Становище на Европейския надзорен орган по защита на данните относно Съобщение на Комисията до Европейския парламент и до Съвета — „Стратегията за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа“

(2011/C 101/02)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

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

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

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

като взе предвид искането за становище в съответствие с Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни ([2]), и по-специално член 41 от него,

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ

I. ВЪВЕДЕНИЕ

1. На 22 ноември 2010 г. Комисията прие съобщение, озаглавено „Стратегията за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа“ (наричано по-нататък „съобщението“) ([3]). Съобщението беше изпратено на ЕНОЗД за консултация.

2. ЕНОЗД приветства факта, че Комисията се е обърнала към него за консултация. Още преди приемането на съобщението ЕНОЗД представи неофициални коментари по проекта на текста, някои от които бяха взети предвид в окончателния вариант на съобщението.

Контекст на съобщението

3. Стратегията за вътрешна сигурност на ЕС (наричана по-нататък СВС), предмет на съобщението, беше приета на 23 февруари 2010 г. по време на испанското председателство ([4]). Стратегията излага модел за сигурност на Европа, който включва, наред с други неща, действия по правоприлагане и съдебно сътрудничество, управление на границите и гражданска защита при надлежно отчитане на споделени европейски ценности като основните права. Тя има следните основни цели:

   — да представи пред обществеността съществуващите инструменти на ЕС, които вече помагат да се гарантира сигурността и свободата на гражданите на ЕС, както и добавената стойност, която създават действията на ЕС в тази област;

   — да доразвие общите средства и политики, като използва по-интегриран подход, при който се обръща внимание на причините за несигурността, а не само на последиците;

   — укрепва правоприлагането и съдебното сътрудничество, управлението на границите, гражданската защита и управлението на бедствия.

4. Целта на СВС е да се справи с най-неотложните заплахи и предизвикателства пред сигурността на ЕС като тежката и организираната престъпност, тероризма и киберпрестъпността, управлението на външните граници на ЕС и изграждането на устойчивост на природните и предизвиканите от човека бедствия. Стратегията предвижда общи насоки, принципи и указания относно начините, по които ЕС следва да реагира при такива проблеми, и в нея се съдържа призив Комисията да предложи обвързани със срокове действия за изпълнение на стратегията.

5. Освен това е важно в този контекст да се направи позоваване на неотдавнашните заключения на Съвета по правосъдие и вътрешни работи относно създаването и прилагането на цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност, приети на 8-9 ноември 2010 г. ([5]) (наричани по-нататък „заключенията от ноември 2010 г.“). Този документ следва заключението на Съвета относно архитектурата на вътрешната сигурност от 2006 г. ([6]), и в него се съдържа призив Съветът и Комисията да определят цялостна СВС на базата на общите ценности и принципи на ЕС, утвърдени от Хартата на основните права на Европейския съюз. ([7])

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) ОВ L 8, 12.1.2001 г., стр. 1.
([3]) COM(2010) 673 окончателен.
([4]) Док. 5842/2/10.
([5]) 3043-то заседание на Съвета по правосъдие и вътрешни работи, 8—10 ноември 2010 г., Брюксел
([6]) Док. 7039/2/06 JAI 86 CATS 34
([7]) Цикълът на политиката на ЕС за борба с организираната и тежката международна престъпност, посочен в заключенията от ноември 2010 г., се състои от четири етапа: 1) разработване на политики въз основа на Оценката на Европейския съюз на заплахата от тежката и организираната международна престъпност (EU SOCTA), 2) определяне на политики и вземане на решения чрез набелязването от страна на Съвета на ограничен брой приоритети, 3) изпълнение и наблюдение на годишни оперативни планове за действие (ОПД) и 4) в края на цикъла на политиката ще се извърши задълбочена оценка, която ще служи като отправна точка за следващия цикъл на политиката.

6. Сред указанията и целите, които следва да обуславят изпълнението на СВС, в заключенията от ноември 2010 г. се посочва обмисляне на активен подход на основата на разузнавателна информация, задължително сътрудничество между агенциите на ЕС, включително по-нататъшното подобряване на обмена на информация помежду им и целта гражданите да осъзнаят значимостта на работата, която Съюзът извършва в тяхна защита. Съща така в заключенията се съдържа призив Комисията да разработи съвместно с експерти от съответните агенции и държави-членки многогодишен стратегически план (наричан по-нататък МСП) за всеки от приоритет, като определи най-подходящата стратегия за решаването на проблема. Комисията се призовава също да разработи чрез консултации с експертите на държавите-членки и агенциите на ЕС независим механизъм за оценяване на изпълнението на МСП. ЕНОЗД ще разгледа тези въпроси по-нататък в настоящото становище, тъй като те са тясно свързани със защитата на личните данни, неприкосновеността на личния живот и другите свързани основни права и свободи и оказват значително въздействие върху тях.

Съдържание и цел на съобщението

7. Съобщението предлага пет стратегически цели, всяка от които е свързана с неприкосновеността на личния живот и защитата на данните:

— разбиване на международните престъпни мрежи,

— предотвратяване на тероризма и мерки срещу радикализацията и набирането на терористи,

— повишаване на нивото на сигурност за гражданите и предприятията в киберпространството

— укрепване на сигурността чрез управление на границите, и

— подобряване на устойчивостта на Европа спрямо кризи и бедствия.

8. Стратегията за вътрешна сигурност в действие, както е предложена в съобщението, определя общ дневен ред за държавите-членки, Европейския парламент, Комисията, Съвета, агенциите и другите участници, включително гражданското общество и местните органи, и предлага начин за тяхната съвместна работа през следващите четири години, за да бъдат постигнати целите на СВС.

9. Съобщението използва като база Договора от Лисабон и в него се признават насоките, заложени в Стокхолмската програма (и нейния план за действие), които подчертават в глава 4.1 необходимостта от цялостна СВС, основана на зачитането на основните права, международната закрила и принципите на правовата държава. Освен това съгласно Стокхолмската програма, разработването, наблюдението и изпълнението на стратегия за вътрешна сигурност следва да стане една от приоритетните задачи Постоянния комитет за вътрешна сигурност (COSI), създаден в съответствие с член 71 от Договора за функционирането на Европейския съюз (ДФЕС). С цел да гарантира ефективното изпълнение на СВС, тя обхваща също аспектите на сигурността на интегрираното управление на границите и, когато е уместно, на съдебното сътрудничество по наказателноправни въпроси, имащи отношение към оперативното сътрудничество в областта на вътрешната сигурност. Важно е също да се отбележи в този контекст, че Стокхолмската програма призовава за интегриран подход към СВС, който следва да взема предвид също така стратегията за външна сигурност, разработена от ЕС, както и останалите политики на ЕС, по-специално онези, които се отнасят до вътрешния пазар.

Цел на становището

10. Съобщението се отнася до различни области на политиката, които формират част от и въздействат върху широко приеманата концепция за „вътрешна сигурност“ в Европейския съюз.

11. Целта на настоящото становище не е да анализира всички области на политиката и специалните теми, обхванати от съобщението, а да:

— разгледа конкретните цели на СВС, предложени в съобщението, от гледна точка на неприкосновеността на личния живот и защитата на данните, и — от тази гледна точка — да подчертае необходимите връзки с други стратегии, обсъдени и приети на равнище ЕС;

— конкретизира редица виждания и концепции за защита на данните, които следва да бъдат взети предвид при проектирането, разработването и прилагането на СВС на равнище ЕС;

— - предостави, когато е полезно и целесъобразно, предложения за това как да бъдат взети предвид опасенията, свързани със защитата на данните при изпълнението на действията, предложени в съобщението.

12. ЕНОЗД ще извърши това, като подчертае по-специално връзките между СВС и стратегията за управление на информацията и работата по цялостната рамка за защита на данните. Освен това ЕНОЗД ще се позове на концепции като: най-добри налични техники и „защита на личния живот още при проектирането“, оценка на въздействието върху неприкосновеността на личния живот и защитата на данните и правата на субекта на данни, които има пряко въздействие върху проектирането и прилагането на СВС. Становището ще предостави също коментар върху редица избрани области от политиката като интегрирано управление на границите, включително EUROSUR и обработката на лични данни от ФРОНТЕКС, както и други области като киберпространството и програмата за проследяване на финансирането на тероризма (ППФТ).

II. **ОБЩИ КОМЕНТАРИ**

Необходимост от по-всеобхватен, интегриращ и „стратегически“ подход към стратегиите на ЕС, свързани със СВС

13. Понастоящем на равнище ЕС се обсъждат и предлагат различни стратегии на ЕС, основани на Договора от Лисабон и Стокхолмската програма, които имат пряко или непряко въздействие върху защитата на данните. СВС е една от тях и е тясно свързана с други стратегии (разгледани в неотдавнашните съобщения на Комисията или предвидени за близкото бъдеще) като Стратегията за управление на информацията и Европейския модел за обмен на информация, стратегията за прилагане на Хартата на основните права на Европейския съюз, всеобхватната стратегия за защита на данните и политиката на ЕС за борба с тероризма. В настоящото становище ЕНОЗД обръща специално внимание на връзките със Стратегията за управление на информацията и всеобхватната рамка за защита на данните, основана на член 16 от ДФЕС, които имат най-очевидни политически връзки със СВС от гледна точка на защитата на данните.

14. Всички тези стратегии представляват сложна „смесица“ от взаимосвързани насоки на политиката, програми и планове за действие, в които се призовава за всеобхватен и интегриран подход на равнище ЕС.

15. В по-общ план, ако бъде приет в бъдещите действия, този подход на „свързване на стратегиите“ ще покаже, че съществува визия на равнище ЕС, когато става дума за стратегии на ЕС, и че тези стратегии, както и неотдавна приетите съобщения, които ги доразвиват, са тясно взаимосвързани, както е в настоящия случай. Стокхолмската програма е общата референтна точка за всички тях. Той ще доведе също така до положителни взаимодействия между различните политики в областта на свободата, сигурността и правосъдието, и ще се избегне възможно дублиране на работа и усилия в тази област. Също толкова важно е този подход да доведе до по-ефективно и съгласувано прилагане на правилата, свързани със защитата на данните, в контекста на всички взаимосвързани стратегии.

16. ЕНОЗД подчертава, че един от стълбовете на СВС е ефективното управление на информацията в Европейския съюз, което следва да се основава на принципите на необходимостта и пропорционалността, за да обоснове необходимостта от обмен на информация.

17. Освен това, както се отбелязва в становището на ЕНОЗД относно съобщението, свързано с управлението на информацията ([8]), ЕНОЗД подчертава, че всички нови законодателни мерки, които биха улеснили съхранението и обмена на лични данни, следва да бъдат предлагани, само ако се основават на конкретни доказателства за необходимостта от тях ([9]). Това правно изискване следва да се трансформира в активен политически подход при изпълнението на СВС. Необходимостта от всеобхватен подход към СВС неизбежно води към необходимост от оценка на всички инструменти и средства, които вече съществуват в областта на вътрешната сигурност, преди да се предлагат нови.

18. В този контекст ЕНОЗД предлага по-честа употреба също така на клаузи, предвиждащи периодично оценяване на съществуващите инструменти, като включените в директивата за запазване на данни, която в момента е предмет на оценяване. ([10])

Защитата на данните като цел на СВС

19. В съобщението има позоваване на защитата на лични данни в параграфа „Политики за сигурност, основани на общи ценности“, където се отбелязва, че средствата и действията за изпълнението на СВС трябва да се основават на общи ценности, включващи принципите на правовата държава и зачитането на основните права, определени в Хартата на основните права на ЕС. В този контекст то определя, че „В случаите, в които ефикасното правоприлагане в ЕС се улеснява чрез обмен на информация, трябва също така да защитаваме правото на личен живот на физическите лица и основното им право на защита на личните данни.“

20. Приветстваме това изявление. Не може да се счита обаче, че в своята същност то обръща достатъчно внимание на въпроса за защита на данните в СВС. В съобщението не се развива защитата на данните ([11]), нито се обяснява как ще се гарантира на практика зачитането на неприкосновеността на личния живот и защитата на данните при действията за изпълнение на СВС.

([8]) Становище от 30 септември 2010 г. относно Съобщение от Комисията до Европейския парламент и Съвета — „Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието.“

([9]) Това е правно изискване; вж. по-специално решение на Съда на Европейския съюз по съединени дела C-92/09 и C-93/09 от 2 ноември 2010 г. В по-конкретен контекст ЕНОЗД също така защитава този подход в други становища относно законодателни решения, свързани с областта на свободата, сигурността и правосъдието: напр. Становище от 19 октомври 2005 г. по три предложения относно второ поколение Шенгенска информационна система (ШИС II); Становище от 20 декември 2007 г. по проекта за предложение за рамково решение на Съвета относно използване на резервационни данни на пътниците (PNR — Passenger Name Record) за целите на правоприлагането; Становище от 18 февруари 2009 г. по предложението за регламент за създаване на система „ЕВРОДАК“ за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕО) № […/…] [за установяване на критерии и механизми за определяне на държава-членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите-членки от гражданин на трета страна или лице без гражданство]; Становище от 18 февруари 2009 г. относно предложението за регламент за установяване на критерии и механизми за определяне на държава-членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите-членки от гражданин на трета страна или лице без гражданство; и Становище от 7 октомври 2009 г. относно предложенията, свързани с достъпа на правоприлагащите органи до Евродак.

([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.

([11]) Защитата на данни се посочва единствено и по-конкретно в контекста на въпроса за обработката на лични данни от ФРОНТЕКС.

21. Според ЕНОЗД една от целите на *Стратегията за вътрешна сигурност в действие* следва да бъде широкото приемане на *защитата*, което следва да гарантира *правилния* баланс между , защитата на гражданите срещу съществуващите заплахи от една страна и защитата на неприкосновеността на личния живот и правото на защита на личните данни от друга. С други думи опасенията, свързани със сигурността и неприкосновеността на личния живот, трябва да се вземат предвид също така сериозно при разработването на СВС, което ще бъде в съответствие със Стокхолмската програма и заключенията на Съвета.

22. Накратко, гарантирането на сигурност при пълно зачитане на неприкосновеността на личния живот и защитата на данните следва да се посочи като конкретна цел на Стратегията за вътрешна сигурност на ЕС. Това следва да се отрази във всички действия, предприети от държавите-членки и институциите на ЕС за изпълнение на стратегията.

23. В този контекст ЕНОЗД се позовава на Съобщение (2010) 609 относно всеобхватен подход за защита на личните данни в Европейския съюз. ([12]) ЕНОЗД скоро ще публикува становище относно това съобщение, но подчертава тук, че не може да се прилага ефективна СВС без подкрепата на солидна схема за защита на данните, която да я допълва и да осигурява взаимно доверие и по-голяма ефективност.

III. ВИЖДАНИЯ И КОНЦЕПЦИИ, ПРИЛОЖИМИ КЪМ ПРОЕКТИРАНЕТО И ИЗПЪЛНЕНИЕТО НА СВС

24. Ясно е, че някои от действията, които произтичат от целите на СВС, могат да увеличат рисковете за неприкосновеността на личния живот и защитата на данните на физическите лица. За да се неутрализират тези рискове, ЕНОЗД би искал да обърне по-специално внимание на концепции като („защита на личния живот още при проектирането“, оценка на въздействието върху неприкосновеността на личния живот и защитата на данните, права на субектите на данни и най-добри налични техники. Всички те следва да се вземат предвид при изпълнението на СВС и могат да допринесат за политики, съобразени в по-голяма степен с неприкосновеността на личния живот и защитата на данните в тази област.

Защита на личния живот още при проектирането

25. ЕНОЗД е защитавал при различни случаи в различни становища концепцията за „заложената“ неприкосновеност на личния живот („защита на личния живот още при проектирането“ или „защита на личния живот по подразбиране“). Понастоящем тази концепция се разработва както за частния, така и за публичния сектор като цяло, и поради това изпълнява също важна роля в контекста на вътрешната сигурност на ЕС и в областта на полицейското и съдебното сътрудничество. ([13])

26. В съобщението тази концепция не се споменава. ЕНОЗД предлага тази концепция да бъде посочена в целевите действия, които трябва да бъдат предложени и предприети за изпълнението на СВС, по-специално в контекста на цел 4 „укрепване на сигурността чрез управление на границите“, където ясно се посочва по-добро използване на новите технологии за гранични проверки и за наблюдение на границите.

Оценка на въздействието върху неприкосновеността на личния живот и защитата на данните

27. ЕНОЗД насърчава Комисията да обсъди — като част от бъдещата работа по проектиране и изпълнение на СВС въз основа на съобщението — какво следва да означава действителна „оценка на въздействието върху неприкосновеността на личния живот и защитата на данните“ (PIA) в областта на свободата, сигурността и правосъдието, и по-специално в СВС.

28. В съобщението се прави позоваване на оценките на заплахата и на риска. Ние приветстваме това. В него обаче — в нито една точка — няма позоваване на оценките на въздействието върху неприкосновеността на личния живот и защитата на данните. ЕНОЗД вярва, че дейността по прилагане на съобщението относно СВС предоставя добра възможност да се разработят такива оценки на въздействието върху неприкосновеността на личния живот и защитата на данните в контекста на вътрешната сигурност. ЕНОЗД отбелязва, че този аспект не е посочен, нито развит както в съобщението, така и в насоките на Комисията за оценка на въздействието ([14]).

29. Поради това ЕНОЗД препоръчва при прилагането на бъдещите инструменти Комисията да провежда по-специфична и строга оценка на въздействието върху неприкосновеността на личния живот и защитата на данните или като отделна оценка, или като част от общата оценка на въздействието върху основните права. Тази оценка на въздействието следва не само да определя общите принципи или да анализира възможностите на политиките, както в настоящия случай, но трябва също така да препоръчва специални и конкретни предпазни мерки.

30. Следователно трябва да бъдат разработени конкретни показатели и характеристики, за да се гарантира, че всяко предложение, което има въздействие върху неприкосновеността на личния живот и защитата на данните в областта на вътрешната сигурност на ЕС, се разглежда задълбочено, включително аспекти като принципа на пропорционалност, принципа на необходимост и принципа на ограничаване на целта.

31. Освен това в този контекст би могло да бъде полезно позоваването на член 4 от Препоръката относно съобщението за радиочестотната идентификация (RFID) ([15]), в която Комисията призовава държавите-членки да гарантират, че в сътрудничество със съответните заинтересовани страни от гражданското общество промишлеността разработва рамка

([12]) Съобщение на Комисията до Европейския парламент, Съвета, Икономическия и социален комитет и Комитета на регионите „Всеобхватен подход за защита на личните данни в Европейския съюз“, COM (2010) 693.

([13]) В становището на ЕНОЗД относно Съобщението на Комисията относно Стокхолмската програма се препоръчва правно задължение създателите и потребителите на информационни системи да използват системи, които са в съответствие с принципа „защита на личния живот още при проектирането.“

([14]) SEC(2009) 92, 15.1.2009 г.

([15]) C(2009) 3200 окончателен, 12.5.2009 г.

за оценки на въздействието върху неприкосновеността на личния живот и защитата на данните. Освен това резолюцията от Мадрид, приета през ноември 2009 г. от Международната конференция на комисарите по неприкосновеността на личния живот и защитата на данните, също насърчи прилагането на PIA преди внедряването на нови информационни системи и технологии за обработка на лични данни или въвеждането на съществени изменения в съществуващите такива.

Права на субектите на данни

32. ЕНОЗД отбелязва, че в съобщението не разглежда специално важният въпрос за правата на субектите на данни, които представляват съществен елемент от защитата на данни и следва да имат въздействие върху проектирането на СВС. От особена важност е да се гарантира, че лицата се ползват с едни и същи права във всички различни системи и инструменти за вътрешна сигурност на ЕС, свързани с начина на обработване на техните лични данни.

33. Много от посочените в съобщението системи създават специфични правила по отношение на правата на субектите на данни (сред които също така категории лица като жертви, предполагаеми престъпници или мигранти), но съществуват значителни различия между системите и инструментите, за което липсва основание.

34. Поради това ЕНОЗД приканва Комисията в близко бъдеще да разгледа по-внимателно въпроса за съгласуването на правата на субектите на данни в ЕС в контекста на СВС и стратегията за управление на информацията.

35. Специално внимание следва да се обърне на механизмите за правна защита. СВС следва да гарантира, че когато правата на физическите лица не се зачитат напълно, администраторите на данните следва да предвидят процедури за оплаквания, които са ефективни и лесно достъпни на практика и във финансово отношение.

Най-добри налични техники

36. При изпълнението на СВС неизбежно се използва като база инфраструктурата на информационните системи, която ще подкрепя действията, предвидени в съобщението. Най-добрите налични техники могат да се разглеждат като средства, осигуряващи правилен баланс между постигането на целите на СВС и зачитането на правата на физическите лица. В настоящия контекст ЕНОЗД би желал да повтори препоръката, направена в предишни становища ([16]) относно необходимостта Комисията да определя и насърчава в сътрудничество със съответните заинтересовани страни от промишлеността конкретни мерки за прилагане на най-добрите налични техники. Такова прилагане означава най-ефективният и напредналият етап в развитието на дейностите и методите за тяхното осъществяване, показващ практическата пригодност на съответните техники за осигуряване на предвидените резултати по ефективен начин и в съответствие с рамката на ЕС относно неприкосновеността на личния живот и защитата на данните. Този подход е напълно съгласуван с вече посочения подход „защита на личния живот още при проектирането“.

37. Когато е приложимо и изпълнимо, следва да бъдат разработени референтните документи относно най-добрите налични техники, за да се осигурят насоки и по-голяма правна сигурност по отношение на действителното изпълнение на мерките, предвидени в рамката на СВС. Това би могло да насърчи хармонизирането на такива мерки в различните държави-членки. И не на последно място, определянето на най-добри налични техники, защитаващи неприкосновеността на личния живот и сигурността, ще улесни надзорната роля на органите по защита на данните, като им осигури технически референции, които са в съответствие с неприкосновеността на личния живот и защитата на данните, приети от администраторите на данни.

38. ЕНОЗД отбелязва също така важността на правилното съгласуване на СВС с дейностите, които вече се осъществяват по седмата рамкова програма за научни изследвания и технологично развитие и рамковата програма „Сигурност и опазване на свободите“. Съвместна визия, чиято цел е да осигури най-добри налични техники, ще позволи иновации в знанията и възможностите, необходими за защита на гражданите, като същевременно се зачитат основните права.

39. Накрая, ЕНОЗД посочва ролята, която Европейската агенция за мрежова и информационна сигурност (ENISA) може да изпълнява при разработването на насоки и при оценката на възможностите за сигурност, които са необходими, за да се гарантира целостта и наличността на информационните системи, както и при насърчаването на тези най-добри налични техники. В тази връзка ЕНОЗД приветства включването на агенцията като основен участник в подобряването на възможностите за справяне с кибератаки и борбата срещу престъпленията в кибернетичното пространство. ([17])

Пояснение относно действащите лица и техните роли

40. В този контекст е необходимо допълнително пояснение относно действащите лица, които са част от или допринасят за архитектурата на СВС. В съобщението се посочват различни действащи лица и заинтересовани страни като

([16]) Становище на ЕНОЗД относно интелигентните транспортни системи, от юли 2009 г., и Становище на ЕНОЗД относно съобщението относно радиочестотната идентификация (RFID) от декември 2007 г., вж. също Годишен доклад на ЕНОЗД за 2006 г., стр. 48—49.

([17]) ЕНОЗД предвижда приемане на становище относно правната рамка на ENISA още през декември 2010 г.

граждани, съдебна система, агенции на ЕС, национални органи, полиция и предприятия. Следва да се обърне по-голямо внимание на специфичните роли и компетентностите на тези действащи лица в специфичните действия, които трябва да бъдат предложени с цел изпълнение на СВС.

IV. СПЕЦИФИЧНИ КОМЕНТАРИ ОТНОСНО ОБЛАСТИТЕ НА ПОЛИТИКАТА, СВЪРЗАНИ СЪС СВС

Интегрирано управление на границите (ИУГ)

41. В съобщението има позоваване на факта, че Договорът от Лисабон осигурява на ЕС по-добри възможности да използва взаимодействията между политиките за управление на границите, свързани с лицата и стоките. По отношение на движението на лица в него се посочва, че „ЕС може да разглежда управлението на миграцията и борбата с престъпността като една двойна цел на стратегията за интегрирано управление на границите“. В документа се разглежда управлението на границите като потенциален мощен инструмент за борба с тежката и организираната престъпност. ([18])

42. ЕНОЗД отбелязва също, че съобщението определя три стратегически направления: 1) по-добро използване на новите технологии за гранични проверки (ШИС II, ВИС, системата за влизане/излизане и програмата за регистриране на пътниците); 2) по-добро използване на новите технологии за наблюдение на границите (Европейската система за наблюдение на границите — EUROSUR) и 3) по-добра координация на държавите-членки посредством Фронтекс.

43. ЕНОЗД се стреми да се възползва от възможността чрез настоящото становище да припомни своите искания, отправени в редица предишни становища, да се установи ясна политика на управление на границите с цялостно спазване на правилата относно защитата на данните на равнище ЕС. ЕНОЗД вярва, че настоящата работа по СВС и управлението на информацията създава добри възможности да се предприемат повече конкретни стъпки към съгласуван подход в политиката към тези области.

44. ЕНОЗД отбелязва, че в съобщението има позоваване не само на съществуващите широкомащабни системи и онези, чиято употреба може да започне в близкото бъдеще (като ШИС, ШИС II и ВИС), но — по същия начин — също на системите, които биха могли да бъдат предложени от Комисията в бъдеще, относно които обаче все още не е взето решение (т.е. програмата за регистриране на пътниците (RTP) и системата за влизане/излизане). В този контекст следва да се припомни, че все още трябва да бъдат изяснени и демонстрирани целите и правното основание за въвеждане на тези системи, също така и с оглед на резултатите и специфичните оценки на въздействието, извършвани от Комисията. Ако това не се случи, съобщението може да се тълкува като предвиждащо процеса на вземане на решение и следователно не взема предвид факта, че все още не е взето окончателното решение дали RTP и системата за влизане/излизане следва да бъдат въведени в Европейския съюз.

45. Поради това ЕНОЗД предлага да се избягват такива предвиждания в бъдещата работа по изпълнението на СВС. Както бе отбелязано по-рано, всяко решение относно въвеждането на нови широкомащабни системи, нарушаващи неприкосновеността на личния живот, трябва да се осъществява единствено след адекватна оценка на всички реализирани и съществуващи системи, като се вземат предвид необходимостта и пропорционалността.

EUROSUR

46. В съобщението се посочва, че Комисията ще представи законодателно предложение за създаване на EUROSUR през 2011 г. с цел да се допринесе за вътрешната сигурност и борбата с престъпността. Посочва се също, че EUROSUR ще използва нови технологии, разработени чрез финансирани от ЕС изследователски проекти и дейности, като сателитни изображения за откриване и проследяване на цели по морските граници, например проследяване на бързи плавателни съдове, превозващи наркотици към ЕС.

47. В този контекст ЕНОЗД отбелязва, че не е ясно, дали и ако това е така, в каква степен законодателно предложение за създаване на EUROSUR, което трябва да се представи от Комисията през 2011 г. ще предвижда също обработване на лични данни в контекста на EUROSUR. Комисията все още не е заела ясна позиция по този въпрос в съобщението. Той е дори още по-значим предвид факта, че в съобщението се прави ясна връзка между EUROSUR и ФРОНТЕКС на тактическо, оперативно и стратегическо ниво (вж. коментарите относно ФРОНТЕКС по-долу) и се търси тясно сътрудничество между двете.

Обработка на лични данни от ФРОНТЕКС

48. ЕНОЗД е издал становище относно преразглеждането на регламента за ФРОНТЕКС от 17 май 2010 г. ([19]), в което той призова за истински дебат и задълбочено разглеждане на въпроса за защита на данните в контекста на укрепването на съществуващите функции на ФРОНТЕКС и възлагането на нови отговорности на агенцията.

49. В съобщението има позоваване на необходимостта да се увеличи приноса на ФРОНТЕКС по външните граници съгласно цел 4 *Укрепване на сигурността чрез управление на границите*. В този контекст в съобщението се посочва, че въз основа на опита и в контекста на общия подход на ЕС спрямо управлението на информацията, Комисията смята, че предоставянето на Фронтекс на правомощия да обработва и

([18]) Съобщение за пресата относно Стратегията за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа, Memo 10/598.

([19]) Становище на ЕНОЗД от 17 май 2010 г. относно предложението за регламент на Европейския парламент и на Съвета за изменение на Регламент (ЕО) № 2007/2004 за създаване на Европейска агенция за управление на оперативното сътрудничество по външните граници на държавите-членки на Европейския съюз (FRONTEX).

използва тази информация в ограничени рамки и в съответствие с ясно определени правила за управление на личните данни ще допринесе значително за разбиване на престъпните организации. Това е нов подход в сравнение с предложението на Комисията за преразглеждане на регламента за ФРОНТЕКС, който понастоящем се обсъжда в Европейския парламент и в Съвета, който не засяга обработката на лични данни.

50. В този контекст ЕНОЗД приветства факта, че съобщението предвижда някакво указание относно обстоятелствата, при които такава обработка може да се окаже необходима (напр. анализ на риска, по-добра ефективност на съвместните операции или на обмена на информация с Европол). По-конкретно в съобщението се разяснява, че понастоящем информацията за престъпници, участващи в мрежи за трафик — която ФРОНТЕКС получава — не може да се използва допълнително за анализ на риска или за по-добро насочване на бъдещи съвместни операции. Освен това съответните данни за предполагаеми престъпници не достигат до компетентните национални органи или Европол за по-нататъшно разследване.

51. Независимо от това ЕНОЗД отбелязва, че в съобщението няма позоваване на текущото обсъждане на преразглеждането на правната рамка на ФРОНТЕКС, което, както бе отбелязано по-рано, разглежда този въпрос с цел да предостави законодателни решения. Освен това формулировката на съобщението, която подчертава ролята на ФРОНТЕКС в контекста за разбиване на престъпни организации, може да се разбира като разширяваща мандата на ФРОНТЕКС. ЕНОЗД предлага тази точка да се вземе предвид както при преразглеждането на регламента за ФРОНТЕКС, така и при изпълнението на СВС.

52. ЕНОЗД обръща внимание също така на необходимостта да се гарантира, че не съществува дублиране на функции между Европол и ФРОНТЕКС. В този контекст ЕНОЗД приветства факта, че в съобщението се отбелязва, че това дублиране на функции между ФРОНТЕКС и Европол трябва да се избягва. Този въпрос обаче следва по-ясно да бъде разгледан както в преразгледания регламент за ФРОНТЕКС, така и в действията за изпълнение на СВС, които предвиждат тясно сътрудничество между ФРОНТЕКС и ЕВРОПОЛ. Това е особено важно от гледна точка на принципите за ограничаване на целта и качеството на данните. Тази забележка се отнася също за бъдещото сътрудничество с такива агенции като Европейската агенция за мрежова и информационна сигурност (ENISA) или Европейската служба за подкрепа в областта на убежището.

Използване на биометрични данни

53. Съобщението не разглежда конкретно настоящото явление, свързано с увеличеното използване на биометрични данни в областта на свободата, сигурността и правосъдието, както и на широкомащабните информационни системи и други инструменти за управление на границите.

54. Поради това ЕНОЗД се възползва от тази възможност, за да припомни своето твърдение ([20]), че този въпрос с висока чувствителност от гледна точка на защитата на данните се взема под сериозно внимание при изпълнението на СВС, по-специално в контекста на управлението на границите.

55. ЕНОЗД препоръчва също така разработване на ясна и строга политика относно използването на биометрични данни в областта на свободата, сигурността и правосъдието въз основа на сериозна оценка и на оценка за всеки отделен случай на необходимостта от използване на биометрични данни в контекста на СВС, като се спазват изцяло такива основни принципи за защита на данните като принципа на пропорционалност, принципа на необходимост и принципа на ограничаване на целта.

Програма за проследяване на финансирането на тероризма (ППФТ)

56. В съобщението се обявява, че през 2011 г. Комисията ще разработи политика на ЕС за извличане и анализ на данни за финансови съобщения, които се съхраняват на територията на Съюза. В този контекст ЕНОЗД се позовава на своето становище от 22 юни 2010 г. относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма (ППФТ II) ([21]). Всички критични забележки, изразени в това становище, са също толкова валидни и приложими в контекста на предвидената работа по рамката на ЕС за данните за финансови съобщения. Поради това те следва да бъдат взети предвид при обсъждането на този въпрос. Специално внимание следва да се обърне на пропорционалността при извличането и обработката на големи количества данни за лица, които не са заподозрени, както и на въпроса за ефективността на надзора от страна на независимите и съдебните органи.

Сигурност за гражданите и предприятията в киберпространството

57. ЕНОЗД приветства значимостта, отдадена в съобщението на превантивните действия на равнище ЕС, и счита, че укрепването на сигурността в информационните мрежи е съществен фактор, допринасящ за правилното функциониране на информационното общество. Също така ЕНОЗД подкрепя специфичните дейности, които подобряват капацитета за справяне с кибератаките, изграждат капацитет в областта на правоприлагането и съдебните органи и създават партньорства с промишлеността, за да предоставят правомощия на гражданите и предприятията. Също така се приветства ролята на ENISA като сътрудник по много от действията, предвидени в тази цел.

([20]) Вж. по-специално становище на ЕНОЗД относно съобщението относно прегледа на управлението на информацията в областта на свободата, сигурността и правосъдието, отбелязано в бележка под линия 8.

([21]) Становище на Европейския надзорен орган по защита на данните от 22 юни 2010 г. относно предложение за решение на Съвета относно сключването на Споразумението между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма (ППФТ II).

58. В *Стратегията за вътрешна сигурност в действие* обаче не се разработват дейностите по правоприлагане, предвидени в киберпространството, нито как тези дейности могат да създадат рискове за правата на физическите лица и какви следва да бъдат предпазните мерки. ЕНОЗД призовава за по-амбициозен подход към подходящите гаранции; този подход следва да защитава основните права на всички физически лица, включително на онези, които могат да бъдат засегнати от действията, предназначени да противодействат на възможните престъпни дейности в тази област.

V. **ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ**

59. ЕНОЗД призовава за свързване на различните стратегии на ЕС и съобщенията в процеса на изпълнение на СВС. Този подход следва да бъде последван от конкретен план за действие, подкрепен от действителна оценка на нуждите, резултатът от която следва да бъде всеобхватна, интегрирана и добре структурирана политика на ЕС за СВС.

60. ЕНОЗД също така се възползва от тази възможност, за да подчертае значението на правното изискване за действителна оценка на всички съществуващи инструменти, които ще се използват в контекста на СВС и за обмен на информация, преди да бъдат предлагани нови. В този контекст е силно препоръчително включването на разпоредбите, изискващи редовни оценки на ефективността на съответните инструменти.

61. ЕНОЗД предлага при подготовката на многогодишния стратегически план, изискван от заключенията на Съвета от ноември 2010 г. да се вземе предвид текущата работа по всеобхватната рамка за защита на данните въз основа на член 16 от ДФЕС, по-специално Съобщение (2009) 609.

62. ЕНОЗД прави редица предложения по отношение на виждания и концепциите, приложими от гледна точка на защитата на данните, които следва да се вземат предвид в областта на СВС, като защита на личния живот още при проектирането, оценка на въздействието върху неприкосновеността на личния живот и защитата на данните, най-добри налични техники.

63. ЕНОЗД препоръчва при прилагането на бъдещите инструменти Комисията да провежда оценка на въздействието върху неприкосновеността на личния живот и защитата на данните или като отделна оценка, или като част от общата оценка на въздействието върху основните права.

64. Той също така приканва Комисията да разработи по-съгласувана и последователна политика относно предварителните условия за използване на биометрични данни в областта на СВС и по-голямо съгласуване на равнище ЕС по отношение правата на субектите на данни.

65. ЕНОЗД накрая прави редица коментари относно обработването на лични данни в контекста на управлението на границите и по-специално от страна на ФРОНТЕКС и по възможност в контекста на EUROSUR.

Съставено в Брюксел на 17 декември 2010 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните