Становище на Европейския надзорен орган по защита на данните относно съобщението на Комисията до Европейския парламент и Съвета „Пространство на свобода, сигурност и правосъдие за гражданите“

(2009/C 276/02)

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

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

1. На 10 юни 2009 г. Комисията прие съобщение до Европейския парламент и Съвета „Пространство на свобода, сигурност и правосъдие за гражданите“ ([1]). В съответствие с член 41 от Регламент (ЕО) № 45/2001 ЕНОЗД представя настоящото становище.

2. Преди да одобри съобщението, Комисията се консултира неофициално с ЕНОЗД чрез писмо от 19 май 2009 г. ЕНОЗД даде отговор на 20 май 2009 г., като изпрати неофициални забележки, които целяха да подобрят още повече текста на съобщението. Освен това ЕНОЗД допринесе активно към писмото от 14 януари 2009 г. на работната група по полицейско и съдебно сътрудничество относно многогодишната програма в областта на свободата, сигурността и правосъдието ([2]).

3. В съобщението (параграф 1) се подчертава, че Съюзът „трябва да приеме нова многогодишна програма, която е насочена към бъдещето с амбиция, като се основава на постигнатия напредък и отчита сегашните слабости. В тази нова програма трябва да се дефинират приоритетите за следващите пет години“. Тази многогодишна програма (известна вече като „Програма от Стокхолм“) ще бъде продължение на програмите от Тампере и Хага, които дадоха силен политически тласък на пространството на свобода, сигурност и правосъдие.

4. Целта на съобщението е да се превърне в основата за тази нова многогодишна програма. Във връзка с това ЕНОЗД отбелязва, че макар и многогодишните програми като такива да не са обвързващи правни инструменти, те оказват значително въздействие върху политиката, която ще разработват институциите в съответната област, тъй като много от конкретните правни и неправни действия ще произлизат от тази програма.

5. Самото съобщение трябва да бъде разглеждано в тази светлина. То се явява следващата стъпка в разискване, което започна в една или друга степен с два, представени през юни 2008 г. доклада на т.нар. групи „Бъдеще“, сформирани от председателството на Съвета за генериране на идеи: „Свобода, сигурност и неприкосновеност на личния живот — европейските вътрешни работи в отворен свят“ ([3]) и „Предложения за бъдещата програма на ЕС в областта на правосъдието“ ([4]).

II. СЪДЪРЖАНИЕ НА СТАНОВИЩЕТО

6. Настоящото съобщение се явява не само отговор на съобщението, но е и принос на ЕНОЗД към по-общия дебат относно бъдещето на пространството на свобода, сигурност и правосъдие, който трябва да доведе до нова стратегическа работна програма (Програмата от Стокхолм), както беше обявено от шведското председателство на ЕС ([5]). В настоящото становище са разгледани и някои последици от евентуалното влизане в сила на Договора от Лисабон.

7. След уточняване на основните аспекти на становището в част III, в част IV се прави цялостна оценка на съобщението.

8. В част V е разгледан въпросът как да се отговори на необходимостта от трайно зачитане на защитата на неприкосновеността на личния живот и личните данни в контекста на нарастващ обмен на лични данни. Предмет на внимание ще бъде параграф 2.3 от Съобщението относно защитата на лични данни и неприкосновеността на личния живот и в по-общ план необходимостта от по-нататъшни правни и неправни действия за подобряване на рамката за защита на данните.

([1]) COM(2009) 262 окончателен („съобщението“).

([2]) Непубликувано. Работната група по полицейско и съдебно сътрудничество беше създадена от Европейската конференция на комисарите по защита на данните, за да изготвя позициите ѝ в областта на правоприлагането и да действа от нейно име при неотложни въпроси.

([3]) Документ на Съвета № 11657/08. По-нататък „Доклад за вътрешните работи“.

([4]) Документ на Съвета № 11549/08 („Доклад относно правосъдието“).

([5]) Работна програма на председателството на ЕС, http://www.regeringen.se.

9. В част VI се разглеждат потребностите и възможностите за съхраняването, достъпа и обмена на информация като инструменти за правоприлагане, или според формулировката в съобщението за „Европа, която закриля“. В параграф 4 от съобщението се посочват няколко цели по отношение на потока на информация и технологичните средства, по-конкретно в параграфи 4.1.2 („Овладяване на информацията“), 4.1.3 („Мобилизиране на необходимите технологични средства“) и 4.2.3.2 („Информационни системи“). В това отношение разработването на европейски модел за информация (в параграф 4.1.2) може да се разглежда като най-предизвикателното предложение. Становището на ЕНОЗД съдържа задълбочен анализ на това предложение.

10. Част VII засяга накратко специфичен въпрос в областта на свободата, сигурността и правосъдието, който има отношение към защитата на данните, а именно достъпът до правосъдие и електронно правосъдие.

III. **АСПЕКТИ НА СТАНОВИЩЕТО**

11. Като отправна точка за анализ на съобщението настоящото становище взема необходимостта от защита на основните права и в по-общ план бъдещето на пространството на свобода, сигурност и правосъдие, оформено от нова многогодишна програма. В становището си ЕНОЗД, основно в консултативното си качество, доразвива приноса си към разработването на политиката на ЕС в тази област. До момента ЕНОЗД е приел повече от трийсет становища и бележки по отношение на инициативи, произтичащи от Програмата от Хага, които могат да се намерят на уебсайта на ЕНОЗД.

12. В оценката на съобщението ЕНОЗД ще вземе под внимание по-специално следните четири аспекта, които имат отношение към бъдещето на пространството на свобода, сигурност и правосъдие. Тези аспекти заемат централно място и в съобщението.

13. Първият аспект е стремглавото нарастване на цифрова информация относно гражданите в резултат на развиващите се информационни и комуникационни технологии ([6]). Обществото се развива към т.нар. „наблюдавано общество“, в което е вероятно всяка операция и почти всеки ход на гражданите да оставя цифрова следа. Т.нар. „интернет на нещата“ и „интелигентна среда“ вече се развиват бързо посредством използването на етикети за радиочестотна идентификация. Все по-широко се използват цифровизирани характеристики на човешкото тяло (биометрика). Това води до един все по-взаимосвързан свят, където организациите в областта на обществената сигурност могат да имат достъп до огромен обем потенциално полезна информация, която да повлияе пряко върху живота на засегнатите лица.

14. Вторият аспект е интернационализацията. От една страна, обменът на данни в дигиталната ера не е ограничен от външните граници на Европейския съюз, докато от друга страна нараства необходимостта от международно сътрудничество във всички дейности на ЕС в рамките на пространството на свобода, сигурност и правосъдие: борбата с тероризма, полицейското и съдебното сътрудничество, гражданското правосъдие и граничният контрол са само някои примери.

15. Третият аспект е използването на данни за целите на правоприлагането: неотдавнашните заплахи за обществото, независимо дали са свързани с тероризма, доведоха до (искания за) повече възможности за правоприлагащите органи да събират, съхраняват и обменят лични данни. В много случаи активно участие вземат частни страни, както се вижда, *inter alia*, от директивата за запазване на данни ([7]) и от различните правни инструменти, свързани с резервационните данни на пътниците (PNR) ([8]).

16. Четвъртият аспект е свободното движение. Постепенното развитие на пространство на свобода, сигурност и правосъдие налага по-нататъшно премахване на вътрешните граници и евентуални пречки пред свободното движение в това пространство. Новите правни инструменти в тази област не бива в никакъв случай да създават повторно препятствия. В сегашния контекст свободното движение включва, от една страна, свободното движение на лица и, от друга страна, свободното движение на (лични) данни.

17. Тези четири аспекта показват, че контекстът, в който се използва информацията, се променя бързо. В този смисъл не може да има съмнение относно значимостта на един стабилен механизъм за защита на основните права на гражданите, и по-конкретно защитата на неприкосновеността на личния живот и данни. Поради тези причини ЕНОЗД се спира на необходимостта от защита като основна отправна точка за настоящия анализ, както беше посочено в точка 11.

([6]) В този смисъл в доклада за вътрешните работи се говори дори за „цифрово цунами“.

([7]) Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г., стр. 54.

([8]) Вж. напр. Споразумение между Европейския съюз и Съединените американски щати относно обработка и предаване на данни от досиетата на пътниците (PNR) от въздушни превозвачи на Министерството на вътрешната сигурност (DHS) на Съединените щати (Споразумение PNR от 2007 г.), ОВ L 204, 4.8.2007 г., стр. 18. и предложение за рамково решение на Съвета относно използване на досиетата на пътниците (PNR — Passenger Name Record) за целите на правоприлагането, COM(2007) 654 окончателен.

IV. **ОБЩА ОЦЕНКА**

18. Съобщението и Програмата от Стокхолм целят да установяват намеренията на ЕС за следващите пет години, като е възможно последиците да са дори по-дългосрочни. ЕНОЗД отбелязва, че съобщението е написано в „неутрален по отношение на Договора от Лисабон“ дух. ЕНОЗД напълно разбира защо Комисията е възприела този подход, но същевременно изразява съжаление, че не са били използвани пълноценно допълнителните възможности, предлагани от Договора от Лисабон. В настоящото становище ще се наблегне в по-голяма степен на Договора от Лисабон.

19. Съобщението стъпва на резултатите от действията на ЕС в пространството на свобода, сигурност и правосъдие през последните години. Тези резултати могат да се определят като продиктувани от събитията, с акцент върху мерки, които разширяват правомощията на правоприлагащите органи и нарушават неприкосновеността на личния живот на гражданите. Такъв определено е случаят в областите с интензивно използване и обмен на лични данни, които следователно са решаващи за защитата на данните. Резултатите са продиктувани от събитията, защото външни събития като 11 септември и бомбените атентати в Мадрид и Лондон дадоха силен импулс за законодателни действия. Така например предаването на данни за пътниците на Съединените щати може да се разглежда като последица от 11 септември ([9]), а бомбените атентати в Лондон породиха Директива 2006/24/ЕО за запазване на данни ([10]). Акцентът беше поставен върху мерки, нарушаващи в по-голяма степен неприкосновеността на личния живот, тъй като законодателят на ЕС насочи вниманието си към мерки, които улесняват използването и обмена на данни, докато обсъждането на мерки, целящи да гарантират защитата на личните данни, не беше толкова спешно. Основната мярка за защита, която беше приета след тригодишни обсъждания в рамките на Съвета, е Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси ([11]). Резултатът беше рамково решение на Съвета, което не е съвсем удовлетворително (вж. точки 29—30).

20. Опитът от последните години показва, че преди да се приемат нови правни инструменти, е необходимо да се разгледат последиците за правоприлагащите органи и за европейските граждани. При това разглеждане следва надлежно да се вземат предвид последиците за неприкосновеността на личния живот и ефективността от гледна точка на правоприлагането, на първо място при предлагането и обсъждането на нови инструменти, но и след прилагането на тези инструменти чрез периодични прегледи. Подобно разглеждане е важно и преди нова многогодишна програма да установи основни инициативи за близкото бъдеще.

21. ЕНОЗД изразява задоволство, че в съобщението защитата на основните права, и по-конкретно защитата на личните данни, се признава като един от ключовите въпроси, които имат отношение към бъдещето на пространството на свобода, сигурност и правосъдие. В параграф 2 от съобщението ЕС се определя като единствено по рода си пространство за защита на основните права въз основа на общи ценности. Освен това е добре, че присъединяването към Европейската конвенция за правата на човека се посочва като особено важен въпрос — дори най-важният въпрос в съобщението. Присъединяването е важна стъпка към осигуряването на хармонична и съгласувана система за защитата на основните права. И не на последно място, в съобщението е обърнато специално внимание на защитата на данните.

22. Този акцент в съобщението показва твърдо намерение да се гарантира защитата на правата на гражданите и по този начин да се възприеме по-балансиран подход. Правителствата се нуждаят от подходящи инструменти, за да се гарантира сигурността на гражданите, но в нашето европейско общество те трябва да зачитат в пълна степен основните права на гражданите. Службата в полза на гражданите ([12]) изисква Европейски съюз, който защитава този баланс.

23. ЕНОЗД е на мнение, че необходимостта от такъв баланс е отчетена много добре в съобщението, включително необходимостта от защита на личните данни. Признава се необходимостта от промяна в акцента. Това е важно, тъй като политиките в пространството на свобода, сигурност и правосъдие не следва да благоприятстват постепенното преминаване към наблюдавано общество. ЕНОЗД очаква Съветът да възприеме същия подход в Програмата от Стокхолм, както и да отчете насоките в точка 25 по-долу.

24. Това е още по-важно, тъй като пространството на свобода, сигурност и правосъдие е област, която „оформя житейските обстоятелства на гражданите, и в частност личното пространство на собствената им отговорност и това на личната и социална отговорност, защитено от основните права“, като беше подчертано съвсем наскоро от Конституционния съд на Германия в съдебното му решение от 30 юни 2009 г., свързано с Договора от Лисабон ([13]).

([9]) Споразумението относно PNR от 2007 г., спомената в предходната бележка под линия и преди това.

([10]) Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г., стр. 54. Макар правното основание да е член 95 от Договора за ЕО, тя беше непосредствен отговор на бомбените атентати в Лондон.

([11]) Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 година относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, ОВ L 350, 30.12.2008 г., стр. 60.

([12]) Вж. заглавието на съобщението.

([13]) Съобщение за печата № 72/2009 от 30 юни 2009 г. на Федералния конституционен съд на Германия, параграф 2, буква в).

25. ЕНОЗД подчертава, че в това пространство:

— информацията следва да се обменя между органите на държавите-членки, включително, когато е уместно, между европейски образувания или бази данни, въз основа на подходящи и ефективни механизми, които зачитат напълно основните права на гражданите и гарантират взаимно доверие,

— това налага не само наличност на информацията, съчетана с взаимно признаване на правните системи на държавите-членки (и ЕС), но и хармонизиране на стандартите за защита на информацията, например, но не само чрез обща рамка за защита на данните,

— тези общи стандарти не следва да се прилагат единствено в случаи с трансгранични измерения. Взаимно доверие може да съществува единствено когато стандартите са стабилни и винаги се спазват, без риск да престанат да се прилагат, след като вече няма трансгранично измерение или то не е очевидно. Като се изключи това, особено когато става въпрос за използването на информация, разликите между „вътрешни“ и „трансгранични“ данни не са приложими на практика ([14]).

V. ПРАВНИ ИНСТРУМЕНТИ ЗА ЗАЩИТА НА ДАННИТЕ

V.1. Към цялостен режим на защита на данните

26. ЕНОЗД одобрява стратегическия подход за отделяне на видно място в съобщението на защитата на данните. Наистина, много инициативи по отношение на пространството на свобода, сигурност и правосъдие почиват на използването на личните данни и добрата защита на данните е решаваща за успеха им. Зачитането на неприкосновеността на личния живот и защитата на данните е не само правно задължение, което все повече се признава на равнище ЕС, но и решаващ за европейските граждани въпрос, както показват резултатите от Евробарометър ([15]). Освен това ограничаването на достъпа до лични данни също е решаващо за гарантирането на доверие от правоприлагащите органи.

27. В параграф 2.3 от съобщението се посочва, че е необходим цялостен режим на защита на личните данни, който обхваща всички области на компетентност на Съюза ([16]). ЕНОЗД подкрепя изцяло тази цел, независимо от влизането в сила на Договора от Лисабон. ЕНОЗД отбелязва също, че такъв режим не означава непременно правна рамка, приложима към всяка обработка. Според сега действащите Договори възможностите за приемане на цялостна, приложима към всяка обработка правна рамка са ограничени поради стълбовата структура и поради факта, че, най-малко по първия стълб, защитата на обработваните от европейските институции данни се извършва въз основа на отделно правно основание (член 286 от ЕО). Същевременно ЕНОЗД посочва, че чрез пълноценното използване на възможностите, предоставени от сега действащите договори, могат да се внесат някои подобрения, като беше вече изтъкнато в съобщението на Комисията „Прилагане на Програмата от Хага — пътят напред“ ([17]). След влизането в сила на Договора от Лисабон, член 16 от Договора за функционирането на ЕС ще предостави необходимото правно основание за една цялостна правна рамка, приложима към всяка обработка.

28. ЕНОЗД отбелязва, че във всеки случай е изключително важно да се гарантира, където е необходимо, последователност в правната рамка за защита на данните чрез хармонизиране и укрепване на различните правни инструменти, приложими в пространството на свобода, сигурност и правосъдие.

Според сега действащите договори

29. Наскоро беше направена първа стъпка чрез приемането на Рамково решение 2008/977/ПВР на Съвета ([18]). Този правен инструмент обаче не може да бъде окачествен като цялостна рамка, най-вече защото разпоредбите му нямат общо приложение. Те не се прилагат при вътрешни ситуации, когато личните данни идват от държавата-членка, която ги използва. Подобно ограничение несъмнено намалява добавената стойност на рамковото решение на Съвета, освен ако всички държави-членки не решат да включат вътрешните ситуации в националното законодателство по прилагането, което е малко вероятно.

30. Друга причина, поради която ЕНОЗД смята, че в дългосрочен план Рамково решение 2008/977/ПВР на Съвета не съдържа задоволителна рамка за защита на данните в пространство на свобода, сигурност и правосъдие, е липсата на съответствие между няколко основни разпоредби и Директива 95/46/ЕО. Според сега действащите договори може да се предприеме втора стъпка чрез разширяване на обхвата и привеждане на рамковото решение на Съвета в съответствие с Директива 95/46/ЕО.

31. Друг подтик за изграждането на цялостен режим за защита на данните би могло да е установяването на ясна, дългосрочна визия. Тази визия би могла да включва

([14]) ЕНОЗД разглежда задълбочено тази последна точка в становището си от 19 декември 2005 г. по предложението за рамково решение на Съвета относно защитата на лични данни, обработвани в рамките на полицейското и съдебно сътрудничество по наказателноправни въпроси (COM(2005) 475 окончателен), ОВ C 47, 25.2.2006 г., стр. 27, параграфи 30—32.

([15]) Защита на данните в Европейския съюз — възприятия на гражданите — аналитичен доклад, Флаш Евробарометър поредица 225, януари 2008 г., http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Вж. също приоритетните въпроси в съобщението.

([17]) COM(2006) 331 окончателен, 28.6.2006 г.

([18]) Вж. бележка под линия 11.

цялостен и съгласуван подход, който определя събирането и обмена на данни — както и използването на съществуващи бази данни, и същевременно гаранциите за защита на данните. Тази визия следва да предотврати ненужното застъпване и дублиране на инструменти (и оттук обработката на лични данни). Тя следва също да укрепи последователността на политиките на ЕС в тази област и доверието в начина, по който публичните органи боравят с данните на гражданите. ЕНОЗД препоръчва Съветът да заяви необходимостта от ясна дългосрочна визия в Програмата от Стокхолм.

32. Освен това ЕНОЗД препоръчва да се оценят и разгледат в по-широк контекст вече приетите в тази област мерки, конкретното им прилагане и ефективност. Тази оценка следва надлежно да взема предвид последиците за неприкосновеността на личния живот и ефективността от гледна точка на правоприлагането. Ако тези оценки покажат, че определени мерки не дават очакваните резултати или не са съразмерни с определените цели, следва да се обмислят следните стъпки:

— като начало, изменяне или отмяна на мерките, доколкото те очевидно не са достатъчно оправдани да носят конкретна добавена стойност на правоприлагащите органи и европейските граждани,

— на второ място, оценяване на възможностите за по-добро прилагане на съществуващите мерки,

— едва на трето място, предлагане на нови законодателни мерки, ако е вероятно тези нови мерки да са необходими с оглед на набелязаните цели. Нови правни инструменти следва да се приемат само ако те носят ясна и конкретна добавена стойност на правоприлагащите органи и на европейските граждани.

ЕНОЗД препоръчва в Програмата от Стокхолм да се посочи система за оценка на съществуващите мерки.

33. Не на последно място, следва да се постави специален акцент върху по-доброто прилагане на наличните предпазни мерки, в съответствие със съобщението на Комисията относно последващите действия по отношение на работната програма за по-добро прилагане на Директивата за защита на данните ([19]) и с направените от ЕНОЗД предложения в становището му по това съобщение ([20]). За съжаление в третия стълб Комисията няма възможността да започне процедури за нарушение.

Според Договора от Лисабон

34. Договорът от Лисабон открива пътя за същинска цялостна рамка за защита на данните. Член 16.2 от Договора за функционирането на Европейския съюз изисква Съветът и Европейският парламент да установят правилата, свързани със защитата на данни от страна на институциите, органите, службите и агенциите на Съюза, от държавите-членки при осъществяването на дейности, които попадат в обхвата на правото на Съюза, и от частни страни.

35. ЕНОЗД възприема акцента в съобщението върху цялостен режим за защита на данните като амбиция от страна на Комисията да предложи правна рамка, която се прилага за всички дейности на обработка. ЕНОЗД напълно одобрява тази амбиция, която укрепва последователността на системата, гарантира правна сигурност и така подобрява защитата. По-конкретно, така в бъдеще ще се избегне трудността да се намери разделителна черта между стълбовете, когато събраните в частния сектор за търговски цели данни се използват по-късно за целите на правоприлагането. Тази разделителна черта между стълбовете не отразява напълно реалността, както се доказва от важните решения на Съда по отношение на PNR ([21]) и във връзка със запазването на данни ([22]).

36. ЕНОЗД предлага в Програмата от Стокхолм да се подчертае тази обосновка за цялостен режим за защита на данните. Тя показва, че такъв режим не е само предпочитание, а необходимост в резултат на променящите се практики в използването на данните. ЕНОЗД препоръчва в Програмата от Стокхолм да се включи като приоритетна необходимостта от нова законодателна рамка, заменяща, *inter alia*, Рамково решение 2008/977/ПВР на Съвета.

37. ЕНОЗД подчертава, че идеята за цялостен режим за защита на данните, основан на обща правна рамка, не изключва приемането на допълнителни правила за защита на данните за полицията и съдебния сектор. Тези допълнителни правила биха могли да вземат под внимание специфичните потребности от правоприлагане, както се предвижда в Декларация 21, приложена към Договора от Лисабон ([23]).

V.2. **Повторно излагане на принципите на защита на данните**

38. В съобщението се отбелязват промените в технологиите, които променят комуникацията между лицата и публичните и частните организации. Това според Комисията налага повторно излагане на няколко основни принципи на защитата на данните.

([19]) COM(2007) 87 окончателен от 7.3.2007 г.

([20]) Становище от 25 юли 2007 г., ОВ C 255, 27.10.2007 г., стр. 1, и по-конкретно точка 30.

([21]) Решение на Съда от 30 май 2006 г., Европейски парламент/Съвет на Европейския съюз (C-317/04) и Комисия на ЕО (C-318/04), обединени дела C-317/04 и C-318/04, ECR (2006), стр. I—4721.

([22]) Решение на Съда от 10 февруари 2009 г., Ирландия/Европейския парламент и Съвета на Европейския съюз, дело C-301/06, непубликувано.

([23]) Вж. Декларация 21 относно защитата на личните данни в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, приложена към заключителния акт на Междуправителствената конференция, която прие Договора от Лисабон, ОВ C 115, 9.5.2008 г., стр. 345.

39. ЕНОЗД приветства тези намерения, изложени в съобщението. Оценката на ефективността на тези принципи в контекста на промените в технологиите е изключително полезна. Като начало е важно да се отбележи, че повторното излагане и утвърждаване на принципите на защита на данните не трябва винаги да се свързва пряко с развитието на технологиите. То може да е необходимо в контекста на други възможности, посочени в част III по-горе, интернационализацията, нарастващото използване на данни за целите на правоприлагането и свободното движение.

40. Освен това ЕНОЗД е на мнение, че тази оценка може да стане част от публичната консултация, обявена от Комисията по време на проведената на 19—20 май 2009 г. конференция „Личните данни — по-голямо използване, по-голяма защита?“. Тази публична консултация би могла да внесе ценен принос ([24]). ЕНОЗД предлага да се подчертае връзката между намеренията на Комисията, заявени в параграф 2.3 от съобщението, и публичната консултация относно бъдещето на защитата на данните, на Съвета в текста на Програмата от Стокхолм и на Комисията в публичните ѝ изявления във връзка с консултацията.

41. За онагледяване на обхвата на тази оценка се посочват следните точки:

— вероятно личните данни в пространството на свобода, сигурност и правосъдие да бъдат от особено чувствително естество, като например данни, свързани с наказателни присъди, полицейски данни и биометрични данни като пръстови отпечатъци и ДНК профили,

— тяхната обработка може да има отрицателни последици за субектите на данни, особено като се имат предвид принудителните правомощия на правоприлагащите органи. Освен това наблюдението и анализът на данни стават все по-автоматизирани, доста често без човешка намеса. Технологията позволява използването на бази данни с лични данни за общо търсене (извличане на данни, профилиране, и т.н.). Правните задължения, на които се основава обработката на данни, следва да бъдат ясно установени,

— крайъгълен камък на закона за защита на данните е, че личните данни се събират за точно определени цели и не се използват по начин, несъвместим с тези цели. Използването за несъвместими цели следва да се допуска само дотолкова, доколкото е установено от закона и необходимо в името на конкретни публични интереси, като установените от член 8.2 от Европейската конвенция за правата на човека,

— необходимостта от спазване на принципа на ограничаване в рамките на целта би могла да има последици за сегашните тенденции в използването на данните. Правоприлагането използва данни, които са били събрани от частни компании за търговски цели в телекомуникационния, транспортния и финансовия сектори. Освен това се създават мащабни информационни системи, например в областта на имиграцията и граничния контрол. Също така се допускат взаимовръзки и достъп до бази данни, като по този начин се разширяват целите, за които данните са били събрани първоначално. Необходимо е тези настоящи тенденции да намерят отражение, включително при нужда да се предприемат всякакви евентуални адаптации и/или допълнителни предпазни мерки.

— освен посочените в съобщението принципи на защитата на данните в оценката следва да се обърне внимание на необходимостта от прозрачност на обработката, която позволява на субекта на данните да упражнява правата си. Прозрачността е особено труден въпрос в областта на правоприлагането, в частност защото трябва да бъде съпоставена с рисковете за разследването,

— следва да бъдат намерени решения във връзка с обмена с трети държави.

42. Освен това оценката следва да се фокусира върху възможностите за подобряване на ефективността на прилагането на принципите на защитата на данните. В този смисъл би било полезно насочването на вниманието към правни инструменти, които засилват отговорностите на администраторите на данни. Тези инструменти трябва да дават на администраторите на данни пълна отчетност по отношение на управлението на данни. В този смисъл полезно понятие е „управлението на данни“. То обхваща всички правни, технически и организационни средства, чрез които организациите осигуряват пълна отговорност за начина, по който се борави с данните, като планиране и контрол, използване на звукови технологии, подходящо обучение на състава, одити на съответствието, и т.н.

V.3. **Технологии, съобразени с правото на личен живот**

43. ЕНОЗД изразява задоволство, че в параграф 2.3 от съобщението се говори за европейски сертификат за технологии, съобразени с правото на личен живот. Освен това би могла да се спомене „защитата на личния живот още при проектирането“, както и необходимостта от определяне на „най-добрите съществуващи техники“, които са в съответствие с рамката на ЕС за защита на данните.

44. ЕНОЗД е на мнение, че „защитата на личния живот още при проектирането на продукта“ и технологиите, съобразени с правото на личен живот, биха могли да бъдат полезни инструменти за по-добра защита и за по-ефективно използване на информацията. ЕНОЗД предлага два пътя напред, които не се изключват взаимно:

— режим за сертифициране на неприкосновеността на личния живот и защитата на данните ([25]) като вариант за създателите и потребителите на информационни системи, със или без подкрепа чрез финансиране от ЕС или законодателство на ЕС,

([24]) Работната група за защита на данните по член 29, в която участва ЕНОЗД, ще работи усилено с цел принос към тази публична консултация.

([25]) Пример за подобен режим е Европейският печат за неприкосновеност на личния живот (EuroPriSe).

— правно задължение за създателите и потребителите на информационни системи да използват системи, които са в съответствие с принципа на защита на личния живот още при проектирането на продукта. Това може да наложи разширяване на настоящия обхват на закона за защита на данните с цел създателите да носят отговорност за разработваните от тях информационни системи ([26]).

ЕНОЗД предлага тези възможни пътища да се посочат в Програмата от Стокхолм.

V.4. **Външни аспекти**

45. Друг, засегнат в съобщението въпрос е разработването и утвърждаването на международни стандарти за защита на данните. Понастоящем се извършват много дейности с оглед установяването на възможни стандарти за глобално прилагане, например от Международната конференция на комисарите по неприкосновеността на личния живот и защитата на данните. В близко бъдеще това би могло да доведе до международно споразумение. ЕНОЗД предлага Програмата от Стокхолм да подкрепи тези дейности.

46. В съобщението се посочва и сключването на двустранни споразумения, въз основа на вече постигнатия напредък със Съединените щати. ЕНОЗД споделя необходимостта от ясна правна рамка за предаването на данни на трети държави и във връзка с това приветства съвместната работа на органите на ЕС и на САЩ в контактната група на високо равнище относно евентуален трансатлантически правен инструмент по отношение на защитата на данните, като същевременно призовава за повече яснота и внимание към определени въпроси ([27]). В този контекст е интересно да се отбележат и идеите в доклада за вътрешните работи за евроатлантическо пространство на сътрудничество в областта на свободата, сигурността и правосъдието, по отношение на което, според доклада, ЕС следва да вземе решение до 2014 г. Такова пространство не би било възможно без подходящи гаранции за защита на данните.

47. Според ЕНОЗД европейските стандарти за защита на данните, основани на Конвенция № 108 на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни ([28]) и съдебната практика на Съда на Европейските общности и на Европейския съд по правата на човека следва да определят нивото на защита в общо споразумение със Съединените щати относно защитата на данните и обмена на данни. Подобно общо споразумение би могло да бъде основата за конкретни договорености за обмена на лични данни. Това придобива още по-голяма важност предвид формулираното в параграф 4.2.1 от съобщението намерение, че Европейският съюз трябва да сключва споразумения за полицейско сътрудничество винаги, когато това е необходимо.

48. ЕНОЗД разбира напълно необходимостта от засилване на международното сътрудничество, в някои случаи със страни, които не защитават основните права. Същевременно ([29]) е от решаващо значение да се вземе предвид, че е вероятно това международно сътрудничество да доведе до голямо нарастване в събирането и международното предаване на данни. Ето защо е особено важно принципите на справедлива и законосъобразна обработка, както и принципите на надлежна процедура изобщо, да се прилагат при събирането и предаването на лични данни отвъд границите на Съюза, както и личните данни да се предават на трети държави или международни организации само ако въпросните трети страни гарантират адекватно ниво на защита или други подходящи предпазни мерки.

49. В заключение ЕНОЗД препоръчва в Програмата от Стокхолм да се наблегне на значението на общи споразумения със Съединените щати и други трети държави за защита на данните и обмен на данни, основани на нивото на защита, гарантирано на територията на ЕС. В по-широк план ЕНОЗД изтъква колко е важно активно да се утвърждава спазването на основните права, и в частност на защитата на данните, в отношенията с трети държави и с международни организации ([30]). Освен това в Програмата от Стокхолм би могло да се спомене принципното виждане, че обменът на лични данни с трети държави изисква адекватно ниво на защита или други подходящи предпазни мерки в тези трети държави.

VI. **ИЗПОЛЗВАНЕ НА ИНФОРМАЦИЯ**

VI.1. **Към европейски модел за информация**

50. Един по-добър обмен на информация в пространството на свобода, сигурност и правосъдие е основна цел на политиките на Европейския съюз. В параграф 4.1.2 от съобщението се подчертава, че сигурността в Европейския съюз почива на добре работещи механизми за обмен на данни между националните органи и европейските действащи лица. В отсъствието на европейски полицейски сили, европейска система за наказателно правораздаване и европейски граничен контрол този акцент върху обмена на информация е логичен. Следователно мерките, свързани с информацията, представляват важен принос на Европейския съюз, който

([26]) Потребителите на информация, както и администраторите или лицата, обработващи данни, са обхванати от закона за защита на данните.

([27]) Вж. Становище на ЕНОЗД от 11 ноември 2008 г. относно Окончателния доклад на контактната група на високо равнище ЕС — САЩ относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни, ОВ C 128, 6.6.2009 г., стр. 1.

([28]) ETS № 108, 28.1.1981 г.

([29]) Вж. Писмо на ЕНОЗД от 28 ноември 2005 г. по повод съобщението на Комисията относно външното измерение на пространството на свобода, сигурност и правосъдие, което може да се намери на уебсайта на ЕНОЗД.

([30]) Съдебната практика напоследък по отношение на списъци на терористи потвърждава необходимостта от гаранции — както и в отношенията със Съединените щати — за да се гарантира, че мерките за борба с тероризма съответстват на стандартите на ЕС за основните права (Обединени дела C-402/05 P и C-415/05 P, Kadi и Al Barakaat Foundation/Съвета, съдебно решение от 3 септември 2008 г., непубликувано).

позволява на органите на държавите-членки да търсят ефективно решение на трансграничната престъпност и ефективно да защитават външните граници. Същевременно те допринасят не само за сигурността на гражданите, но и за тяхната свобода — свободното движение на лица беше вече споменато като аспект на настоящото становище — и за правосъдието.

51. Тъкмо поради тези причини в Програмата от Хага беше въведен принципът на наличност. Според този принцип информация, необходима за борбата с престъпността, следва да преминава вътрешните граници на ЕС безпрепятствено. Опитът напоследък показва, че е трудно да се приложи този принцип в законодателните мерки. Предложението на Комисията за рамково решение на Съвета относно обмена на информация съгласно принципа на наличност от 12 октомври 2005 г. ([31]) не беше прието от Съвета. Държавите-членки не бяха готови да приемат последиците от принципа на наличност в пълното му измерение. Вместо това бяха приети инструменти с по-ограничен обхват ([32]) като Решение 2008/615/ПВР на Съвета от 23 юни 2008 г. за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност („Решение от Прюм“) ([33]).

52. Докато принципът на наличност беше в сърцевината на Програмата от Хага, сега Комисията очевидно възприема по-скромен подход. Той предвижда по-нататъшно насърчаване на обмена на информация между органите на държавите-членки чрез въвеждането на европейски модел за информация. Шведското председателство на ЕС има същото виждане ([34]). То ще представи предложение за стратегия относно обмена на информация. Съветът вече започна работа по този амбициозен проект за стратегия на Европейския съюз за управление на информацията, която е тясно свързана с европейския модел за информация. ЕНОЗД отбелязва това развитие с голям интерес и подчертава вниманието, което следва да бъде отделено в тези проекти на елементите, свързани със защитата на данните.

Европейски модел за информация и защита на данните

53. Като начало следва да се подчертае, че бъдещето на пространството на свобода, сигурност и правосъдие не следва да се определя от технологиите, т.е. почти безграничните възможности, предлагани от новите технологии, следва винаги да се съпоставят със съответните принципи за защита на данните и да се използват само дотолкова, доколкото съответстват на тези принципи.

54. ЕНОЗД отбелязва, че съобщението представя информационния модел не само като технически: силна способност за стратегически анализ и по-добро събиране и обработка на оперативна информация. Освен това ЕНОЗД отчита, че следва да се вземат предвид аспекти, свързани с политиките, като критерии за събиране, обмен и обработка на данните, събрани във връзка със сигурността, при спазване на принципите на защита на данните.

55. Както понастоящем, така и в бъдеще и информационните технологии, и правните условия ще бъдат от основно значение. ЕНОЗД приветства съобщението, което използва за отправна точка разбирането, че един европейски модел за информация не може да почива на съображения от техническо естество. Особено важно е, че информацията се събира, обменя и обработва единствено въз основа на конкретни нужди за сигурност и като се вземат предвид принципите на защита на данните. Освен това ЕНОЗД изцяло подкрепя необходимостта от определяне на механизъм за последващи действия, позволяващ да се оцени функционирането на обмена на информация; ЕНОЗД предлага Съветът да разработи допълнително тези елементи в Програмата от Стокхолм.

56. В този смисъл ЕНОЗД подчертава, че защитата на данните, чиято цел е да защитава гражданите, не следва да се възприема като възпрепятстваща ефективното управление на данните. Тя предоставя важни средства за подобряването на съхранението, достъпа и обмена на информация. Правата на субекта на данни да бъде информиран за това коя информация, отнасяща се до него, се обработва и да коригира невярна информация също могат да укрепят точността на данните в системите за управление на данните.

57. По същество законът за защита на данните има за последици следното: ако данните са необходими за конкретна и законосъобразна цел, те могат да се използват; ако не са необходими за ясно определена цел, личните данни не следва да се използват. В първия случай може да са необходими допълнителни мерки за предоставянето на адекватни гаранции.

58. ЕНОЗД обаче се отнася критично към степента, в която съобщението посочва „набелязването на бъдещи нужди“ като част от информационния модел. ЕНОЗД подчертава, че и в бъдеще принципът на ограничаване в рамките на целта следва да бъде водещ при изграждането на информационни системи ([35]). Този принцип е една от основните гаранции, които системата за защита на данните дава на гражданите: те трябва да могат да знаят предварително за каква цел се събират свързани с тях данни и че те ще бъдат използвани само за тази цел, особено в бъдеще. Тази гаранция дори е заложена в член 8 от Хартата на основните права на Европейския съюз. Принципът на ограничаване в рамките на целта допуска изключения, които в частност са свързани с пространството на свобода, сигурност и правосъдие, но тези изключения не следва да определят изграждането на система.

([31]) COM(2005) 490 окончателен.

([32]) От гледна точка на наличността; решението от Прюм съдържа широкообхватни разпоредби за използването на биометрични данни (ДНК и пръстови отпечатъци).

([33]) ОВ L 210, 6.8.2008 г., стр. 1.

([34]) Вж. Работна програма на председателството на ЕС, цитирана в бележка под линия 5, стр. 23.

([35]) Вж. също точка 41 по-горе.

Избор на подходяща архитектура

59. Изборът на подходяща архитектура за обмен на информация е в основата на всичко. Значението на подходяща информационна архитектура се отчита в съобщението (параграф 4.1.3), но за съжаление само във връзка с оперативната съвместимост.

60. ЕНОЗД изтъква друг аспект: в рамките на европейския модел за информация изискванията за защита на данните следва да бъдат неотделима част от всяко развитие на системата и не следва да се възприемат единствено като необходимо условие за законността на една система ([36]). Използването следва да се определя от концепцията за „защита на личния живот още при проектирането“ и необходимостта да се уточнят „най-добрите съществуващи техники“ ([37]), както беше посочено в точка 43 по-горе. Европейският модел за информация следва да почива на тези концепции. 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“. ЕНОЗД препоръчва Съветът да включи тези елементи в Програмата от Стокхолм.

Оперативна съвместимост на системи

61. ЕНОЗД подчертава, че оперативната съвместимост не е чисто технически въпрос, а носи и последици за защитата на гражданите, и в частност за защитата на данните. В контекста на защитата на данните оперативната съвместимост на системите, ако е добра, има очевидни предимства за избягване на двойното съхраняване. Същото така обаче е очевидно, че техническото осъществяване на достъп или обмен на данни в много случаи се превръща в силен подтик за действителен достъп до тези данни или обмена им. С други думи, оперативната съвместимост крие конкретни рискове от взаимно свързване на бази данни, които обслужват различни цели ([38]). Тя може да повлияе на строгите ограничения върху целта на базите данни.

62. Накратко, самият факт, че обменът на цифрова информация между оперативно съвместими бази данни или сливането на тези бази данни са технически възможни, не оправдава изключение от принципа за ограничаване в рамките на целта. В конкретни случаи оперативната съвместимост следва да се основава на ясни и премислени избори в областта на политиките. ЕНОЗД предлага това да се уточни в Програмата от Стокхолм.

([36]) Вж. „Насоки и критерии за разработването, прилагането и използването на технологии за сигурност, укрепващи неприкосновеността на личния живот“, разработени в рамките на проекта PRISE (http://www.prise.oeaw.ac.at).

([37]) Най-добри съществуващи техники означава най-ефективната и напреднала фаза в разработването на дейности и методи на действие, която е показателна за практическата пригодност на определени техники за принципното осигуряване на съответствие на приложенията и системите за сигурност на информационните технологии с изискването на регулаторната рамка на ЕС за неприкосновеност на личния живот, защита на данните и сигурност.

([38]) Вж. забележките на ЕНОЗД по отношение на Съобщението на Комисията относно оперативната съвместимост на европейските бази данни, 10 март 2006 г., които могат да се намерят на интернет адрес: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2. **Използване на събрана информация за други цели**

63. В съобщението не е специално засегната една от най-важните тенденции през последните години, а именно използването за целите на правоприлагането на данни, събрани в частния сектор за търговски цели. Тази тенденция се отнася не само до данни за трафика в областта на електронните комуникации и данните на лица, които летят до (определени) трети държави ([39]), но се съсредоточава и върху финансовия сектор. Пример за това е Директива 2005/60/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 г. за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризъм ([40]). Друг добре известен и широко обсъждан пример засяга обработката от Дружеството за световна междубанкова финансова телекомуникация (SWIFT) ([41]) на лични данни, необходими за целите на програмата на американското министерство на финансите за проследяване на финансирането на тероризма.

64. ЕНОЗД смята, че тези тенденции заслужават специално внимание в Програмата от Стокхолм. Те могат да се разглеждат като отклонения от принципа за ограничаване в рамките на целта и често нарушават сериозно неприкосновеността на личния живот, тъй като използването на тези данни може да разкрие много за поведението на лицата. Всеки път, когато се предлагат такива мерки, трябва да се представят много убедителни доказателства, че подобна нарушаваща неприкосновеността мярка е необходима. Ако такива доказателства бъдат представени, трябва да се гарантира, че правата на лицата са напълно защитени.

65. ЕНОЗД е на мнение, че използването за правоприлагане на лични данни, събрани за търговски цели, следва да се допуска само при строго определени условия, като например:

— данните се използват само за точно определени цели, като например борбата с тероризма или тежка престъпност, като решение се взема за всеки отделен случай,

— данните се предават чрез система „push“, а не чрез система „pull“ ([42]),

([39]) Вж. например точка 15 по-горе.

([40]) ОВ L 309, 25.11.2005 г., стр. 15.

([41]) Вж. становище 10/2006 на работна група „Член 29“ относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT).

([42]) В системата „push“ администраторът на данни изпраща данните при поискване („тласка“) на правоприлагащия орган. В системата „pull“ правоприлагащият орган има достъп до базата данни на администратора и извлича („тегли“) информация от тази база данни. В системата „pull“ за администратора на данни е по-трудно възобнови отговорността си.

— искането за данни следва да е съразмерно, с тесен фокус и по принцип да се основава на подозрения за конкретни лица,

— следва да се избягват рутинни търсения, извличане на данни и съставяне на профили,

— всяко използване на данни за целите на правоприлагането следва да се вписва с цел упражняване на ефективен контрол върху използването от субекта на данни в рамките на правата му и от съдебните органи.

VI.3. **Информационни системи и органи на ЕС**

Информационни системи със или без централизирано съхраняване ([43])

66. През последните години броят на информационните системи въз основа на законодателство на ЕС нарасна значително в пространството на свобода, сигурност и правосъдие. Понякога се вземат решения за създаването на система, която налага централизирано съхраняване на данни на европейско равнище, а в други случаи законът предвижда единствено обмен на информация между национални бази данни. Шенгенската информационна система е може би най-добрият пример за система с централизирано съхраняване. От гледна точка на защитата на данните Решение 2008/615/ПВР на Съвета („Решение от Прюм“) ([44]) е най-значимият пример за система без централизирано съхраняване, тъй като то предвижда огромен обмен на биометрични данни между органите в държавите-членки.

67. Съобщението е нагледен пример, че тази тенденция на създаване на нови системи ще продължи. Един пример, взет от параграф 4.2.2, е информационна система, която разширява Европейската информационна система за съдимост (ECRIS), така че да обхване граждани на държави, които не членуват в ЕС. Комисията вече възложи извършването на проучване относно Европейския списък на осъдени граждани на трети държави, което евентуално би могло да доведе до централизирана база данни. Друг пример е обменът на информация за лица, вписани в регистри по несъстоятелност в други държави-членки, в рамките на електронното правосъдие (параграф 3.4.1 от съобщението) без централизирано съхраняване.

68. Една децентрализирана система би имала определени преимущества от гледна точка на защитата на данните. Така се избягва двойното съхраняване на данни от органа на държавата-членка и от централизираната система, отговорността за данните е ясна, тъй като органът на държавата-членка ще бъде администратор на данните, а контролът от съдебните органи и от органите за защита на данните може да се извършва на равнище държава-членка. Но тази система също има слабости при обмена на данни с други юрисдикции, като например да се гарантира, че информацията се поддържа в актуално състояние и в държавата на произход, и в държавата на местоназначение, както и как да се осигури ефективен контрол от двете страни. Още по-сложно е да се гарантира отговорност за техническата система при обмена. Тези слабости могат да бъдат преодолени, като се избере централизирана система, поне за части от която отговорност носят европейски органи (като например техническата инфраструктура).

69. В този смисъл би било полезно да се разработят самостоятелни критерии за избора между централизирани и децентрализирани системи, като се гарантират ясни и премислени избори на политиките в конкретните случаи. Тези критерии могат да допринесат за функционирането на самите системи, както и защитата на данните на гражданите. ЕНОЗД предлага в Програмата от Стокхолм да се включи намерението за разработване на такива критерии.

Широкомащабни информационни системи

70. Параграф 4.2.3.2 от съобщението разглежда накратко бъдещето на широкомащабните информационни системи с акцент върху Шенгенската информационна система (ШИС) и визовата информационна система (ВИС).

71. В параграф 4.2.3.2 се споменава и създаването на система за електронно записване на влизанията и излизанията от територията на държавите-членки на Европейския съюз, както и програми за регистрирани пътници. Системата беше оповестена по-рано от Комисията като част от „пакета от мерки за границите“ по инициатива на заместник-председателя Фратини ([45]). В предварителните си забележки ([46]) ЕНОЗД се отнесе доста критично към това предложение, тъй като необходимостта от такава нарушаваща неприкосновеността система в допълнение към съществуващите широкомащабни системи не беше ясно обоснована. ЕНОЗД не вижда допълнителни доводи в полза на необходимостта от такава система и затова предлага на Съвета тази идея да не се споменава в Програмата от Стокхолм.

72. В този контекст ЕНОЗД би желал да се позове на становищата си по повод различни инициативи в областта на обмена на информация на ЕС ([47]), в които е направил многобройни предложения и забележки относно последиците за защитата на данните от използването на големи бази данни на равнище ЕС. Наред с другото, ЕНОЗД обърна специално внимание на необходимостта от

([43]) Централизирано съхраняване в този контекст се разбира като съхраняване на централно европейско равнище, докато децентрализирано съхраняване означава съхраняване на равнище държави-членки.

([44]) Вж. бележка под линия 33.

([45]) Съобщение на Комисията „Подготовка на следващите стъпки в управлението на границите в Европейския съюз“, 13.2.2008 г., COM(2008) 69.

([46]) Предварителни забележки на ЕНОЗД по три съобщения на Комисията относно управлението на границите (COM(2008) 69, COM(2008) 68 и COM(2008) 67), 3 март 2008 г. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) По-конкретно: Становище от 23 март 2005 г. относно предложението за регламент на Европейския парламент и на Съвета относно визовата информационна система (ВИС) и обмена на данни между държавите-членки относно визите за краткосрочно пребиваване, ОВ C 181, 23.7.2005 г., стр. 13, и Становище от 19 октомври 2005 г. относно три предложения във връзка със Шенгенската информационна система от второ поколение (ШИС II), ОВ C 91, 19.4.2006 г., стр. 38.

въвеждането на твърди и съобразени гаранции, и на съразмерността и нуждата от оценки на въздействието, преди да се предлагат или предприемат мерки в тази област. ЕНОЗД винаги е застъпвал виждането за правилен и съответстващ на защитата на данните баланс между изискванията за сигурност и защитата на неприкосновеността на лицата, които са обект на системите. ЕНОЗД възприе същата позиция в качеството си на надзорник на централните части на системите.

73. Освен това ЕНОЗД използва тази възможност, за да наблегне на необходимостта от последователен подход към обмена на информация на ЕС като цяло, изразяващ се в правна, техническа и надзорна последователност между вече действащите системи и тези, които са в процес на разработване. Всъщност, днес, повече отколкото преди, има ясна необходимост от смело и цялостно виждане за това как следва да изглежда обменът на информация на ЕС и какво да е бъдещето на широкомащабните информационни системи. Само въз основа на такова виждане би могло да се преосмисли създаването на система за електронно записване на влизанията и излизанията от територията на държавите-членки на Европейския съюз.

74. ЕНОЗД предлага в Програмата от Стокхолм да се посочи намерението за разработване на такова виждане, което следва да включва обмисляне на евентуалното влизане в сила на Договора от Лисабон и съответните последици за системите, базирани на правно основание от първи и трети стълб.

75. И най-накрая, в съобщението се споменава създаването на нова агенция, която следва да бъде компетентна и за електронната система за влизане/излизане. Междувременно Комисията прие предложение за създаването на такава агенция ([48]). ЕНОЗД подкрепя принципно това предложение, тъй като то може да увеличи ефективното функциониране на тези системи, включително на защитата на данните. ЕНОЗД ще представи становище своевременно.

Европол и Евроюст

76. Ролята на Европол се споменава няколко пъти в съобщението, което изтъква като приоритетен въпрос, че Европол трябва да заема централно място в координирането, обмена на информация и обучението на работещите в сферата. Освен това, в параграф 4.2.2 от съобщението се споменават неотдавнашните промени в правната рамка за сътрудничество между Европол и Евроюст и се посочва, че укрепването на Евроюст ще продължи, по-специално в областта на разследването на трансграничната организирана престъпност. ЕНОЗД подкрепя изцяло тези цели, при условие че се спазват по подходящ начин предпазните мерки за защита на данните.

77. Във връзка с това ЕНОЗД приветства новото проектоспоразумение, постигнато наскоро между Европол и Евроюст ([49]), което цели подобряване и укрепване на взаимното сътрудничество между двата органа и предвижда ефикасен обмен на информация помежду им. Това е дейност, в която ефикасната и ефективна защита на данните играе решаваща роля.

VI.4. **Използване на биометрични данни**

78. ЕНОЗД отбелязва, че в съобщението не се разглежда въпросът за нарастващото използване на биометрични данни в различни правни инструменти на Европейския съюз относно използването на информационния обмен, включително в инструментите за създаване на широкомащабните информационни системи. Този факт буди съжаление, като се има предвид, че въпросът е от особено важно и чувствително естество в контекста на защитата на данните и неприкосновеността на личния живот.

79. Макар да признава предимствата като цяло от използването на биометричните данни, ЕНОЗД непрекъснато изтъква голямото въздействие от използването на такива данни върху правата на лицата и предлага във всяка конкретна система да се включат строги предпазни мерки за използването на биометрични данни. В този контекст решението неотдавна на Европейския съд по правата на човека по делото *S. и Marper/Обединеното кралство* ([50]) дава полезни индикации, по-конкретно във връзка с обосновката и границите на използване на биометрични данни. По-конкретно, използването на ДНК информация може да разкрие чувствителна информация за лица, а трябва да се вземат предвид и нарастващите технически възможности за извличане на информация от ДНК. Освен това в случая със широкомащабното използване на биометрични данни в информационните системи съществува проблем в резултат на вътрешно-присъщи неточности при събирането и сравняването на биометрични данни. Поради тези причини законодателят на ЕС следва да се ограничава при използването на тези данни.

80. Друг често възникващ през последните години въпрос е използването на пръстови отпечатъци на деца и на възрастни хора предвид вътрешно-присъщите несъвършенства на биометричните системи при тези възрастови групи. ЕНОЗД поиска задълбочено проучване, за да се определи точно акуратността на системите ([51]). ЕНОЗД предложи възрастово ограничение от 14 години за деца, освен ако проучването не покаже друго. ЕНОЗД предлага този въпрос да се засегне в Програмата от Стокхолм.

([48]) Предложение на Комисията от 24 юни 2009 г. за регламент на Европейския парламент и на Съвета за създаване на агенция за оперативното управление на Шенгенската информационна система от второ поколение (ШИС II), визовата информационна система (ВИС), EURODAC и други широкомащабни информационни системи в областта на свободата, сигурността и правосъдието (COM(2009) 293/2).

([49]) Проект за споразумение, който е одобрен от Съвета и предстои да бъде подписан от двете страни. Вж. регистър на Съвета:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Обща молба 30562/04 и 30566/04, S. и Marper срещу Обединеното кралство, решение от 4 декември 2008 г., Европейски съд по правата на човека, непубликувано.

([51]) Становище от 26 март 2008 г. относно предложението за регламент за изменение на Регламент (ЕО) № 2252/2004 на Съвета относно стандартите за отличителните знаци за сигурност и биометричните данни в паспортите и документите за пътуване, издавани от държавите-членки, ОВ C 200, 6.8.2008 г., стр. 1.

81. Като се има предвид казаното, ЕНОЗД предполага, че би било полезно да се разработят самостоятелни критерии за използването на биометрични данни. Тези критерии следва да гарантират, че данните се използват само когато това е необходимо, адекватно и съразмерно, както и когато законодателят е установил изрична, ясно определена и законосъобразна цел, По-конкретно, биометричните данни и в частност ДНК данните не следва да се използват, ако същият резултат може да се постигне чрез използването на друга, не толкова чувствителна информация.

VII. **ДОСТЪП ДОД ПРАВОСЪДИЕ И ЕЛЕКТРОННО ПРАВОСЪДИЕ**

82. Технологиите ще се използват и като средство за по-добро съдебно сътрудничество. Според параграф 3.4.1 от съобщението електронното правосъдие предоставя на гражданите по-лесен достъп до правосъдие. То представлява портал, съдържащ информация и видеоконференции като част от правната процедура. Освен това то позволява правни процедури онлайн и предвижда взаимното свързване на национални регистри, като например регистри по несъстоятелност. ЕНОЗД отбелязва, че в съобщението не се посочват нови инициативи относно електронното правосъдие, а се утвърждават дейности, които са вече в ход. ЕНОЗД участва в някои от тези дейности като последващо действие по становището му от 19 декември 2008 г. относно Съобщението на Комисията „Към европейска стратегия в областта на електронното правосъдие“ ([52]).

83. Електронното правосъдие е амбициозен проект, който трябва да бъде изцяло подкрепен. То може ефективно да подобри съдебната система в Европа и съдебната защита на гражданите. Електронното правосъдие е значителна стъпка напред към Европейско пространство на правосъдие. Като се има предвид тази положителна оценка, мога да се направят няколко забележки:

— технологичните системи за електронно правосъдие следва да бъдат изградени в съответствие с принципа „защита на личния живот още при проектирането“. Както вече беше посочено, във връзка с европейския модел за информация изборът на подходяща архитектура е в основата на всичко,

— взаимовръзката и оперативната съвместимост на системите следва да спазва принципа за ограничаване в рамките на целта,

— отговорностите на различните участници следва да бъдат точно определени,

— последиците за лицата от свързването на национални регистри с деликатни лични данни, като например регистри по несъстоятелност, следва да бъдат анализирани предварително.

VIII. **ЗАКЛЮЧЕНИЯ**

84. ЕНОЗД одобрява акцента в съобщението върху защитата на основните права, и по-конкретно защитата на личните данни като един от ключовите въпроси, които имат отношение към бъдещето на пространството на свобода, сигурност и правосъдие. ЕНОЗД е на мнение, че в съобщението правилно се насърчава постигането на баланс между необходимостта от подходящи инструменти за гарантиране на сигурността на гражданите и защитата на основните им права. ЕНОЗД отчита, че следва да се наблегне повече на защитата на личните данни.

85. ЕНОЗД подкрепя напълно параграф 2.3 от съобщението и настоява за цялостен режим за защита на данните, който обхваща всички области на компетентност на ЕС, независимо от влизането в сила на Договора от Лисабон. Във връзка с това ЕНОЗД препоръчва:

— да се заяви необходимостта от ясна дългосрочна визия за такъв цялостен режим в Програмата от Стокхолм,

— да се оценят приетите в тази област мерки, тяхното конкретно прилагане и ефективност, като се вземат предвид последиците за неприкосновеността на личния живот и ефективността от гледна точка на правоприлагането,

— като приоритетна в Програмата от Стокхолм да се включи необходимостта от нова законодателна рамка, заменяща, *inter alia*, Рамково решение 2008/977/ПВР на Съвета.

86. ЕНОЗД приветства намеренията на Комисията да потвърди отново принципите на защита на данните, които трябва да бъдат свързани с публичната консултация, обявена от Комисията по време на проведената на 19—20 май 2009 г. конференция „Личните данни — по-голямо използване, по-голяма защита?“. По същество, ЕНОЗД подчертава важността на принципа за ограничаване в рамките на целта като крайъгълен камък на закона за защита на данните и насочването на вниманието към възможностите за увеличаване на ефективността на приложението на принципите на защита на данните чрез инструменти, които могат да укрепят отговорностите на администраторите на данни.

87. „Защитата на личния живот още при проектирането“ и технологии, съобразени с правото на личен живот, биха могли да се насърчават чрез:

— режим за сертифициране на неприкосновеността на личния живот и защитата на данните като вариант за създателите и потребителите на информационни системи,

— правно задължение за създателите и потребителите на информационни системи да използват системи, които са в съответствие с принципа на защита на личния живот още при проектирането на продукта.

88. Що се отнася до външните аспекти на защитата на данните, ЕНОЗД препоръчва:

— в Програмата от Стокхолм да се наблегне на значението на общи споразумения със Съединените щати и други трети държави за защита на данните и обмена на данни,

([52]) Становище на ЕНОЗД от 19 декември 2008 г. относно Съобщението на Комисията „Към европейска стратегия в областта на електронното правосъдие“, ОВ C 128, 6.6.2009 г., стр. 13

— активно да се утвърждава спазването на основните права, и в частност на защитата на данните, в отношенията с трети държави и международни организации,

— в Програмата от Стокхолм да се посочи, че обменът на лични данни с трети държави изисква адекватно ниво на защита или други подходящи предпазни мерки в тези трети държави.

89. ЕНОЗД отбелязва с голям интерес развитието по посока на стратегия на Европейския съюз за управление на информацията и на европейски модел за информация, и подчертава вниманието, което следва да бъде отделено в тези проекти на елементите, свързани със защитата на данните, като това предстои да бъде доразвито в Програмата от Стокхолм. Архитектурата за обмен на информация следва да се основава на „защита на личния живот още при проектирането на продукта“ и на „най-добрите съществуващи техники“.

90. Самият факт, че обменът на цифрова информация между оперативно съвместими бази данни или сливането на тези бази данни са технически възможни, не оправдава изключение от принципа за ограничаване в рамките на целта. В конкретни случаи оперативната съвместимост следва да се основава на ясни и премислени избори в областта на политиките. ЕНОЗД предлага това да се уточни в Програмата от Стокхолм.

91. ЕНОЗД е на мнение, че използването за правоприлагане на лични данни, събрани за търговски цели, следва да се допуска само при строго определени условия, уточнени в точка 65 от настоящото становище.

92. Други предложения по отношение на използването на лична информация включват:

— разработването на критерии по същество за избора между централизирани и децентрализирани системи, както и посочването на намерението за разработване на такива критерии в Програмата от Стокхолм,

— създаването на система за електронно записване на влизанията и излизанията от територията на държавите-членки на Европейския съюз, както и програми за регистрирани пътници, не следва да се посочва в Програмата от Стокхолм,

— подкрепа за заздравяването на Европол и Евроюст, и за новото, наскоро изготвено споразумение между Европол и Евроюст,

— разработване на самостоятелни критерии за използването на биометричните данни, като се гарантира, че данните се използват само когато това е необходимо, адекватно и съразмерно, както и когато законодателят е посочил изрична, ясно определена и законосъобразна цел. ДНК данните не следва да се използват, ако същият резултат може да се постигне чрез използването на друга, не толкова чувствителна информация.

93. ЕНОЗД изразява подкрепа за електронното правосъдие и прави няколко забележки по това как проектът би могъл да бъде подобрен (вж. точка 83).

Съставено в Брюксел на 10 юли 2009 г.

Peter HUSTINX

Европейски надзорен орган по защита на данните