I

(Резолюции, препоръки и становища)

СТАНОВИЩА

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ЗА ЗАЩИТА НА ДАННИТЕ

Становище на Европейския надзорен орган по защита на данните 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

(2009/C 128/01)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

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

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

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

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 НАСТОЯЩОТО СТАНОВИЩЕ

I. ВЪВЕДЕНИЕ — КОНТЕКСТ НА СТАНОВИЩЕТО

1. На 28 май 2008 г. председателството на Съвета на Европейския съюз обяви пред Корепер, че с оглед на срещата на върха на ЕС на 12 юни 2008 г. контактната група на високо равнище ЕС—САЩ относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни, е завършила своя доклад. Докладът бе оповестен на 26 юни 2008 г. ([1])

2. В него се определят общи принципи за защита на неприкосновеността на личния живот и личните данни като първа стъпка към обмен на информация със Съединените щати за целите на борбата с тероризма и тежката транснационална престъпност.

3. При оповестяването на доклада председателството на Съвета заяви, че би приветствало всяка идея за последващи действия по доклада и по-конкретно реакции на направените в доклада препоръки за бъдещи действия. С настоящото становище, основаващо се на публично обявеното актуално положение и без да се засягат други допълнителни позиции, които би могъл да изрази в хода на развитието на дискусията по този въпрос, ЕНОЗД се отзовава на тази покана.

4. ЕНОЗД отбелязва, че работата на контактната група на високо равнище (КГВР) се осъществява, особено след 11 септември 2001 г., в обстановка на развитие на обмена на данни между ЕС и САЩ, посредством международни споразумения или други видове правни инструменти. Сред тях са споразуменията на Европол и Евроюст със САЩ, както и споразуменията за резервационните данни на пътниците и случаят Swift, които доведоха до размяна на писма между длъжностни лица от ЕС и САЩ за установяване на минимални гаранции за защита на данните ([2]).

([1]) Документ на Съвета № 9831/08, достъпен на: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Споразумение между Съединените американски щати и Европейската полицейска служба от 6 декември 2001 г., и Допълнително споразумение между Европол и САЩ относно обмена на лични данни и свързана информация, публикувано на уебсайта на Европол;
— Споразумение между Съединените американски щати и Евроюст относно съдебното сътрудничество, 6 ноември 2006 г., публикувано на уебсайта на Евроюст;
— Споразумение между Европейския съюз и Съединените американски щати относно обработка и предаване на резервационни данни на пътниците от въздушни превозвачи на Министерството на вътрешната сигурност (DHS) на Съединените щати (Споразумение относно резервационни данни на пътниците от 2007 г.), подписано в Брюксел, 23 юли 2007 г. и Вашингтон, 26 юли 2007 г., ОВ L 204, 4.8.2007 г., стр. 18.
— Размяна на писма между органите на САЩ и ЕС относно програмата за проследяване на финасирането на тероризма, 28 юни 2007 г.

5. Освен това ЕС води преговори и договаря подобни инструменти, които предвиждат обмяна на лични данни с други трети държави. Такъв скорошен пример е Споразумението между Европейския съюз и Австралия относно обработката и предаването на произхождащи от Европейския съюз резервационни данни за пътниците (PNR данни) от въздушни превозвачи на Австралийската митническа служба ([3]).

6. От този контекст става ясно, че исканията на правоприлагащите органи на трети държави за лична информация непрекъснато се разширяват по обем, както и че те обхващат не само традиционни правителствени бази данни, но и други видове досиета, по-специално досиета, съдържащи данни, събирани от частния сектор.

7. Като важен елемент ЕНОЗД припомня също, че въпросът за предаването на лични данни на трети държави в рамките на полицейското и съдебно сътрудничество по наказателноправни въпроси е разгледан в Рамковото решение на Съвета относно защитата на личните данни, обработвани в рамките на полицейско и съдебно сътрудничество по наказателноправни въпроси, което вероятно ще бъде прието преди края на 2008 г. ([4])

8. Може само да се очаква този трансатлантически обмен на информация да нараства и да засегне и допълнителни сектори, в които се обработват лични данни. В този контекст диалогът относно „трансатлантическото правоприлагане“ се приветства, но същевременно е и чувствителен въпрос. Приветства се, тъй като би могъл да предостави по-ясна рамка за обмена на данни, който се осъществява или предстои да се осъществи. Чувствителен въпрос е, тъй като подобна рамка би узаконила значително по обем предаване на данни в областта на правоприлагането — област, в която въздействието върху лицата е особено силно, а стриктните и надеждни предпазни клаузи и гаранции са още по-необходими ([5]).

9. В следващата глава от настоящото становище ще бъде разгледано актуалното положение и възможните бъдещи действия. В глава III ще бъдат разгледани обхватът и естеството на инструмента, които биха позволили обмен на информация. В глава IV на становището ще бъдат анализирани в генерален план правните въпроси, свързани със съдържанието на евентуално споразумение. Ще бъдат разгледани условията за оценка на нивото на защита, предвидено в Съединените щати, и ще бъде обсъден въпросът за използването на регулаторната рамка на ЕС като критерий за оценка на това ниво на защита. В тази глава ще бъдат изброени и основните изисквания, които трябва да бъдат включени в такова споразумение. Накрая, в глава V на становището ще бъде направен анализ на принципите на неприкосновеността на личния живот, приложени към доклада.

([3]) ОВ L 213, 8.8.2008 г., стр. 49.

([4]) Рамково решение на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, редакция от 24 юни 2008 г., достъпна на http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) По отношение на необходимостта от ясна правна рамка, вж. глави III и IV от настоящото становище.

II. **Актуално състояние и възможни бъдещи действия**

10. ЕНОЗД оценява актуалното положение по следния начин. Постигнат е известен напредък при определянето на общи стандарти относно обмена на информация и защитата на неприкосновеността на личния живот и личните данни.

11. Същевременно все още не е приключила подготовката за каквото и да било споразумение между ЕС и САЩ. Необходима е допълнителна работа. В самия доклад на КГВР се посочват редица нерешени въпроси, най-важен сред които е този за „правната защита“. Продължават разногласията по въпроса за необходимия обхват на съдебната защита ([6]). Други пет нерешени въпроса са посочени в глава 3 от доклада. От настоящото становище става ясно, че много други въпроси остават нерешени, например въпросът за обхвата и естеството на един евентуален инструмент за обмен на информация.

12. Тъй като предпочитаният в доклада вариант е обвързващо споразумение — предпочитание, което ЕНОЗД споделя — предпазливият подход става още по-необходим. Преди да бъде постигнато споразумение, е необходима допълнителна и задълбочена подготовка.

13. Накрая, според ЕНОЗД, би било най-добре сключването на споразумение да се осъществи в рамките на Договора от Лисабон, в зависимост, разбира се, от влизането му в сила. Действително, в рамките на Договора от Лисабон не би възникнала правна несигурност относно разделителните линии между стълбовете на ЕС. Освен това ще бъде гарантирано пълноценното участие на Европейския парламент, както и съдебният контрол от страна на Съда на ЕО.

14. При тези обстоятелства, най-добрият начин за действие би бил разработването на пътна карта за постигане на евентуално споразумение на по-късен етап. Една такава пътна карта би могла да включва следните елементи:

— Насоки за продължаване на работата на КГВР (или на друга група), както и времеви график.

— На един ранен етап, дискусия и евентуално споразумение по основните въпроси като обхват и естество на споразумението.

— Въз основа на общо разбиране на тези основни въпроси, по-нататъшно доразвиване на принципите за защита на данните.

— Участие на заинтересованите страни на различни етапи от процедурата.

— От европейска страна, разглеждане на въпроса за институционалните ограничения.

([6]) Страница 5 от доклада, B.

III. **ОБХВАТ И ЕСТЕСТВО НА ИНСТРУМЕНТА ЗА ОБМЕН НА ИНФОРМАЦИЯ**

15. Според ЕНОЗД от решаващо значение е обхватът и естеството на един евентуален инструмент, включително принципите за защита на личните данни, да бъдат ясно определени, като първа стъпка от по-нататъшното разработване на този инструмент.

16. По отношение на обхвата важни въпроси, на които предстои да бъде намерен отговор, са:

— кои са участващите страни в рамките на и извън областта на правоприлагане,

— какво се има предвид под „цел на правоприлагането“ и връзката между тази цел и други цели като национална сигурност и по-конкретно граничен контрол и обществено здравеопазване,

— как инструментът би се вписал в перспективата за глобална трансатлантическа зона за сигурност.

17. В определението на естеството следва да бъдат изяснени следните въпроси:

— ако има отношение, в рамките на кой стълб ще бъде договарян инструментът,

— дали инструментът ще бъде обвързващ за ЕС и САЩ,

— дали ще има пряк ефект, т.е. да съдържа права и задължения за лицата, които могат да бъдат прилагани пред съдебен орган,

— дали самият инструмент ще позволява обмен на информация или ще установи минимален стандарт за обмен на информация, който да бъде допълван от специфични споразумения,

— по какъв начин инструментът ще бъде свързан със съществуващите инструменти: дали ще бъде съобразен с тях, дали ще ги замени или допълни?

III.1. **Обхват на инструмента**

Участващи страни

18. Въпреки че в доклада на КГВР не се посочва ясно точният обхват на бъдещия инструмент, съдържащите се в него принципи дават възможност да се заключи, че инструментът предвижда да обхване предаване, извършвано както между частни страни и публични органи ([7]), така и между публични органи.

— Между частни страни и публични органи:

19. ЕНОЗД вижда логика в това един бъдещ инструмент да бъде приложим и за предаване, осъществявано между частни страни и публични органи. Разработването на такъв инструмент се осъществява на фона на постъпващи през последните години искания от страна на САЩ за информация от частни страни. Действително ЕНОЗД отбелязва, че частните страни все повече се превръщат в системен източник на информация от гледна точка на правоприлагането, както на равнище ЕС, така и на международно ниво ([8]). Случаят SWIFT установи важен прецедент, при който към частна компания бе отправено искане за системно предаване на данни под формата на информационни масиви до правоприлагащите органи на трета държава ([9]). Същата логика следва събирането на резервационни данни на пътниците от авиокомпаниите. В становището си по проекта за рамково решение за европейска система за резервационни данни на пътниците ЕНОЗД вече постави под въпрос легитимността на тази тенденция ([10]).

20. Съществуват още две причини за колебание по отношение на включването на предаване между частни страни и публични органи в обхвата на бъдещия инструмент.

21. На първо място, такова включване би могло да произведе нежелан ефект на територията на самия ЕС. ЕНОЗД храни сериозни опасения, че ако данните на частни компании (например финансови институции) могат по принцип да бъдат предавани на трети държави, това би могло да доведе до силен натиск същият тип данни да бъдат еднакво налични и за правоприлагащите органи в рамките на ЕС. Схемата за резервационните данни на пътниците е пример за такова нежелателно развитие, което започна със събиране на информационни масиви от данни на пътниците от страна на САЩ, за да се транспонира след това и във вътрешния европейски контекст ([11]), без необходимостта и пропорционалността на системата да са били ясно демонстрирани.

22. На второ място, в становището си по предложението на Комисията относно ЕС и резервационните данни на пътниците ЕНОЗД постави и въпроса за рамката на

([7]) Вж. по-специално глава 3 от доклада, „Нерешени въпроси, свързани с трансатлантическите отношения“, точка 1: „Последователност в задълженията на частните структури при предаване на данни“.

([8]) Вж. по този въпрос Становището на ЕНОЗД от 20 декември 2007 г. относно предложението за Рамково решение на Съвета за използването на резервационните данни на пътниците за целите на правоприлагането, ОВ C 110, 1.5.2008 г., стр. 1. „По традиция между правоприлагането и дейностите на частния сектор съществува ясно разграничение, при което задачите по правоприлагането се изпълняват от определени за целта органи, и по-специално полицейски сили, а частни участници се привличат, в зависимост от конкретния случай, за предаване на лични данни на тези правоприлагащи органи. Понастоящем съществува тенденция за налагане на сътрудничество за целите на правоприлагането на частни участници на систематична основа“.

([9]) Вж. становище 10/2006 на работна група „Член 29“, от 22 ноември 2006 г. относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT), WP 128.

([10]) Становище от 20 декември 2007 г. op.cit

([11]) Вж. предложението за Рамково решение на Съвета относно използването на резервационни данни на пътниците (PNR данни) за целите на правоприлагането, посочени в бележка под линия 8, което в момента се обсъжда в Съвета.

защитата на данните (първи или трети стълб), която е приложима към условията на сътрудничеството между публичните органи и частните страни: дали разпоредбите следва да се основават на качеството на контрольора на данните (частния сектор) или на преследваната цел (правоприлагане)? Разделителната линия между първия и третия стълб съвсем не е ясна в ситуации, когато на частни страни се налагат задължения за обработване на лични данни за целите на правоприлагането. В този контекст е особено важно, че в неотдавнашното си становище по делото относно запазването на данни генерален адвокат Bot ([12]) предлага да се установи разделителна линия за такива ситуации, но към предложението си добавя: „Тази разделителна линия определено не е защитена от критики и в някои отношения би могла да изглежда изкуствена.“ Освен това ЕНОЗД отбелязва, че решението на Съда по отношение на резервационните данни на пътниците ([13]) не отговаря напълно на въпроса за приложимата правна рамка. Така например фактът, че някои дейности не са обхванати от Директива 95/46/ЕО не означава автоматично, че тези дейности могат да бъдат регулирани в рамките на третия стълб. В резултат, това вероятно оставя празнота по отношение на приложимото право и във всеки случай води до правна несигурност по отношение на правните гаранции, с които разполагат субектите на данните.

23. От тази гледна точка ЕНОЗД изтъква необходимостта от гаранции, че бъдещият инструмент с общи принципи за защита на данните не може сам по себе си да легитимира трансатлантическо предаване на лични данни между частни страни и публични органи. Такова предаване може да бъде включено в бъдещ инструмент само при условие че:

— бъдещият инструмент предвижда, че предаване е позволено само когато е доказано, че то е абсолютно необходимо за конкретна цел, като решението се взема за всеки отделен случай,

— самото предаване се ползва със засилени гаранции за защита на данните (както е посочено в настоящото становище).

Нещо повече, ЕНОЗД отбелязва несигурността относно приложимата рамка за защита на данните и поради това настоява предаването на лични данни между частни страни и публични органи в никакъв случай да не се включва в правото на ЕС в настоящия му вид.

— Между публични органи:

24. Точният обхват на обмена на информация остава неясен. Като първа стъпка в бъдещата работа по общия инструмент, следва да бъде изяснен предвижданият обхват на един такъв инструмент. По-конкретно остават въпроси относно това дали:

— що се отнася до бази данни в ЕС инструментът би бил насочен към централизирани бази данни, (частично) управлявани от ЕС, като например базите данни на Европол и Евроюст, или децентрализирани бази данни, управлявани от държавите-членки, или и двете,

— обхватът на инструмента се разширява до взаимосвързани мрежи, т.е. дали предвижданите гаранции ще обхванат данните, които се обменят между държавите-членки или агенциите, както в ЕС, така и в САЩ,

— инструментът би обхванал само обмен между бази данни в областта на правоприлагането (полиция, съдебна система, евентуално митнически органи) или също така други бази данни, като например данъчните бази данни,

— инструментът би бил свързан и с бази данни на агенциите за национална сигурност или би позволявал достъп на тези агенции до бази данни по правоприлагането на територията на другата договаряща страна (ЕС към САЩ и обратно),

— инструментът би обхващал предаване на информация за конкретен случай, или постоянен достъп до съществуващи бази данни. Последната хипотеза определено би повдигнала въпроси, свързани с пропорционалността, както е обсъдено по-нататък в глава V, в точка 3.

Цел на правоприлагането

25. Определянето на целта на евентуално споразумение също оставя място за несигурност. Целите на правоприлагането са ясно посочени във въведението, както и в първия принцип, приложен към доклада, и ще бъдат допълнително анализирани в глава IV на настоящото становище. Както ЕНОЗД вече отбелязва, в тези изявления личи, че обменът на данни би се съсредоточил върху въпроси от областта на третия стълб, но би могло да възникне съмнение дали това не е само една първа стъпка към по-широк обмен на информация. Изглежда ясно, че целите на „обществената сигурност“, посочени в доклада, включват борбата с тероризма, организираната престъпност и други престъпления. Дали обаче това има за цел да позволи и обмен на данни за целите на други обществени интереси, като евентуални рискове за общественото здраве?

26. ЕНОЗД препоръчва целта да бъде ограничена до ясно определена обработка на данни и да бъдат аргументирани изборите на политика, довели до такова определяне на целта.

([12]) Становище на генерален адвокат Bot от 14 октомври 2008 г., Ireland v. Европейския парламент и Съвета, (дело C-301/06), параграф 108.

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

Глобална трансатлантическа зона за сигурност

27. Широкият обхват на този доклад следва да бъде разглеждан в контекста на перспективата за глобалната трансатлантическа зона за сигурност, обсъждана от така наречената „Група за бъдещето“ ([14]). Публикуваният през юни 2008 г. доклад на тази група поставя известен акцент върху външното измерение на политиката в областта на вътрешните работи. В него се застъпва становището, че *„до 2014 г. Европейският съюз следва да вземе решение във връзка с политическата цел за установяване на евроатлантическо пространство на сътрудничество със САЩ в областта на свободата, сигурността и правосъдието със САЩ“*. Такова сътрудничество би излязло извън рамките на сигурността в стриктния смисъл на думата и най-малкото би довело до включване на въпросите, регулирани от сегашния дял IV от Договора за ЕО, като имиграция, визи и сътрудничество в областта на убежището и гражданското право. Трябва да се постави въпросът доколко едно споразумение по основните принципи на защита на данните, като посочените в доклада на КГВР, би могло и следва да бъде основа за обмен на информация в такава широка област.

28. При нормални обстоятелства, до 2014 г. стълбовата структура ще престане да съществува и ще има едно правно основание за защита на данните в рамките на самия ЕС (по силата Договора от Лисабон, член 16 от Договора за функционирането на Европейския съюз). Същевременно фактът, че на равнище ЕС съществува хармонизация по отношение на *регулирането* на защитата на данните, не предполага, че всяко споразумение с трета държава може да позволява *предаване* на всякакви лични данни, независимо от целта. В зависимост от контекста и условията на обработка могат да бъдат необходими адаптирани гаранции за защита на данните в специфични области като правоприлагането. ЕНОЗД препоръчва последиците от тези различни перспективи да бъдат отчетени при подготовката на едно бъдещо споразумение.

III.2. **Естество на споразумението**

Европейска институционална рамка

29. Във всички случаи в краткосрочен план е важно да се определи в рамките на кой стълб ще бъдат водени преговорите по споразумението. Това е особено необходимо заради вътрешната регулаторна рамка за защита на данните, която ще бъде засегната от такова споразумение. Ще бъде ли това рамка от областта на първия стълб — основно Директива 95/46/ЕО с нейния специфичен режим за предаване на данни към трети държави — или ще бъде рамка от областта на третия стълб с по-малко строг режим за предаване към трети държави? ([15])

30. Въпреки че, както вече бе споменато, целите на правоприлагането преобладават, в доклада на КГВР все пак се отбелязва събирането на данни от частни структури, а целите могат да бъдат тълкувани и в широк смисъл, който да надхвърли стриктната сигурност, като се включат напр. въпроси на имиграцията и граничния контрол, а евентуално и общественото здраве. С оглед на тази неопределеност, би било силно препоръчително да се изчака хармонизацията на стълбовете по силата на правото на ЕС съгласно предвиденото в Договора от Лисабон, да се установят ясно правното основание за преговорите и конкретната роля на европейските институции, по-специално на Европейския парламент и на Комисията.

Обвързващ характер на инструмента

31. Следва да се изясни дали заключенията от обсъжданията ще доведат до сключване на Меморандум за разбирателство или друг необвързващ инструмент, или до обвързващо международно споразумение.

32. ЕНОЗД подкрепя изразеното в доклада предпочитание за обвързващо споразумение. Според ЕНОЗД едно официално обвързващо споразумение е необходима предпоставка за всяко предаване на данни извън ЕС независимо от целта, за която се предават данните. Предаването на данни към трети държави не може да се осъществява без наличието на адекватни условия и гаранции, включени в конкретна (и обвързваща) правна рамка. С други думи един меморандум за разбирателство или друг необвързващ инструмент може да бъде полезен за предоставяне на насоки за преговори за допълнителни обвързващи споразумения, но в никакъв случай не може да замени необходимостта от обвързващо споразумение.

Пряк ефект

33. Разпоредбите на инструмента следва да бъдат еднакво обвързващи за САЩ и за ЕС и неговите държави-членки.

34. Освен това следва да се гарантира, че лицата имат право да упражняват правата си, и особено да получат правна защита, въз основа на договорените принципи. Според ЕНОЗД този резултат може да бъде постигнат най-добре, ако съществените разпоредби на инструмента са формулирани така, че да произвеждат пряк ефект спрямо гражданите на Европейския съюз и да е възможно позоваване на тях в Съда. Следователно в инструмента трябва ясно да бъден посочен прекият ефект на разпоредбите на международното споразумение, както и условията на неговото транспониране във вътрешното европейско и национално право, за да се гарантира ефективността на мерките.

Връзка с други правни инструменти

35. Друг фундаментален въпрос е степента, в която това споразумение е самостоятелно или трябва да бъде допълвано за всеки конкретен случай от допълнителни споразумения относно специфичен обмен на данни. Действително е спорно дали едно споразумение с един набор от стандарти би могло да обхване по адекватен начин многобройните специфични особености на обработката на данни

([14]) Доклад на неформалната консултативна група на високо равнище относно бъдещето на европейската политика на вътрешни работи „Свобода, сигурност, неприкосновеност — европейски вътрешни работи в един открит свят“ юни 2008 г., достъпен на register.consilium.europa.eu

([15]) Вж. членове 11 и 13 от DPFD, посочена в точка 7 от настоящото становище.

в рамките на третия стълб. Още по-съмнително е дали то би могло да *позволи*, без допълнителни дискусии и гаранции, бланкетно одобрение на всяко предаване на лични данни, независимо от целта и естеството на съответните данни. Освен това споразуменията с трети държави не са задължително постоянни, тъй като могат да бъдат свързани с конкретни заплахи, да бъдат обект на преразглеждане и на клаузи за прекратяване. От друга страна, едни общи минимални стандарти, установени в обвързващ инструмент, биха могли да улеснят всяка допълнителна дискусия по предаването на лични данни във връзка с конкретни бази данни или операции по обработка.

36. Ето защо ЕНОЗД би подкрепил по-скоро разработването на минимален набор от критерии за защита на данните, който да бъде допълван при всеки конкретен случай с допълнителни специфични разпоредби, както е посочено в доклада на КГВР, отколкото алтернативата за самостоятелно споразумение. Тези допълнителни специфични разпоредби са предпоставка, за да се разреши предаването на данни в конкретен случай. По този начин би се насърчил хармонизираният подход по отношение на защитата на данните.

Прилагане на съществуващите инструменти

37. Следва да бъде разгледан и въпросът за това как едно евентуално споразумение от общ характер би се съобразило с вече сключените споразумения между ЕС и САЩ. Следва да се отбележи, че тези съществуващи споразумения нямат същия обвързващ характер: специално следва да бъдат отбелязани споразумението за резервационните данни на пътниците (това, което представя по-добре правната сигурност), споразумението с Европол и Евроюст, или размяната на писма по случая SWIFT ([16]). Дали една нова обща рамка би допълнила тези съществуващи инструменти или те ще останат непроменени, а новата рамка ще се прилага само за друг бъдещ обмен на лични данни? Според ЕНОЗД съображенията за правна последователност налагат хармонизиран набор от правила, приложими и допълващи както съществуващите, така и бъдещи обвързващи инструменти относно предаването на данни.

38. Предимството на прилагането на общо споразумение към съществуващи инструменти би било укрепването на техния обвързващ характер. Това би било особено желателно по отношение на инструменти, които не са правно обвързващи, например размяната на писма по случая SWIFT, тъй като това най-малкото би наложило съответствие с набор от общи принципи за неприкосновеността на личния живот.

IV. **ОБЩА ПРАВНА ОЦЕНКА**

39. В настоящата глава ще бъдат разгледани начините за оценка на нивото на защита на специфична рамка или инструмент, както и въпросът за критериите, които да се използват, и за необходимите основни изисквания.

Адекватно ниво на защита

40. Според ЕНОЗД следва да бъде ясно, че един от основните резултати на бъдещия инструмент би бил, че предаването на лични данни към Съединените щати може да се осъществява само дотолкова, доколкото органите на САЩ гарантират адекватно ниво на защита (и обратно).

41. ЕНОЗД счита, че само една реална проверка за адекватност би осигурила достатъчно гаранции по отношение на нивото на защита на личните данни. Според него едно общо рамково споразумение с обхват, еднакъв с този от доклада на КГВР, трудно би издържало реална проверка за адекватност. Адекватността на генералното споразумение може да бъде призната, само ако бъде съчетана с адекватността на специфични споразумения, сключени за всеки конкретен случай.

42. Оценката на нивото на защита, предоставяно от трети държави, не е необичайна практика, особено за Европейската комисия. в рамките на първия стълб адекватността е изискване за предаване. Тя е оценявана по няколко повода по силата на член 25 от Директива 95/46/ЕО въз основа на специфични критерии, и потвърдена с решения на Европейската комисия ([17]). В рамките на третия стълб такава система не е изрично предвидена: оценка на адекватността на защитата се предвижда само в специфичния контекст на членове 11 и 13 от все още неприетото рамково решение за защита на данните ([18]) и се предоставя на държавите-членки.

43. В настоящия случай обхватът на упражнението засяга целите на правоприлагането, а дискусиите се провеждат от Комисията под наблюдението на Съвета. Този контекст е различен от оценката на принципите на безопасното пристанище или на адекватността на канадското законодателство и е свързан в по-голяма степен с неотдавнашните преговори в областта на резервационните данни на пътниците, проведени със САЩ и Австралия в контекста на правната рамка в областта на третия стълб. Същевременно принципите, определени от КГВР, са споменати и в контекста на Програмата за премахване на визовия режим, която се отнася до границите и имиграцията, и следователно до въпроси от областта на първия стълб.

44. ЕНОЗД препоръчва всяка констатация за адекватност по силата на бъдещия инструмент да доразвива опита в тези

([16]) Виж бележка под линия 2.

([17]) Решения на Комисията относно адекватността на защитата на лични данни в трети държави, включително Аржентина, Канада, Швейцария, Съединените щати, Гърнси, о. Ман и Джърси, са достъпни на http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Ограничено до предаване до трета държава или международен орган от държава-членка на данни, получени от компетентен орган в друга държава-членка.

различни области. ЕНОЗД препоръчва доразвиване на понятието „адекватност“ в контекста на бъдещия инструмент, въз основа на критерии, подобни на тези, използвани при предходно определяне на адекватността.

Взаимно признаване — реципрочност

45. Вторият елемент от нивото на защита се отнася до взаимното признаване на системите на ЕС и САЩ. В това отношение в доклада на КГВР се посочва, че целта следва да бъде „да се получи признание за ефективността на системите за защита на неприкосновеността и данните на всяка от страните в областите, обхванати от тези принципи“ ([19]) и да се постигне „еквивалентно и реципрочно прилагане на правото на защита на неприкосновеността и личните данни“.

46. За ЕНОЗД е очевидно, че взаимното признаване (или реципрочността) е възможно единствено, ако е гарантирано адекватно ниво на защита. С други думи, бъдещият инструмент следва да хармонизира едно минимално ниво на защита (чрез констатиране на адекватност, като отчита необходимостта от специфични споразумения за всеки конкретен случай). Реципрочност би могла да бъде призната, само ако е изпълнено това предварително условие.

47. Първият елемент, който трябва да бъде взет предвид, е реципрочността на съществени разпоредби от областта на защитата на данните. Според ЕНОЗД евентуално споразумение следва да разглежда концепцията за реципрочност на съществени разпоредби за защита на данните по начин, който гарантира от една страна, че обработката на данни в рамките на територията на ЕС (и на САЩ) изцяло зачита разпоредбите на вътрешното право относно защитата на данните, а от друга страна, че обработката извън държавата на произход на данните и попадаща в обхвата на споразумението, зачита принципите на защитата на данните, включени в споразумението.

48. Вторият елемент е реципрочност на механизмите за правна защита. Следва да се гарантира, че европейските граждани разполагат с адекватни средства за защита, когато отнасящи се до тях данни се обработват в Съединените щати (независимо от правото, което се прилага за тази обработка), както и че Европейският съюз и неговите държави-членки предоставят същите права на гражданите на САЩ.

49. Третият елемент е реципрочност на достъпа на правоприлагащите органи до лични данни. Ако някой инструмент позволява на властите на САЩ достъп до данни, произхождащи от Европейския съюз, реципрочността би изисквала същият достъп да бъде предоставен на органите на ЕС във връзка с данните, произхождащи от САЩ. Реципрочността не трябва да засяга ефективността на защитата на субекта на данните. Това е предпоставка за разрешаване на „трансатлантически“ достъп за органите по правоприлагане. По-конкретно това означава, че:

— Не следва да се разрешава пряк достъп на органите на САЩ до данни в рамките на територията на ЕС (и обратно). Достъп следва да се предоставя само на непряка основа при условията на система „push“.

— Този достъп следва да се осъществява под контрола на органите за защита на данните и на съдебните органи в държавата, където се извършва обработката на данните.

— Достъпът на органите на САЩ до бази данни в рамките на ЕС следва да зачита съществени разпоредби относно защитата на данните (вж. по-горе) и да гарантира пълноценна правна защита на субекта на данните.

Точност на инструмента

50. Конкретизирането на условията за оценка (адекватност, еквивалентност, взаимно признаване) е от съществено значение, тъй като то определя съдържанието по отношение на точността, правната сигурност и ефективността на защитата. Съдържанието на бъдещия инструмент трябва да бъде прецизно и точно.

51. Освен това следва да се поясни, че всяко специфично споразумение, сключено като последваща стъпка, ще трябва да включва подробни и пълни гаранции за защита на данните във връзка със субекта на предвиждания обмен на данни. Само такова двойно ниво на конкретни принципи за защита на данните би гарантирало необходимото „близко съответствие“ между общото споразумение и специфичните споразумения, както вече бе посочено в точки 35 и 36 от настоящото становище.

Разработване на модел за други трети държави

52. Специално внимание заслужава степента, в която споразумение със САЩ би могло до послужи като модел за други трети държави. ЕНОЗД отбелязва, че освен САЩ, горепосоченият доклад на групата „Група за бъдещето“ определя и Русия като стратегически партньор на ЕС. Доколкото принципите са неутрални и съответстват на фундаментални гаранции в ЕС, те биха могли да установят полезен прецедент. Същевременно конкретни аспекти, свързани например с правната рамка на получаващата държава или с целите на предаване, биха попречили на адекватното транспониране на споразумението. От също толкова решаващо значение ще бъде наличието на демократично управление в тези трети държави: следва да се гарантира, че договорените принципи ще бъдат ефективно зачитани и прилагани в държавата-получател.

Какви критерии да бъдат използвани за оценка на нивото на защита?

53. Имплицитната или експлицитна адекватност следва винаги да съответства на международната и европейска правна рамка и по-специално на съвместно договорените

([19]) Глава А. Обвързващо международно споразумение, стр. 8.

гаранции за защита на данните. Те са залегнали в Насоките на ООН, Конвенция 108 на Съвета на Европа и допълнителния протокол към нея, насоките на ОИСР и проекта за рамково решение за защита на данните, както и — по отношение на аспектите от областта на първия стълб — в Директива 95/46/ЕО ([20]). Всички тези инструменти съдържат подобни принципи, които са широко признати като сърцевината на защитата на личните данни.

54. Още по-важно е посочените по-горе принципи да бъдат надлежно отчетени, като се взима предвид въздействието на потенциално споразумение, подобно на споразумението, предвидено от КГВР. Инструмент, който се отнася до целия сектор на *прилагане* на трета държава, действително би могъл да създаде безпрецедентна ситуация. Съществуващите решения за адекватност в областта на първия стълб и сключените споразумения с трети държави в областта на третия стълб на ЕС (Европол, Евроюст) винаги са били свързвани със специфично предаване на данни, докато тук може да бъде възможно предаване с много по-широк обхват, като се има предвид преследваната мащабна цел (борба с криминални престъпления, национална и обществена сигурност, гранично прилагане) и неизвестното количество засегнати бази данни.

Основни изисквания

55. Условията, които трябва да бъдат изпълнени в контекста на предаване на лични данни към трети държави, са развити в работен документ на работната група по член 29 ([21]). Всяко споразумение относно минималните принципи за неприкосновеност на личния живот следва да издържи проверка за съответствие, гарантираща ефективността на гаранциите за защита на данните.

— Относно същността: принципите за защита на данните следва да предоставят високо ниво на защита и да отговарят на стандартите в съответствие с принципите на ЕС. Дванадесетте принципа, включени в доклада на КГВР, ще бъдат допълнително анализирани в този контекст в глава V от настоящото становище.

— Относно специфичността: в зависимост от естеството на споразумението и особено ако става дума за официално международно споразумение, правилата и процедурите следва да бъдат достатъчно подробни, за да позволят ефективно прилагане.

— Относно надзора: за да се гарантира съответствие с договорените правила следва да се въведат специфични механизми за контрол, както вътрешни (одит), така и външни (прегледи). Тези механизми трябва да бъдат еднакво достъпни и за двете страни по споразумението. Надзорът включва механизми за гарантиране на съответствие на макроравнище, като механизми на съвместни прегледи, както и съответствие на микроравнище, като индивидуална правна защита.

56. Освен тези три основни изисквания особено внимание следва да се обърне на специфичните особености, свързани с обработката на лични данни в контекста на правоприлагането. Това е действително област, в която основните права могат да се превърнат в обект на известни ограничения. Ето защо следва да бъдат създадени гаранции, които да компенсират ограничаването на правата на лицата, особено по отношение на следните аспекти, с оглед на въздействието им върху лицето:

— Прозрачност: информацията и достъпът до лични данни могат да бъдат ограничавани в контекста на правоприлагането, например поради необходимостта от провеждане на дискретни разследвания. И докато в ЕС традиционно се създават допълнителни механизми за компенсиране на такова ограничаване на основни права (често включващи независими органи за защита на данните), трябва да се гарантира, че подобни компенсаторни механизми ще бъдат достъпни след като информацията бъде предадена на трета държава.

— Правна защита: поради посочените по-горе съображения лицата следва да разполагат с алтернативни възможности за защита на своите права, по-специално чрез независим надзорен орган и пред съдебен орган.

— Запазване на данни: аргументът за срока за запазване на данни може да не е прозрачен. Трябва да бъдат предприети мерки, така че това да не пречи на ефективното упражняване на права от субекта на данните или от надзорните органи.

([20]) — Насоки на ООН относно компютъризираните досиета с лични данни, приети от Общото събрание на 14 декември 1990 г., достъпни на www.unhchr.ch/html/menu3/b/71.html
— Конвенция на Съвета на Европа за защита на лицата при автоматична обработка на лични данни, 28 януари 1981 г., досъпна на www.conventions.coe.int/treaty/en/Treaties/html/108.html
— Насоки на ОИСР относно защитата на личната неприкосновеност и трансграничния поток на лични данни, приета на 23 септември 1980 г., достъпна на www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Проект за Рамково решение на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, достъпен на http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 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 (ОВ L 281, 23.11.1995 г., стр. 31).

([21]) Работен документ от 24 юли 1998 г. относно предаване на лични данни до трети държави: Прилагане на членове 25 и 26 от Директивата на ЕС за защита на данните; WP12.

— Отговорност на правоприлагащите органи: в отсъствието на ефективна прозрачност, механизмите за контрол от страна на отделното лице или на институционалните участници по никакъв начин не могат да бъдат изчерпателни. Ще продължи да бъде от решаващо значение този контрол да бъде стабилно установен, с оглед на чувствителността на данните и на принудителните мерки, които могат да бъдат налагани на лицата, въз основа на обработката на такива данни. Отговорността е решаващ аспект по отношение на националните механизми за контрол на държавата-получател, но също така и по отношение на възможностите за преглед по държави или регион на произход на данните. Такива механизми за преглед са предвидени в специфични споразумения като споразумението за резервационните данни на пътниците и ЕНОЗД силно препоръчва те да бъдат включени и в генералния инструмент.

V. **АНАЛИЗ НА ПРИНЦИПИТЕ**

Въведение

57. В настоящата глава се прави анализ на включените в документа на КГВР 12 принципа от следната гледна точка:

— Тези принципи показват, че САЩ и ЕС имат някои общи виждания относно нивото на принципите, като могат да бъдат отбелязани и прилики с принципите в Конвенция 108.

— Същевременно постигането на споразумение относно нивото на принципите не е достатъчно. Правният инструмент следва да бъде достатъчно силен, за да гарантира съответствие.

— ЕНОЗД изразява съжаление, че принципите не се съпътстват от обяснителен меморандум.

— Преди да се пристъпи към описание на принципите, следва да бъде ясно заявено, че двете страни тълкуват еднакво използваните формулировки, например по отношение на понятието лична информация или защитено лице. В този смисъл евентуални определения биха били желателни.

1. Конкретизиране на целта

58. Първият принцип, посочен в приложението към доклада на КГВР, гласи, че личната информация се обработва за легитимни цели на правоприлагането. Както бе посочено по-горе, за Европейския съюз това означава предотвратяване, задържане, разследване или наказателно преследване на наказуеми деяния. За САЩ обаче тълкуването на правоприлагането надхвърля наказуемите деяния и включва „цели на граничното прилагане, обществената сигурност и националната сигурност“. Последиците от тези несъответствия в обявените цели на ЕС и САЩ остават неясни. Макар в доклада да се споменава, че на практика целите могат да съвпадат до голяма степен, от решаващо значение остава да се установи точно до каква степен те *не* съвпадат. В областта на правоприлагането с оглед на въздействието на предприетите мерки върху лицата, принципът за ограничаването на целта трябва да бъде стриктно спазван, а обявените цели трябва да бъдат ясни и дефинирани. Отчитайки предвидената в доклада реципрочност, сближаването на тези цели също изглежда важно. Накратко, необходимо е изясняване на тълкуването на този принцип.

2. Интегритет/качество на данните

59. ЕНОЗД приветства разпоредбата, изискваща точна, съответстваща, своевременна и пълна лична информация, според нуждите на законосъобразната обработка. Този принцип е главно условие за всяка ефективна обработка на данни.

3. Необходимост/пропорционалност

60. Принципът ясно показва връзката между събраната информация и необходимостта от тази информация за постигане на целите на правоприлагането, установени в закона. Това изискване за законово основание е позитивен елемент за удостоверяване на легитимността на обработката. Въпреки това ЕНОЗД отбелязва, че макар и това да укрепва правната сигурност на обработката, правното основание за такава обработка се съдържа в правото на трета държава. Правото на трета държава не може само по себе си да съставлява легитимно основание за предаване на лични данни ([22]). В контекста на доклада на КГВР изглежда се предполага, че легитимността на правото на трета държава, т.е. на САЩ, се признава по принцип. Следва да се държи сметка, че ако такива аргументи могат да бъдат приети тук, отчитайки факта, че САЩ са демократична държава, същата схема не би била валидна и не би могла да бъде транспонирана в отношенията с друга трета държава.

61. Всяко предаване на лични данни трябва да има връзка с въпроса, да бъде необходимо и уместно, съгласно приложението към доклада на КГВР. ЕНОЗД изтъква, че за да бъде пропорционална, обработката не трябва да навлиза ненужно в личното пространство, а условията на процеса да бъдат балансирани, като се отчитат правата и интересите на субектите на данни.

62. Поради тази причина достъпът до информация следва да се предоставя за всеки отделен случай, в зависимост от практическите нужди в контекста на конкретно разследване. Постоянният достъп на правоприлагащите органи на трета държава до бази данни, намиращи се в ЕС, би бил разглеждан като непропроционален и недостатъчно аргументиран. ЕНОЗД припомня, че дори в контекста на

([22]) Вж. по-конкретно член 7, букви в) и д) от Директива 95/46/ЕО. В становището си 6/2002 от 24 октомври 2002 г. относно предаването на информация от списъка на пътниците и други данни от авиокомпаниите на органите на САЩ, работната група по член 29 заяви, че „не изглежда приемливо, едностранно решение, взето от трета държава по съображения за собствените ѝ обществени интереси да води до установяване на рутинна практика и „предаване на едро“ на данни, защитени по силата на директивата.“

съществуващи споразумения за обмен на данни, напр. в случая със споразумението за резервационните данни на пътниците, обменът на данни се основава на специфични обстоятелства и се сключва за ограничен период от време ([23]).

63. По същата логика срокът на запазване на данните следва да бъде регулиран: данните следва да бъдат съхранявани, само докато са необходими, като се отчита преследваната специфична цел. Ако са престанали да имат отношение към определената цел, те следва да бъдат заличавани. ЕНОЗД категорично се противопоставя на изграждането на „складове“ за данни, в които да се съхранява информация за нищо неподозиращи лица с оглед на евентуална бъдеща необходимост.

4. Информационна сигурност

64. В принципите са разработени мерки и процедури за опазване на данните от злоупотреба, промени и от други рискове, както и разпоредба за ограничаване на достъпа на оправомощени лица. ЕНОЗД счита това за удовлетворително.

65. Освен това принципът би могъл да бъде допълнен от разпоредба, посочваща, че следва да се водят дневници на лицата, които имат достъп до данните. Това би повишило ефективността на гаранциите за ограничаване на достъпа и би предотвратило злоупотреба с данните.

66. Освен това в случай на нарушения на сигурността следва да бъде предвидено взаимно информиране: получателите в САЩ, както и в ЕС, биха носили отговорност за информиране на своите партньори в случай, че данните, които получават са предмет на незаконно разкриване. Това би допринесло за повишена отговорност в посока към сигурност при обработката на данни.

5. Специални категории лична информация

67. Според ЕНОЗД предвиденото изключение, което позволява всякаква обработка на чувствителни данни, за които вътрешното право предвижда „подходящи гаранции“, значително отслабва принципа, който забранява обработка на чувствителна информация. Тъкмо поради чувствителния характер на данните всяка дерогация от принципа за забрана трябва да бъде адекватно и точно аргументирана със списък от цели и обстоятелства, при които определен тип чувствителни данни могат да бъдат обработвани, както и посочване на качеството на контрольорите, оправомощени да обработват такъв тип данни. ЕНОЗД счита, че една от гаранциите, които трябва да бъдат приети, и, че чувствителните данни не следва да съставляват сами по себе си елемент, който би могъл да предизвика разследване. Достъп до тях може да се предоставя при определени обстоятелства, но само като допълнителна информация по отношение на субекта на данни, който вече се разследва. Тези гаранции и условия трябва да бъдат изброени изчерпателно в текста на принципа.

6. Отговорност

68. Както е изтъкнато в точки 55—56 от настоящото становище, отговорността на публичните органи, които обработват лични данни, трябва да бъде ефективно гарантирана, и в споразумението да бъдат предоставени гаранции за начина, по който ще бъде осъществявана тази отговорност. Това е още по-важно, като се има предвид липсата на прозрачност, която традиционно се свързва с обработката на лични данни в контекста на правоприлагането. От тази гледна точка, споменаването — какъвто е понастоящем случаят с приложението, че публичните органи носят отговорност, без да се предоставят каквито и да било допълнителни обяснения относно условията и последиците от тази отговорност, не е удовлетворителна гаранция. ЕНОЗД препоръчва в текста на инструмента да бъде включено обяснение в този смисъл.

7. Независим и ефективен надзор

69. ЕНОЗД напълно подкрепя включването на разпоредба, предвиждаща независим и ефективен надзор, упражняван от един или няколко публични надзорни органа. Според ЕНОЗД трябва ясно да се заяви по какъв начин се тълкува понятието „независимост“, по-специално от кого са независими и на кого докладват тези органи. В това отношение са необходими критерии, които следва да отчитат институционалната и функционална независимост във връзка с изпълнителните и законодателните органи. ЕНОЗД припомня, че това е съществен елемент за гарантиране на ефективно съответствие с договорените принципи. Правомощията на тези органи за намеса и прилагане са решаващи и от гледна точка на въпроса за отговорността на публичните органи, които обработват лични данни, както е посочено по-горе. Тяхното съществуване и компетентност следва да бъдат ясно разпознаваеми за субектите на данни, за да им се позволи да упражняват своите права, особено ако няколко органа са компетентни в зависимост от контекста на обработката.

70. Нещо повече, ЕНОЗД препоръчва в едно бъдещо споразумение да се предвидят и механизми за сътрудничество между надзорните органи.

8. Индивидуален достъп и нанасяне на поправки

71. Необходими са специфични гаранции, когато става въпрос за достъп и нанасяне на поправки в контекста на правоприлагането. В този смисъл ЕНОЗД приветства принципа, който гласи, че на лицата се предоставя/следва да се предостави достъп до и средства за търсене на „поправка и/или заличаване на тяхна лична информация“. Същевременно остава известна несигурност по отношение на определението за лица (следва да бъдат защитени всички субекти на данни, а не само гражданите на съответната държава) и на условията, при които лицата могат да оспорват обработката на свързана с тях информация.

([23]) Споразумението изтича и престава да поражда действие седем години след датата на подписването му, освен ако страните взаимно договорят да го заменят с друго.

Необходимо е уточняване на понятието „подходящи случаи“, при които може или не може да се повдига възражение. За субектите на данни следва да бъде ясно при какви обстоятелства — в зависимост от вида орган, вида разследване или други критерии — те ще могат да упражняват правата си.

72. Освен това ако липсва пряка възможност за повдигане на възражение по повод на обработка по аргументирани причини, следва да се предвиди възможност за непряка проверка посредством независим орган, отговарящ за надзора на обработката.

9. Прозрачност и обявяване

73. ЕНОЗД изтъква още веднъж важността на ефективната прозрачност, за да се даде възможност на лицата да упражняват правата си и да се допринесе за цялостната отговорност на публичните органи, обработващи лични данни. ЕНОЗД подкрепя принципите във вида, в който се предлагат, и се застъпва по-конкретно за необходимостта от общо и индивидуално информиране на лицето. Това е отразено в принципа, изведен в точка 9 от приложението.

74. Същевременно в глава 2, А. В („Договорени принципи“) от доклада се отбелязва, че в САЩ под „прозрачност“ може да се разбира „индивидуално или съчетано публикуване във Федералния регистър, индивидуално информиране, и разкриване в рамките на съдебно производство“. Трябва да бъде ясно, че сама по себе си публикацията в официален вестник не е достатъчна, за да гарантира подходящо информиране на субекта на данни. Освен необходимостта от индивидуално информиране ЕНОЗД припомня, че информацията трябва да бъде предоставена във форма и на език, който е лесно разбираем за субекта на данни.

10. Правна защита

75. За да се гарантира ефективното упражняване на правата им, лицата трябва да могат да подават оплакване пред независим орган за защита на данните, както и да разполагат със средства за правна защита пред независим и безпристрастен съдебен орган. И двете възможности за правна защита следва да бъдат еднакво достъпни.

76. Достъпът до независим орган за защита на данните е необходим, тъй като предоставя гъвкава и не толкова скъпа помощ, в контекст (правоприлагането), който би могъл да бъде неразбираем за лицата. Органите по защита на данните могат да предоставят помощ и при упражняване на права на достъп от името на субектите на данни, в случаите когато изключения препятстват последните да получат пряк достъп до свои лични данни.

77. Достъпът до съдебната система е допълнителна и необходима гаранция, че субектите на данни могат да търсят правна защита от орган, който принадлежи към клон на демократична система, различна от публичните институции, които реално обработват техните данни. Съдът на ЕО ([24]) счита такова ефективно средство за правна защита пред съд за „съществено с цел на индивида да се гарантира ефективна защита на правото му. (...) [Той] отразява общ принцип на правото на Общността, който подчертава общите за държавите-членки конституционни традиции и е залегнал в членове 6 и 13 от Европейската конвенция за защита на правата на човека и основните свободи.“ Наличието на съдебно средство за защита е изрично предвидено и в член 47 от Хартата на основните права на Европейския съюз, и в член 22 от Директива 95/46 ЕО, без да се засяга възможността за административна защита.

11. Автоматизирани индивидуални решения

78. ЕНОЗД приветства разпоредбата, предвиждаща подходящи гаранции в случаи на автоматизирана обработка на лична информация. ЕНОЗД отбелязва, че общото разбиране за това, което се счита за „значимо противодействие по отношение на съответните интереси на лицето“ би изяснило условията за прилагане на този принцип.

12. Последващо предаване

79. Условията за извършване на последващо предаване са в някои случаи неясни. По-конкретно, когато последващото предаване трябва да съответства на международни договорености и споразумения между изпращащите и получаващите държави, следва да бъде уточнено дали това се отнася до споразумения между двете държави, които са започнали предаването, или двете държави, участващи в последващото предаване. Според ЕНОЗД при всички случаи са необходими споразумения между двете държави, които са започнали първото предаване.

80. Освен това ЕНОЗД отбелязва доста широкото определение за „легитимни обществени интереси“, което позволява последващо предаване. Обхватът на обществената сигурност остава неясен, а разширяването на предаването в случай на нарушаване на етичните правила или на регулираните професии изглежда неоправдано и прекомерно в контекста на правоприлагането.

VI. **ЗАКЛЮЧЕНИЕ**

81. ЕНОЗД приветства съвместната дейност на органите на ЕС и САЩ в областта на правоприлагането, където защитата на личните данни е от решаващо значение. Въпреки това ЕНОЗД би желал да наблегне на факта, че въпросът е комплексен, особено що се отнася до неговия точен обхват и естество, поради което заслужава внимателен и

([24]) Дело 222/84 *Johnston* [1986] ECR 1651; Дело 222/86 *Heylens* [1987] ECR 4097; Дело C-97/91 *Borelli* [1992] ECR I-6313).

задълбочен анализ. Въздействието на един трансатлантически инструмент върху защитата на данните следва да бъде обмислено внимателно във връзка със съществуващата правна рамка и последствията за гражданите.

82. ЕНОЗД призовава за повече яснота и конкретни разпоредби, по-специално по отношение на следните аспекти:

— Яснота по отношение на естеството на инструмента, който следва да бъде правно обвързващ, за да предоставя достатъчно правна сигурност;

— Задълбочена констатация на адекватността въз основа на съществените изисквания по отношение на аспектите, свързани със същността, специфичността и надзора на схемата. ЕНОЗД счита, че адекватността на генералния инструмент би могла да бъде призната, само ако се комбинира с адекватни специфични споразумения за всеки отделен случай.

— Дефинирано приложно поле с ясно и точно определение на преследваните цели на правоприлагането;

— Уточнения относно условията, при които частни структури могат да участват в схеми за предаване на данни;

— Съответствие с принципа на пропорционалност, предполагащ обмен на данни за всеки отделен случай, при наличието на конкретна нужда;

— Силни механизми за надзор и механизми за правна защита, достъпни за субектите на данни, включително административни и съдебни средства за защита;

— Ефективни мерки, гарантиращи упражняването на правата на всички субекти на данни, независимо от гражданството им;

— Участие на независими органи за защита на данните във връзка по-специално с надзора и подпомагането на субектите на данни.

83. ЕНОЗД набляга на факта, че следва да се избягва всякакво прибързване при изработването на принципите, тъй като това само би довело до незадоволителни решения, обратни на желаните по отношение на защитата на данните. Следователно най-добрият начин за бъдеща работа на този етап е разработването на пътна карта за постигане на евентуално споразумение на по-късен етап.

84. Освен това ЕНОЗД призовава за повече прозрачност в процеса на изработване на принципите за защита на данните. Единствено чрез привличане на всички участници, включително Европейския парламент, инструментът би могъл да извлече полза от демократичния дебат и да получи необходимата подкрепа и признание.

Съставено в Брюксел на 11 ноември 2008 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните