешената обработка, като вземат предвид рисковете, свързани с обработката, и естеството на данните.

89. Този член обаче е прекалено общ и му липсва конкретност, също и в настоящия контекст. Той не определя ясно какво значи подходящи технически и организационни мерки в контекста на социалните мрежи. По този начин настоящото положение се характеризира с правна несигурност, която създава проблеми както за регулаторните органи, така и за лицата, чиито лични данни и неприкосновеност на личния живот не са напълно защитени.

90. В светлината на гореизложеното ЕНОЗД настоява Комисията да подготви законодателни актове, които да включват като минимум общо изискване за задължителни настройки за неприкосновеност на личния живот, допълнено с по-точни изисквания:

а) предоставяне на настройки, ограничаващи достъпа до потребителските профили до собствените контакти на потребителя, избрани от самия него. Настройките трябва освен това да изискват изричното съгласие на потребителя, преди някой от профилите да стане достъпен за трети страни;

б) да се осигури, че профилите с ограничен достъп няма да могат да се откриват от вътрешни/външни браузъри.

91. Освен предоставянето на задължителни настройки по подразбиране за неприкосновеност на личния живот, остава въпросът дали допълнителни, специфични мерки за защита на данните и някои други мерки (например във връзка със защитата на непълнолетни лица) може също да се окажат подходящи. Това поставя по-широкия въпрос дали е уместно да се създава специална рамка за този тип услуги, която, освен че ще предоставя задължителни настройки за неприкосновеност на личния живот, ще регулира и други аспекти. ЕНОЗД желае Комисията да разгледа този въпрос.

VII. НАСТРОЙКИ НА БРАУЗЪРИТЕ ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ ПО ПОДРАЗБИРАНЕ, ГАРАНТИРАЩИ ИНФОРМИРАНОТО СЪГЛАСИЕ ДА СЕ ПОЛУЧАВАТ РЕКЛАМИ

92. Доставчиците на рекламна мрежа използват „бисквитки“ (cookies) за проследяване на поведението на отделните потребители, когато те сърфират в интернет, за да проучват техните интереси и да изграждат профили. Тази информация се използва след това, за да им бъдат изпращани целеви реклами ([4]).

VII.1. Оставащи предизвикателства и рискове при настоящата правна рамка за защита на данните/неприкосновеност на личния живот

93. Тази обработка попада в обхвата на Директивата за защита на данните (когато става въпрос за лични данни), както и на член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Този член изисква изрично потребителят да бъде информиран и да му бъде дадена възможност да реагира, като приеме или отхвърли поставянето на приспособления като „бисквитки“ и др. п. на неговия компютър или на друго устройство ([5]).

94. Досега доставчиците на рекламни мрежи разчитаха на настройките на браузъра и политиките за неприкосновеност на личния живот, за да бъдат информирани

([1]) Viviane Reding, член на Европейската комисия, отговарящ за информационно общество и медии, „Помисли, преди да пратиш! Как да направим уебсайтовете на социалните мрежи по-безопасни за децата и подрастващите?“ Ден на безопасния интернет, Страсбург, 9 февруари 2010 г.

([2]) Становище на Европейския икономически и социален комитет относно въздействието на уебсайтовете на социалните мрежи върху гражданите/потребителите, 4 ноември 2009 г.

([3]) Разяснен също в съображение 33 от настоящия документ.

([4]) Проследяващите „бисквитки“ представляват малки текстови файлове, съдържащи единен идентификатор. Обикновено доставчиците на мрежи (както и операторите на уебсайтове и издателите) поставят „бисквитки“ на твърдия диск на посетителите, и по-специално в браузъра на потребителите на интернет, когато потребителите посещават за първи път уебсайтове, обслужващи реклами, които част от тяхната мрежа. „Бисквитката“ ще даде на доставчика на рекламна мрежа възможност да разпознае предишен посетител, завръщащ се в този уебсайт или посещаващ кой да е друг уебсайт, който е партньор на рекламната мрежа. Такива неколкократни посещения ще дадат на доставчика на рекламна мрежа възможност да изградят профил на госта.

([5]) Член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации беше неотдавна изменен, с цел да бъде засилена защитата срещу прихващане на комуникациите на потребителя чрез използване на — например — шпионски софтуер и „бисквитки“, съхранявани в компютъра или в друго устройство на потребителя. Съгласно новата директива на потребителите трябва да се предостави по-добра информация и полезни начини за определяне дали желаят да бъдат съхранявани „бисквитки“ в терминалните им устройства.

потребителите и да им се даде възможност да приемат или отхвърлят „бисквитките“. Те обясняваха в политиката на издателите за неприкосновеност на личния живот как потребителят да се откаже изобщо от получаване на „бисквитки“ или да ги приема на базата на всеки отделен случай. По този начин те считаха, че изпълняват своето задължение да предложат на потребителите правото да откажат „бисквитки“.

95. Въпреки че на теория този метод (чрез браузъра) може наистина да осигури ефективно информирано съгласие, в действителност нещата са много различни. Обикновено на потребителите им липсва основно разбиране за събирането на данни изобщо, а още по-малко от трети страни, за стойността на тези данни, за това как работи технологията и по-специално как и къде могат да се откажат. Стъпките, които потребителите трябва да предприемат, за да заявят своя отказ, изглеждат не само сложни, но и прекалени (първо трябва да настроят браузъра си да приема „бисквитки“ и после да изберат опцията „отказ“).

96. В резултат на практика много малко хора избират опцията за отказ, не защото са взели информирано решение да приемат поведенческо рекламиране, а по-скоро защото не разбират, че като не изберат тази опция, те всъщност са го приели.

97. Ето защо въпреки че от правна гледна точка член 5, параграф 3 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации осигурява ефективна правна защита, на практика за потребителите на интернет се смята, че са приели да бъдат проследявани за целите на изпращане на поведенчески реклами, докато фактически в много, ако не и в повечето случаи те са в пълно неведение, че се извършва проследяване.

98. Работната група по член 29 подготвя становище, чиято цел е бъдат изяснени правните изисквания за получаване на поведенчески реклами, което е много добре. Тълкуването може обаче да се окаже само по себе си недостатъчно за решаването на този проблем и може да се наложи Европейският съюз да предприеме допълнителни действия.

VII.2. **Необходимост от допълнителни действия, а именно въвеждане на задължителни настройки по подразбиране за неприкосновеност на личния живот**

99. Както е описано по-горе, интернет браузърите дават обикновено възможност за контрол на някои видове „бисквитки“. Към настоящия момент настройките по подразбиране на повечето интернет браузъри приемат всички „бисквитки“. С други думи, по подразбиране браузърите са настроени да приемат всички „бискивтки“, независимо от целта на „бисквитката“. Само ако потребителят промени настройките на своя браузър за отказ на „бисквитките“, което, както беше казано, много малко потребители правят, той/тя няма да получава „бисквитки“. Освен това няма софтуер за неприкосновеност на личния живот при първоначално инсталиране или актуализиране на приложенията на браузъра.

100. Един от начините за решаване на този проблем е снабдяването на браузърите с настройки по подразбиране за неприкосновеност на личния живот. С други думи, те да имат настройка „отказ на бисквитки на трети страни“. Като допълнение към това и за по-голяма ефективност браузърите трябва да изискват от потребителите да прегледат настройките на софтуера за неприкосновеност на личния живот при първото инсталиране или актуализирането на браузъра. Необходими са повече подробности и по-ясна информация относно видовете „бисквитки“ и полезността на някои от тях. Потребителите, които искат да бъдат проследявани за получаване на реклами, ще бъдат надлежно осведомявани и ще трябва да променят настройките на браузъра. Това ще им даде по-голям контрол върху техните лични данни и неприкосновеността на личния им живот. Това според ЕНОЗД ще бъде ефикасен начин да бъде зачетено и запазено съгласието на потребителите ([1]).

101. Като се вземе предвид, от една страна, широкото разпространение на проблема — с други думи, броят на потребителите на интернет, които са проследявани към настоящия момент на базата на съгласие, което е мнимо, и, от друга страна, мащабът на засегнатите интереси, необходимостта от допълнителни предпазни мерки се засилва. Използването на принципа на PbD в приложенията на интернет браузърите може да бъде много сериозна крачка напред към предоставяне на контрол на лицата върху практиките за събиране на данни, използвани за рекламни цели.

102. Поради тези причини ЕНОЗД настоява Комисията да обсъди законодателни мерки, изискващи задължителни настройки по подразбиране за неприкосновеност на личния живот в браузърите и предоставяне на адекватна информация.

VIII. **ДРУГИ ПРИНЦИПИ, НАСОЧЕНИ КЪМ ЗАЩИТА НА ЛИЧНИЯ ЖИВОТ/ЛИЧНИТЕ ДАННИ НА ФИЗИЧЕСКИТЕ ЛИЦА**

103. Въпреки че принципът на PbD има големи възможности за подобряване на защитата на личните данни и неприкосновеността на личния живот на лицата, разработването и прилагането в законодателството на допълнителни принципи са необходими, за да се осигури доверието на потребителите към ИКТ. В този контекст ЕНОЗД се спира на принципа на отчетността и на допълването на задължителна рамка за нарушения на сигурността, приложима в различните сектори.

VIII.1. **Принцип на отчетността за гарантиране на изпълнението на принципа за защита на личния живот още при разработването**

104. Докладът на работната група по член 29 под надслов „Бъдеще на неприкосновеността на личния живот“ ([2]) препоръча включването на принципа на отчетността в

([1]) Същевременно ЕНОЗД разбира, че това няма да реши изцяло проблема, докато има „бисквитки“, които не могат да бъдат контролирани чрез браузъра, какъвто е случаят с така наречените „флаш бисквитки“. За тях създателите на браузъра ще трябва да включат флаш контрол в своите опции по подразбиране за „бисквитките“ при пускане в употреба на нови браузъри.

([2]) Становище 168 на Работната група по член 29 относно бъдещето на неприкосновеността на личния живот, съвместен принос към консултациите на Европейската комисия по правната рамка за основното право на защита на личните данни, прието на 1 декември 2009 г.

Директивата за защита на данните. Този принцип, който е признат в някои многонационални инструменти за защита на данните ([1]), изисква от организациите да прилагат процедури за спазване на съществуващите закони и да създадат методи за оценка и доказване на съответствието със законодателството и с други задължителни инструменти.

105. ЕНОЗД подкрепя изцяло препоръката на работната група по член 29. Той счита, че този принцип ще бъде много важен за насърчаване на ефективното прилагане на принципите и задълженията за защита на данните. Отчетността ще изисква от администраторите на данни да докажат, че са въвели механизма, необходим за привеждане в съответствие с действащото законодателство за защита на данните. Това вероятно ще допринесе за ефективното прилагане на принципа за защита на личния живот още при разработването в ИКТ технологиите като особено подходящ елемент за доказване на отчетността.

106. За измерване и доказване на отчетността администраторите на данни може да използват вътрешни процедури и трети страни, които да извършват одити или друг вид контроли и проверки, като в резултат може да се присъждат печати или награди. В този контекст ЕНОЗД настоява Комисията да обсъди дали освен общия принцип на отчетност няма да е добре да се наложат по законодателен път специфични мерки за отчетност, като необходимост от представяне на оценки за въздействието върху неприкосновеността на личния живот и защитата на данните, и при какви обстоятелства.

VIII.2. **Нарушение на сигурността: допълване на правната рамка**

107. Измененията от миналата година на Директивата за правото на неприкосновеност на личния живот и електронни комуникации въведоха изискване да бъдат уведомявани за нарушения на сигурността на данни засегнатите физически лица, както и съответните органи. Нарушението на сигурността на данни се определя в общия случай като нарушение, което води до унищожаване, загуба, разкриване и т.н. на лични данни, предавани, съхранявани или по друг начин обработвани във връзка с услугата. Отделните лица се изисква да бъдат уведомявани, ако нарушението на сигурността на личните данни има вероятност да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот. Такъв може да бъде случаят, когато нарушението може да доведе до кражба на самоличност или съществено унижение и накърняване на репутацията. Уведомяването на съответните власти се изисква при всяко нарушение на сигурността на данни, независимо от това дали има риск за лицата.

Прилагане на задълженията при нарушение на сигурността във всички сектори

108. За съжаление това задължение се отнася само до доставчиците на обществено достъпни електронни съобщителни услуги, като телефонни компании, доставчици на достъп до интернет, доставчици на уебпоща и т.н. ЕНОЗД настоява Комисията да представи предложения относно нарушенията на сигурността, приложими към всички сектори. Що се отнася до съдържанието на такава рамка, ЕНОЗД счита, че правната рамка за нарушенията на сигурността, възприета в Директивата за правото на неприкосновеност на личния живот и електронни комуникации, постига подходящ баланс между защитата на правата на лицата, включително правото им на лични данни и неприкосновеност на личния живот, и задълженията, наложени на обхванатите субекти. Същевременно това е рамка с истински „зъби“, тъй като е подкрепена със съдържателни разпоредби за прилагането ѝ, което дава на органите достатъчно правомощия за разследване и санкции в случай на нарушения.

109. Ето защо ЕНОЗД настоява Комисията да приеме законодателно предложение за прилагане на тази рамка във всички сектори, ако е необходимо със съответните изменения. Освен това по този начин ще се гарантира прилагането на едни и същи норми и процедури във всички сектори.

Допълване на правната рамка, залегнала в Директивата за правото на неприкосновеност на личния живот и електронни комуникации, чрез комитология

110. Преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации дава право на Комисията да приеме технически мерки за прилагане, т.е. подробни мерки за уведомяване при нарушения на сигурността чрез процедура по комитология ([2]). Това оправомощаване се обосновава от необходимостта да се гарантира последователно изпълнение и прилагане на правната рамка за нарушенията на сигурността. Последователното изпълнение допринася за това гражданите в цялата Общност да се радват на еднакво висока степен на защита и обхванатите субекти да не бъдат товарени с различни изисквания за уведомяване.

111. Директивата за правото на неприкосновеност на личния живот и електронни комуникации беше приета през ноември 2009 г. Не се очертава никаква причина, която да оправдае отлагането на старта на работата, насочена към приемане на техническите мерки за прилагане. ЕНОЗД организира два семинара, които имаха за цел обмен и събиране на опит относно уведомяването за нарушенията на сигурността. Той е готов да сподели резултатите от тази проява и очаква да работи съвместно с Комисията и другите заинтересовани страни по прецизирането на общата правна рамка за нарушенията на сигурността на данни.

112. ЕНОЗД настоява Комисията да предприеме в близко бъдеще необходимите стъпки. Преди приемането на техническите мерки за прилагане Комисията трябва да проведе широки консултации с ENISA, ЕНОЗД и работната група по член 29. Освен това консултациите трябва да включват и други „съответни заинтересовани страни“, по-специално за информация относно най-добрите разполагаеми технически и икономически начини на прилагане.

([1]) Основни насоки на ОИСР от 1980 г. за защитата на личния живот и трансграничните потоци лични данни ; Мадридска декларация за защитата на личния живот относно глобални стандарти за неприкосновеност на личния живот в един глобален свят, 3 ноември 2009 г.

([2]) Комитологията включва приемането на технически мерки за прилагане чрез комитет от представители на държавите-членки, председателстван от Комисията. За Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилага така наречената процедура по регулиране с контрол, което значи, че Европейският парламент, както и Съветът, може да се противопоставят на мерки, предложени от Комисията. За допълнителна информация вж.: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **ЗАКЛЮЧЕНИЯ**

113. Доверието, или по-скоро липсата на такова, е посочено като основен проблем при появата и успешното внедряване на информационни и комуникационни технологии. Ако хората нямат доверие на ИКТ, тези технологии вероятно ще претърпят провал. Доверието в ИКТ зависи от различни фактори, като ключово значение сред тях има гаранцията, че тези технологии няма да подкопаят основните права на физическите лица на неприкосновеност на личния живот и защита на личните данни.

114. С цел да бъде допълнително укрепена правната рамка за защита на данните/неприкосновеност на личния живот, чиито принципи остават изцяло в сила в информационното общество, ЕНОЗД предлага Комисията да заложи принципа за защита на личния живот още при разработването на различни равнища на законодателството и изготвянето на политиките.

115. Той препоръчва на Комисията да се придържа към следните четири насоки на действие:

а) да предложи включване на обща разпоредба относно защитата на личния живот още при разработването в правната рамка за защита на данните. Тази разпоредба трябва да бъде технологично неутрална и нейното изпълнение трябва да е задължително на различните етапи;

б) да прецизира тази обща разпоредба чрез специфични разпоредби, когато в различните сектори се предлагат специфични правни инструменти. Тези специфични разпоредби може да бъдат включени още сега в правните инструменти въз основа на член 17 от Директивата за защита на данните (и друго съществуващо законодателство);

в) да включи PbD като ръководен принцип в Европейската програма за цифрово развитие;

г) да въведе PbD като принцип в други инициативи на ЕС (главно незаконодателни).

116. В три посочени области на ИКТ, ЕНОЗД препоръчва на Комисията да прецени необходимостта от внасяне на предложения за прилагане на принципа за защита на личния живот още при разработването по специфични начини:

а) по отношение на RFID да бъдат предложени законодателни мерки, регулиращи основните въпроси на използването на RFID, при неуспех на ефективното прилагане на съществуващата правна рамка чрез саморегулиране. По-специално, да се приложи принципът на предварителното съгласие в точката на продажба, според който всички приемо-предаватели за RFID, прикрепени към потребителските продукти, да бъдат дезактивирани по подразбиране в точката на продажба;

б) по отношение на социалните мрежи да бъдат подготвени законодателни актове, които да включват като минимум общо изискване за задължителни настройки за неприкосновеност на личния живот, допълнено с по-точни изисквания относно ограничаване на достъпа до потребителските профили до собствените контакти на потребителя, избрани от самия него, и да се осигури, че профилите с ограничен достъп няма да могат да се откриват от вътрешни/външни браузъри;

в) по отношение на насочените реклами да бъдат обсъдени законодателни мерки за задължителни настройки на браузъра за отказ по подразбиране от „бисквитки“ на трети страни и за изискване към потребителите да прегледат настройките на софтуера за неприкосновеност на личния живот при първото инсталиране или актуализирането на браузъра.

117. Накрая, ЕНОЗД предлага на Комисията:

а) да обсъди прилагането на принципа на отчетност в съществуващата Директива за защита на данните; и

б) да разработи рамка от правила и процедури за прилагане на разпоредбите в Директивата за неприкосновеност на личния живот и електронните комуникации за уведомяване при нарушение на сигурността и да разшири обхвата им така, че да се отнасят общо до всички администратори на данни.

Съставено в Брюксел на 18 март 2010 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните