ИКОНОМИКА И УПРАВЛЕНИЕ, ГОД. VI, №3

доц. д-р ГАБРИЕЛА БЕЛОВА
ЮГОЗАПАДЕН УНИВЕРСИТЕТ „НЕОФИТ РИЛСКИ", БЛАГОЕВГРАД

НЯКОИ ПРОБЛЕМИ ВЪВ ВРЪЗКА СЪС ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В ЕВРОПЕЙСКИЯ СЪЮЗ

PROBLEMS RELATED TO THE PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

Associate Prof. Dr. GABRIELA BELOVA
SOUTH-WEST UNIVERSITY "NEOFIT RILSKI", BLAGOEVGRAD

Abstract: The development of the European integration increases the importance of personal data protection of European citizens. The author traces back the legislation of personal data protection to the current practice of the European Court of Justice and the European Court of Human Rights. She also examines the functions and the competences of the European Data Protection Supervisor as one of the newest bodies of the European Union. The new development of personal data protection in accordance with the Lisbon Treaty is also examined. Recently, both European institutions and Member States show exceptional activity in suggesting new measures related to data base, sources of information, the duration of its storage and the ways in which it would be transferred. In any case, however, there is a delicate balance between privacy and other fundamental rights and democratic principles, as well as the considerations related to the protection of public order and security.
Key Words: protection of personal data, privacy, European Data Protection Supervisor

Защитата на личните данни е сравнително нова тема, която се свързва предимно с развитието на информационните технологии, даващо възможност за бързо обработване на огромни бази с лична информация и пораждащо опасения от злоупотреби. Подписването на споразумение между Европейския съюз и САЩ през м. юли 2010 г. относно достъпа до банкова информация бе постигнато след сериозни промени следствие на възражения и изразена загриженост от страна на Европейския парламент. Основното настояване на евродепутатите бе споразумението да бъде в съответствие с изискванията на Лисабонския договор и особено на Хартата за основните права, както и Съединените щати да се съобразят напълно с европейските стандарти за защита на личните данни и да се намери правилния баланс между антитерористичните мерки и правата и свободите на гражданите. В свои изказвания европейският комисар по вътрешните работи г-жа Сесилия Малстрьом подчертава, че европейските граждани трябва да знаят как техните лични данни се съхраняват и обменят, а също така, че Европейският съюз за първи път приема един дългосрочен и всеобхватен подход по тази проблематика[1].

Всъщност, правото на лична неприкосновеност е признато за основно човешко право. Защитата на личните данни, като аспект на правото на неприкосновеност намира приложение в най-разнообразни сфери от нашия живот и това понякога води до сложни въпроси и поражда неподозирани проблеми. Често се налага да се търси баланс между личната неприкосновеност и други основни човешки права и демократични принципи. Разграничаването на личната сфера от интереса на обществото все

[1] 'EU lists data-sharing policies for the first time', eu observer.com, 20.07.2010

по-често води и до сблъсък между защитата на личната неприкосновеност и обществената сигурност. "Претеглянето" на интересите и намирането на баланс между тях изискват не само демократична култура, но и изграждането на общи правила и стандарти, които да ни водят в преценката[1].

Защитата на личните данни придобива нарастваща популярност с развитието на европейската интеграция. Преди всичко защото е свързана с необходимостта да се решават все по-конкретни практически проблеми за свободното движението на хора, услуги стоки и капитали в страните членки на Съюза.

1. Защитата на личните данни като основно човешко право

Както бе посочено, защитата на личните данни обикновено се свързва с правото на лична неприкосновеност. Неприкосновеността на личността е уредена в Член 8 на Конвенцията за защита човешките права и основни свободи, подписана на 4 ноември 1950 г. в рамките на Съвета на Европа. Член 8 е озаглавен **„Право на зачитане на личния и семейния живот"** и гласи следното:

1. Всеки има право на неприкосновеност на личния и семейния си живот, на жилището и на тайната на кореспонденцията.

2. Намесата на държавните власти в упражняването на това право е недопустима, освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

Чл. 6 от Договора за създаване на Европейската общност (ДЕО)[2] забранява всякаква дискриминация, основаваща се на националността, а член 8 от провъзгласената в Ница през м. декември 2000 г. Харта на основните права на европейските граждани вече е озаглавен **„Защита на личните данни"** и има следното съдържание:

1. Всеки има право на защита на личните му данни.

2. Тези данни трябва да се ползват лоялно, за конкретни нужди със съгласието на заинетересованото лице или на друго законно основание, предвидено в закона. Всеки има право на достъп до събраните за него данни, както и да иска поправки в тях.

3. Спазването на тези правила подлежи на контрол от страна на независим орган.

Самият факт на обособяването на защитата на личните данни в самостоятелен текст говори, че това представлява отделно фундаментално човешко право, различаващо се от неприкосновеността на личността, която е уредена в Чл.7 от Хартата[3]. В полза на самостоятелността на защитата на данните може да бъде приведен и възприетият от Съда на Европейските общности подход по обединени дела C-465/00, C-138/01 и C-139/01 *Rechnungshof* с предмет три преюдициални запитвания. Правото на защита на данните включва всички лични данни и **не е ограничено само до личния и семейния живот** на индивида, а напротив обхваща и въпроси, свързани с **работата и доходите му**. Съдът

[1] Следва да се има предвид, че първият закон за защита на личните данни е изготвен и приет в германската провинция Есен на 7 октомври 1970 г. През 70-те години на XX век започват да се приемат и национални закони – сред "пионерите" в Европа са: Швеция (1973), ФРГ (1976), Франция (1978), Дания (1978), Норвегия (1978),Австрия (1978) и Люксембург.

[2] Подписан в Рим на 25 март 1957 г., в сила от 1 януари 1958 г.

[3] Чл. 7 от Хартата буквално повтаря текста на Чл.8 на ЕКПЧ, че всеки има право на неприкосновеност на личния и семейния си живот, на жилището и на тайната на кореспонденцията.

приема, че въпросните данни по делата по главното производство относно доходите на служителите в някои структури, представляват лични данни по смисъла на член 2, буква а) от Директива 95/46, тъй като става дума за „информация, свързана с идентифицирано или подлежащо на идентификация лице". Тяхното регистриране и използване от въпросната структура, както и тяхното предаване на Rechnungshof и включването им от него в доклад, предназначен да бъде съобщен на различни политически инстанции и широко разпространен, представлява обработване на лични данни по смисъла на член 2, буква б) от упоменатата директива. СЕО решава, позовавайки се на решения на Европейския съд по правата на човека, че терминът „личен живот" не следва да се интерпретира рестриктивно и че „никаква важна причина не позволява от него да се изключат професионалните дейности"[1].

Международноправните документи, свързани със защитата на личните данни, не са твърде много на брой, поради което по-важните от тях все пак биха могли да бъдат посочени:

- **Конвенция № 108 на Съвета на Европа** от 28.01.1981 г. за защита на лицата при автоматизираната обработка на лични данни[2]. Към Конвенцията е приет допълнителен протокол относно контролните органи и трансграничните потоци от данни[3]. В рамките на Съвета на Европа действат и редица препоръки и резолюции на Комитета на министрите, свързани със защита на личните данни в различни области като застраховането, статистиката, медицинските данни, телекомуникации, плагежни и други операции, трудова заетост, социално осигуряване и др.[4]
- **Основни насоки относно електронната обработка на** личните данни**,** приети от Общото събрание **на ООН** на 14 декември 1990 г**.**
- **Препоръка /ръководни принципи** относно основните насоки за защитата на личната неприкосновеност и трансграничните потоци на лични данни, приета от Съвета на **Организацията за икономическо сътрудничество и развитие** на 23 септември 1980 г.

В рамките на **Европейския съюз** основната разпоредба от първичното право, регламентираща защитата на личните данни, е **член 286, ДЕО**, който гласи:

От 1 януари 1999 г. актовете на Общността относно закрилата на физическите лица при обработването на личните данни и свободното движение на тези данни се прилагат спрямо институциите и органите, създадени по или въз основата на този договор.

Преди датата по § 1 Съветът, съгласно процедурата по чл. 251, създава независим контролен орган, отоговорен за контрола по прилагането на тези актове на Общността спрямо институциите и органите на Общността и приема други релевантни разпоредби, в зависимост от случая.

Сред вторичното право на Общността, безспорно би следвало да бъде изведена на преден план приетата на 24 октомври 1995 г. е приета **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 за свободното движение на тези данни. Именно тази директива вземат под внимание всички държави, приели своите национални закони за защита на

[1] Вж. Европейски съд по правата на човека., Решение по дело Amann/Швейцария от 16 февруари 2000 г., Recueil des arrêts et décisions 2000-II, § 65, и Решение Rotaru/Румъния от 4 май 2000 г., Recueil des arrêts et décisions 2000-V, § 43.

[2] Ратифицирана със закон, приет от 39-о Народно събрание на 29.05.2002 г. - ДВ, бр. 56 от 7.06.2002 г. Издадена от Министерството на вътрешните работи, обн. ДВ, бр. 26 от 21.03.2003 г., в сила от 1.01.2003 г.

[3] CETS 181.

[4] Напр. No R (2002) 9, No R (99) 5, No R (97) 18 и др.

личните данни след 1995 г., независимо от тяхната географска принадлежност, превръщайки я в единствения световен стандарт в посочената област. През 2003 г. Европейската комисия публикува първия си доклад по прилагането на директивата[1]. Друг приет в рамките на ЕС акт е **Директива 2002/58/ЕО** на ЕП и Съвета за обработване на лични данни и защита неприкосновеността в електронния съобщителен сектор, както и правилата, свързани с Шенгенското пространство, Европол и Евроюст.

2. Директива 95/46/ЕО

Директива 95/46/ЕО си поставя за цел осигуряване на висока степен на защита на личните данни като част от правото на личен живот на индивидите, приемайки, че е невъзможно нито ограничаването, нито забраната на свободното движение на лични данни между държавите-членки. Директивата се отнася както за публичния, така и за частния сектор. По смисъла на Член 2 на Директива 95/46/ЕО терминът **„лични данни“** означава всяка информация, свързана с **идентифицирано** или **подлежащо на идентификация лице**; като за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност. Налице е едно разширително тълкуване, излизащо извън традиционното разбиране за лични данни като трите имена на физическото лице, ЕГН или номер на документ за самоличност.

Също толкова широко е дефинирано и понятието за **„обработване на лични данни“** – обработване означава всяка операция или набор от операции, извършвани или не с автоматични средства, прилагани към личните данни, като **събиране, запис, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на предоставяне на данните, актуализиране или комбиниране, блокиране, изтриване или унищожаване**[2].

Държавите-членки обаче предвиждат, че обработването на лични данни може да се извършва, само ако:

- съответното физическо лице е дало **недвусмислено** своето **съгласие** за това; или
- обработването е необходимо за **изпълнението на договор**, по който съответното физическо лице е страна, или за да се предприемат стъпки по искане на съответното физическо лице преди сключването на договора; или
- обработването е необходимо за спазването на правно задължение от **администратора** на личните данни**;** или
- обработването е необходимо, за да бъдат защитени **жизнено важни интереси** на съответното физическо лице; или
- обработването е необходимо за изпълнението на задача, която се осъществява в **обществен интерес** или при упражняване на официалните правомощия, които са предоставени на администратора или на трето лице, на което се разкриват данните;или
- обработването е необходимо за целите на **законните интереси,** преследвани от администратора или от трето лице/лица, на които се разкриват данните, с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице, които изискват защита в съответствие с Директивата.

[1] COM/2003/0265 final

[2] Чл. 2 Директива 95/46/ЕО

Основен принцип на Директивата е събираните личните данни:

- да бъдат адекватни, релевантни, и да **не са прекомерни по отношение на целите**, за които се събират и/или обработват допълнително. Събирането на лични данни се извършва с оглед на **конкретни, ясно формулирани и законни цели** и да не бъдат допълнително обработени по начин, който е несъвместим с тези цели. Допълнителната обработка на данните за исторически, статистически или научни цели няма да се разглежда като несъвместима, при условие че държавите-членки предоставят необходимите гаранции за това;
- да бъдат **точни** и при необходимост **да се актуализират**; трябва да се предприемат всички възможни разумни стъпки, за да се гарантира, че данни, които са неточни или непълни по отношение на целите, за които са събрани, или за които се обработват допълнително, се изтриват или поправят;
- да бъдат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително.

Директива 95/46/ЕО забранява обработването на т.нар. **специални лични данни** (*sensitive data*), разкриващи расов или религиозен произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи, като и обработването на данни, свързани със здравословното състояние и половия живот. Изключенията от тази забрана са в случаите, когато:

- съответното физическо лице е дало изричното си **съгласие** за обработването на такива данни;
- обработването е необходимо за изпълнението на **задълженията на администратора** в областта на трудовото законодателство;
- обработването е необходимо **за защита на жизнените интереси** на съответното или на друго физическо лице;
- обработването се извършва при изпълнение на законосъобразната дейност на **организация с нестопанска цел** (фондация, сдружение или друга организация с нестопанска цел, с политическа, философска, религиозна или профсъюзна цел, при условие че обработването е свързано единствено с членовете на тази организация или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че данните не се разкриват на трети лица без съгласието на съответното физическо лице);
- обработването е свързано с данни, които са направени **публично достояние** от съответното физическо лице, или са заведени правни искове.

С оглед на тяхното съдържание и начин на упражняване правата на индивидите по отношение на личните данни могат да бъдат разграничени като право на **информираност,** право на **възражение** и право на **достъп**. Правото на информация означава, че всяко физическо лице има право да получи от администратора ясна и достатъчна информация в разбираема форма относно данните, които се обработват. Правото на възражение се упражнява от физическите лица пред администратора срещу обработване на личните им данни. В тези случаи, ако то е основателно, личните данни не могат повече да бъдат обработвани.

Индивидите също така имат право на достъп в разумен срок от време до информация или потвърждение за това, дали отнасящи се до него данни се обработват, както и информация най-малкото за целите на тази обработка, категориите данни и получателите или категориите получатели, на които данните се разкриват. В резултат на упражняване на правото си на достъп до отнасящи се до съответните физически лица данни, индивидите могат да

поискат заличаване, коригиране или блокиране на лични данни от администратора, когато обработването им не отговаря на изискванията на Директива 95/46/ЕО.

На тези права на индивидите кореспондират задълженията и отговорността на администратора за сигурността и поверителния характер на обработването на личните данни, както и за уведомяването на **надзорния орган** в съответната държава членка. Всяка държава-членка предвижда, че на нейната територия един или повече държавни органи отговарят за контрола на прилагането на разпоредбите, приети за защита на личните данни на индивидите. Тези органи се ползват с **пълна независимост** при упражняване на функциите, които са им възложени. Обхватът на компетенциите на надзорните органи на държавите членки е очертан в чл. 28 от Директива 95/46/ЕО, но „пълна независимост" означава липса на каквито и да е възможности за контрол от страна на националните правителства.

Вътре в рамките на Европейския съюз обработването на личните данни се осъществява при условията на свободно движение на данните, но също така и висока степен на защита и хармонизирани правила. **Предаването (трансфер) на лични данни**, които са подложени или предназначени за обработка към трети страни извън Европейския съюз е възможно само ако въпросната трета страна гарантира адекватна степен на защита на личните данни[1]. Достатъчният характер на степента на защита, предоставяна от трета страна, се преценява в светлината на всички обстоятелства, свързани с операцията по предаването на данни или набор от операции по предаване на данни; специално внимание се обръща на характера на данните, целта и продължителността на предлаганата операция или операции по обработката им, на страната по произхода и страната по крайното местоназначение, на законовите правила, както общи, така и секторни, които са в сила във въпросната трета страна, както и на професионалните правила и мерките за сигурност, които се спазват в тази страна. Европейската комисия може да вземе решение за наличие на адекватна защита на обмена на личните данни с трети страни, каквито след 2000 г. са взети по отношение на Аржентина, Канада, Швейцария[2].

С оглед преодоляването на различията относно неприкосновеността на личността между Европа и Съединените щати, от Европейската комисия и от Търговския департамент на САЩ бе разработена т.нар. *Safe Harbor* рамка за сътрудничество. Включването в тази рамка удостоверява, че съответната американска компания или организация предоставя достатъчна степен защита на личните данни, съответстваща на изискванията на Директива 95/46/ЕО. В резултат на положените усилия бе прието и Решение за адекватност 2000/520/ЕО от 26.07.2000 г. на Европейската комисия, касаещо Съединените щати.

3. Практика на СЕО по отношение на Директива 95/46/ЕО

Сравнително наскоро през 2006 г. **Съдът на Европейските общности** имаше възможност да се произнесе относно споразумение между ЕС и САЩ относно предоставянето на лични данни на пътниците при самолетни пътувания (PNR Agreement). Терминът **PNR (Passenger Name Record)** включва данни относно имената на пътниците; дестинацията; детайли, свързани с издаването на билета; агенцията, през

[1] Zerdick, Thomas "Protection of Personal Data" Brussels 7-8 September 2006 "Croatia and Turkey: Screening Chapter 23 – Judiciary and Fundamental Rights" http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

[2] Commission Decision 2003/490/EC; 2002/2/EC; 2000/518/EC.

която се закупува билетът; лицето/компанията, извършваща резервацията. Първоначално Международната асоциация за въздушен транспорт (IATA) определя рамките и съдържанието на тези данни, като те се предоставят само при самолетните пътувания. Впоследствие PNR данните започват да се използват и и при резервиране на хотели, рент-а-кар и други дейности. След събитията от 11 септември 2001 г. PNR данните включват пълните имена на пътниците (дотогава практиката е да се използва фамилното име и инициалите на собственото), паспортните данни (националност, номер на паспорта и дата на изтичане), както и датата, и мястото на раждане. Разширяването на обхвата на PNR данните предизвиква загрижеността на редица неправителствени организации относно неприкосновеността на личността, тъй като данните могат да съдържат домашен и служебен адрес, телефонни номера, данни от кредитни карти, инвалидност – т.е. данни от медицински или финансов характер, които според европейските стандарти би трябвало да се ползват с определена степен на защита. В САЩ със събирането, трансфера и запазването на данните се занимава специална структура - Бюро за митническа и гранична защита към новосъздадения Департамент за вътрешна сигурност (Department for Homeland Security). През 2004 г. американската администрация започва да преговаря с Европейската комисия относно подписването на споразумение за трансфер на PNR данни (US - EU PNR Agreement)[1]. Европейската комисия счита, че нивото на защита при трансфера на PNR данните ще съответства на изискванията на Директива 95/46/ЕО[2], тъй като данните ще бъдат събирани и използвани само с оглед на "превенция и борба с тероризма и свързаните с него престъпления, други сериозни престъпрения, включително организираната престъпност, които са транснационални по своята същност". По силата на това споразумение европейските авиокомпании трябва до 15 минути след излитането на въздухоплавателното средство да предоставят PNR данните на компетентните американски власти, а за неизпълнение на своето задължение заплащат глоба от 5 хиляди долара за информацията за всеки пътник. Европейският парламент инициира съдебно производство пред СЕО, като счита, че решението[3] е прието от Комисията при превишаване на пълномощията й (*ultra vires*) и нарушава основни принципи, възприети в Директива 95/46/ЕО като неприкосновеността на личността и защитата на личните данни. С решение от 30 май 2006 г[4]. СЕО обявява за недействително решението на Съвета[5] за сключването на споразумението между ЕС и САЩ относно транфера на PNR данните, както и решението на Европейската комисия за наличие на адекватна защита на трансферираните данни[6]. Решението на Съда започва с позоваване на разпоредбата на Чл. 8 от ЕКПЧ, касаеща неприкосновеността на личния и семейния живот[7]. СЕО приема, че споменатото споразумение следва да бъде сключено не въз основа на общата транспортна политика на Съюза (която спада към общностния стълб), а трансферът на PNR данните се извършва с оглед на дейности, причислявани към втория и третия

[1] http://ec.europa.eu/idabc/en/document/2596/362
[2] Directive 95/46 EC

[3] Commission Decision 2004/535/EC of 14 May 2004. За повече информация вж. Elspeth Guid & Evelin Brower, The Political Life of Data: the ECJ Decision on the PNR Agreement between the EU and the US, July, 2006, Centre for European Policy Studies, available at http://www.libertysecurity.org/IMG/pdf/1363.pdf.
[4] Решение по обединените дела Case C-317/04 и Case C-318/04
[5] Council Decision 2004/496/EC of 17 May 2004
[6] Commission Decision 2004/535/EC of 14 May 2004.
[7] Следва да се има предвид, че ЕС все още не е страна по ЕКПЧ.

стълб, а именно "обществена сигурност, отбрана и наказателноправно сътрудничество"; следователно Директива 95/46/ЕО е неприложима, тъй като Чл.3, ал.2 изрично изключва приложението ѝ по отношение на втория и третия стълб и ограничава трансфера на данните само до общностния стълб. Според СЕО споразумението ЕС – САЩ не е сключено на подходящото правно основание, което от своя страна поставя въпроса за неотложното премахване на стълбовата архитектура на Съюза, което се очаква да стане факт с влизането в сила на Лисабонския договор.

Безспорно, решението по т.нар PNR – дела, постановяващо анулирането на споразумението за трансфер на данни на пътници по презокеанските полети към Департамента за вътрешна сигурност на САЩ, е един от най-ярките и последни по време примери за ангажираността на Съда на Европейските общности със защитата на личните данни. СЕО обаче е имал възможността да се произнесе и преди това по преюдициално запитване в рамките на производството срещу ***г-жа Lindqvist***, която е обвинена в нарушение на шведското законодателство относно защитата на лични данни, като е публикувала на нейния интернет сайт лични данни на известен брой лица, които работят като доброволци в енория на Протестантската църква на Швеция[1]. СЕО достига до редица важни заключения, като например, приема, че фактът на упоменаване на интернет страница на различни лица и тяхното идентифициране по име или по друг начин, например чрез посочването на техния телефонен номер, или на информация относно техните условия на труд и хобита, **съставлява „пълна или частична обработка на лични данни с автоматизирани средства"** по смисъла на член 3, параграф 1 от Директива 95/46/ЕО. Такова обработване на лични данни **не се обхваща от никое от изключенията** в член 3, параграф 2, т.е. случаите по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната и при дейности на държавата в областта на наказателното право**.** Упоменаването на факта, че лице е наранило своя крак и е на половин работен ден от медицински съображения, представлява **специални лични данни** относно здравето по смисъла на член 8, параграф 1. Не е налице **„предаване (на данни) на трета страна"** по смисъла на член 25 от Директива 95/46/ЕО, когато лице в държава-членка качи лични данни на интернет страница, която се съхранява при неговия hosting provider, който е установен в тази държава или в друга държава-членка, като така прави тези данни достъпни за всеки, който се свърже с интернет, включително хора в трета страна.

По обединени дела C-465/00, C-138/01 и C-139/01 ***Rechnungshof*** с предмет три преюдициални запитвания[2], СЕО приема, че разпоредбата на Член 6, параграф 1, буква в и член 7, букви в и д от Директива 95/46/ЕО не се противопоставят на национална регламентация, при условие че бъде установено, че широкото огласяване не само на размера на годишните доходи, когато те надвишават определен таван, на лица, които са служители на структури, подчинени на контрола на Rechnungshof, но също и на имената на тези, които получават упоменатите доходи, е необходимо и съобразено с целта за добро управление на публичните финанси, което препращащите юрисдикции следва да проверят. Цитираните разпоредби от Директива 95/46/ЕО са директно приложими и в това отношение на тях може да се позовава частно лице пред националните юрисдикции, за да отклони прилагането на норми от вътрешното

[1] Case C-101/01 Bodil Linqvist, решение на СЕО от 6 ноември 2003 г.

[2] Cases C-465/00, C-138/01 и C-139/01 Rechnungshof, решение от 20 май 2003 г.

право, които противоречат на тези разпоредби.

4. Европейският надзорен орган по защита на данните[1] – един от най-новите органи на съюза

Включването на фигурата на Европейския надзорен орган по защита на данните към органите на Европейския съюз се основава на разпоредбата на чл. 286, ДЕО, която предвижда създаването на независим контролен орган, отговорен за контрола на обработката и движението на личните данни в рамките на ЕС, а също така на 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 тези данни[2]; на Решение 1247/2002/ЕО от 1 юли 2002 г. относно статута и общите условия, регулиращи изпълнението на задълженията на Европейския надзорен орган по защита на данните[3] и на Решение 2004/55/ ЕО на Европейския парламент и на Съвета от 22 декември 2003 г. за определяне на независим надзорен орган, предвиден в член 286 от ДЕО[4].

Постът на Европейския надзорен орган по защита на данните (ЕНОЗД) е създаден през 2001 г. Основното му задължение е да контролира всички институции на ЕС да зачитат правото на личен живот на хората. Когато институциите на ЕС обработват личните данни, те трябва да зачитат правото на лицето на личен живот. Европейският супервайзор следи всички аспекти на обработка на личните данни.

"Обработката", както вече бе посочено, обхваща дейности като събирането на информация, записването и съхраняването и, обработката, изпращането и или разкриването на достъпа до нея, както и блокирането, заличаването или унищожаването на данни. На институциите и органите на ЕС не се разрешава да обработват лични данни, разкриващи расовия или етнически произход, политическите убеждения, религиозните или философски вярвания, както и членството в синдикални организации. Те нямат право да обработват данни за здравето или за сексуалния живот, освен ако не са необходими за целите на здравеопазването. Данните се обработват от специалист, положил клетва за опазване на професионалната тайна.

Европейският надзорен орган по защита на данните работи със служителите за защита на данни към всяка институция на ЕС, за да осигури прилагането на правилата за секретност. През 2009 г. г-н Петер Йохан Хъстинкс беше повторно назначен за европейски супервайзор за защита на данните, а г-н Джовани Бутарели замени Хоакин Баио Делгадо на поста помощник-супервайзор.

В посочения по-горе **Регламент (ЕО) 45/2001** от 18 декември 2000 г. е записано, че Член 286 от Договора изисква актовете на Общността относно защитата на лицата по отношение на обработката на лични данни и свободното движение на такива данни да се прилагат спрямо институциите и органите на Общността. Регламент 45/2001 именно е правният инструмент, който да осигурява на физическите лица законно приложими права и създава независим надзорен орган, който да отговаря за наблюдението и контрола на обработката на лични данни от тези институции и органи. Основната задача на Европейския надзорен орган по защита на данните е **да контролира институциите и органите на Общността**, тъй като изрично в преамбюла е записано, че мерките не следва да се прилагат спрямо органи, които са установени извън рамките на

[1] European Data Protection Supervisor (EDPS)
[2] Official Journal L 8, 12.01.2001
[3] Official Journal L 183, 12.07.2002
[4] Official Journal L 12, 17.01.2004

Общността, а Европейският надзорен орган по защита на данните не следва да е компетентен да наблюдава и контролира обработката на лични данни от такива органи. Докато за всяка институция и орган на Общността е въведено задължението да назначи най-малко едно длъжностно лице за защита на данните, което да гарантира вътрешното прилагане на разпоредбите на Регламент 45/2001, както и че операциите по обработка няма вероятност да засегнат неблагоприятно правата и свободите на субектите на данни[1]. Същевременно ЕНОЗД има специфични контролни правомощия по отношение на EURODAC (които позволяват сравнение на пръстови отпечатъци на кондидатстващи за право на убежище) в съответствие с Чл. 20 от Регламента, уреждащ статута на EURODAC[2]. Подобни задачи за Европейския надзорен орган по защита на данните се предвиждат и относно други информационни системи, свързани с Пространството на свобода, сигурност и правосъдие.

Освен изключително важните контролни правомощия Европейският надзорен орган по защита на данните изпълнява и функции на **консултация** и **сътрудничество**. По-специално, институциите и органите на Общността информират Европейския надзорен орган по защита на данните при съставяне на административни мерки във връзка с обработката на лични данни. При приемане на законодателно предложение във връзка със защитата на правата и свободите на лицата по отношение на обработката на лични данни, Комисията провежда консултации с Европейския надзорен орган по защита на данните. Широкото тълкуване на правомощията на Европейския надзорен орган по защита на данните проличава във формулировката на Чл.41, §2 от Регламент 45/2001, където е записано, че той консултира **всички** институции и органи на Общността по **всички** въпроси, касаещи обработката на лични данни. Този подход е потвърден и от СЕО в решенията му по т.нар. PNR-дела[3].

В рамките на задължението за **сътрудничество**, операции по обработка, които поради своето естество, обхват или цели има вероятност да представляват специфични опасности за правата и свободите на субектите на данни, се подлагат на **предварителна проверка** от страна на Европейския надзорен орган по защита на данните.

В съответствие с Чл. 27, §2 такава опасност могат да представляват следните операции:

а) обработка на данни, свързани със здравето и предполагаеми престъпления, престъпления, присъди или мерки за неотклонение;

б) операции по обработка, които са предназначени за оценка на аспекти на личността на субекта на данните, включително неговите/нейните способности, ефективност и поведение;

в) операции по обработка, позволяващи връзки между данни, които се обработват за различни цели и които не са предвидени в националното или общностно законодателство;

г) операции по обработка с цел изключване на лица от право, облага или договор.

Предварителните проверки се извършват от Европейския надзорен орган по защита на данните след получаване на нотификация от съответното длъжностно лице за защита на данните, което в случай на съмнение относно необходимостта от извършване

[1] Чл. 24 от Регламент 45/2001

[2] Council Regulation (EC) No 2725/2000 of 11 Dec. 2000 concerning the establishment of "EURODAC" for the comparison of fingerprints for the effective application of the Dublin Convention, O.J. 2000, L 316/1.

[3] Решение на СЕО от 30 май 2006 г. по обединени дела C-317 & 318/04, *European Parliament* v. Council and Commission.

на предварителна проверка се консултира с Европейския надзорен орган по защита на данните.

Европейският надзорен орган по защита на данните представя становището си в срок от два месеца след получаване на нотификацията. Когато сложността на въпроса го изисква, този срок може с решение на Европейския надзорен орган по защита на данните да се удължи с още два месеца. При отсъствие на представено становище до края на двумесечния или евентуално удължен срок, становището се счита за положително.

Изключително важни с оглед защитата на основните човешки права са предвидените в Чл. 32 на Регламент 45/2001 възможности за **съдебна защита**. Всяко физическо лице, без да се засягат останалите средства за съдебна защита, може да подаде жалба до Европейския надзорен орган, ако счита, че са нарушени правата му по Член 286 от ДЕО, вследствие на обработка на негови лични данни от институция или орган на Общността. При отсъствие на отговор от Европейския надзорен орган в срок от шест месеца, жалбата се счита за отхвърлена. Решенията на Европейския надзорен орган по защита на данните могат се обжалват пред Съда на Европейските общности. Всяко лице, което е претърпяло вреда в резултат на незаконна операция по обработка или всякакво несъвместимо с настоящия регламент действие, има право на обезщетение за нанесените вреди в съответствие с Чл. 288 ДЕО.

Като обобщение, в случай, че субект на данните счита, че европейска институция или орган е обработвала личните му данни в противоречие с Регламент 45/2001, той може да предприеме едно от следните действия:

- да сезира Първоинстанционния съд да отмени атакуваното решение в срок от два месеца от публикуването на решението или от съобщаването му на ищеца или при липса на такова – от деня, вкойто ищецът е узнал за него (Чл. 230, ДЕО §4 и 5);
- да подаде жалба до Европейския омбудсман срещу действие, представляващо лошо администриране в двегодишен срок (Чл. 2, пар. 2 от Статута на Европейския омбудсман);
- да подаде жалба до Европейския надзорен орган, ако счита, че са нарушени правата му вследствие на обработка на негови лични данни от институция или орган на Общността (Чл. 32, §2 от Регламент 45/2001). Впоследствие няма пречка да бъде сезиран ПИС при условията, посчени по-горе или да бъде подадена жалба до Омбудсмана;
- субектът на данните може да се обърне към длъжностното лице за защита на данните, след което няма пречка да се премине към едно от горепосочените възможни средства за защита;
- субектът на данните може да се обърне към самата европейска институция или орган, след което няма пречка да се премине към едно от горепосочените възможни средства за защита.

Както е известно, Европейският надзорен орган по защита на данните не попада в списъка на институциите, изброени в Чл. 7, ДЕО, следователно от чисто формална гледна точка той не би могъл да бъде окачествен като “институция” на Общността. Внимателният прочит на Чл. 47 от Регламент 45/2001, сочи, че Европейският надзорен орган по защита на данните може:

а) да дава съвети на субектите на данни при упражняване на техните права;

б) да сезира контролиращия орган при твърдение за нарушение на разпоредбите, уреждащи обработката на лични данни, и при необходимост да отправя предложения за изправяне на това нарушение и за подобряване на защитата на субектите на данни;

в) да разпорежда удовлетворяването на молби за упражняване на определени права във връзка с данни, когато такива молби са били отхвърлени в нарушение на разпоредбите на членове от 13 до 19;

г) да отправя предупреждения и мъмрене до контролиращия орган;

д) да разпорежда коригиране, блокиране, заличаване или унищожаване на всички данни, които са били обработени в нарушение на разпоредбите, уреждащи обработката на лични данни, както и уведомяване за тези действия на трети страни, пред които са били разкрити данните;

е) да налага временна или постоянна забрана за обработка;

ж) да сезира съответната институция или орган на Общността, а при необходимост и Европейския парламент, Съвета и Комисията;

з) да сезира Съда на Европейските общности при предвидените в Договора условия;

и) да взема участие в заведени пред Съда на Европейските общности дела.

Освен това, Европейският надзорен орган по защита на данните има право да получава от институция или орган на Общността цялата информация, която е необходима за неговите разследвания, както и при основателни съмнения да има достъп до всички помещения, в които институция или орган на Общността осъществява своята дейност. В допълнение, неговият бюджет фигурира в отделна позиция в раздел VIII на общия бюджет на Европейския съюз, а по въпроси, касаещи персонала, Европейският надзорен орган по защита на данните има същия статут, както институциите на Общността. От гореизложеното е видно, че макар ЕНОЗД да е само орган, обемът на неговите правомощия го доближава в значителна степен до статута на институциите на Европейския съюз. Особено важно е да бъде отбелязана привилегированата позиция, която Регламент 45/2001 създава за Европейския надзорен орган по защита на данните по отношение на участието му в съдебните производства (вж. букви „з" и „и" на Чл. 47, § 1). На практика с разпоредбата на Чл. 47, §1 на Регламент 45/2001 са постигнати същите правни последици, предвидени по отношение на европейските институции и Европейската централна банка в Чл. 230, ДЕО[1]. Очевидно, за Съда на Европейските общности формалният статут на институция не е решаващ за гарантирането на възможността да бъде сезиран от Европейския надзорен орган по защита на данните.

В правната литература неведнъж е поставян въпросът за точния статут на Европейския надзорен орган по защита на данните, без обаче да е получаван ясен отговор. Изследователите по-скоро са склонни да приемат, че това е *sui generis* орган; той не е нито агенция, нито регулаторен орган, нито омбудсман, нито съдебен орган[2]. Европейският надзорен орган по защита на данните определено не може да бъде определен като агенция, тъй като агенциите обикновено притежават контролни правомощия по отношение на вътрешния пазар, а не по отношение на европейските институции. В правото на Общността понятието „регулаторен орган" се свързва с либерализирането и конкурентността в определени сектори на вътрешния пазар, които са били монополизирани, като телекомуникациите и енергетиката.

---

[1] Чл. 230, ДЕО §2 и 3 гласят съответно:

Съдът е компетентен да правораздава по дела, заведени от държава членка, Европейския парламент, Съвета или Комисията на основание на некомпетентност, съществено процедурно нарушение, нарушение на този договор или на норма по неговото прилагане или злоупотреба с власт.

Съдът е компетентен да правораздава при същите условия по дела, заведени от Сметната палата и от ЕЦБ за защита не техните правамащия.

[2] HIJMANS, Hielke THE EUROPEAN DATA PROTECTION SUPERVISOR: THE INSTITUTIONS OF THE EC CONTROLLED BY AN INDEPENDENT AUTHORITY, *Common Market Law Review, 43, pp.* 1313–1342, 2006.

Възможността пред Европейския надзорен орган по защита на данните да се подават жалби го доближава до статута на омбудсмана, но както изтъкват някои автори, този орган не е алтернатива на съдебната защита на индивидите, а е част от нея, включително и посредством правото му да сезира Съда на Европейските общности. Европейският надзорен орган по защита на данните едва ли може да бъде характеризиран като съдебен орган, въпреки, че се доближава до условията, формулирани по делото *Dorsch Consult*[1]. Там е записано, че за да определи дали органът, отправил преюдициалното запитване е юрисдикция по смисъла на Чл. 234, ДЕО, СЕО взема предвид редица фактори, между които дали съответният орган е създаден по законов ред, дали е постоянен, дали юрисдикцията му е задължителна, дали процудурата е *inter partes*, дали спазва върховенството на закона и дали е независим. Точно правомощията на Европейския надзорен орган по защита на данните да сезира СЕО и да взема участие в заведени пред Съда дела обаче са доказателство за това, че той не е чисто съдебен орган, тъй като един съдебен орган по дефиниция не би могъл да се намесва в производството пред друг правораздавателен орган, нито да го сезира като страна по дадено дело. Европейският надзорен орган по защита на данните в съответствие с Чл. 47 от Регламент 45/2001 може да се явява в няколко качества пред СЕО: да се намесва в заведени пред СЕО дела, да сезира Съда и да бъде ответник по дела, заведени пред СЕО. Досегашната практика свидетелства единствено за случаи на намеса/участие в заведени пред Съда дела. Така например, със свое решение от 17 март 2005 г. по т.нар. PNR - дела[2] СЕО позволява на Европейския надзорен орган да се намеси в подкрепа на позицията на Европейския парламент, а през 2006 г и по делото, свързано с Директива 2006/24/ЕО на Европейския парламент и на Съвета за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи[3].

В допълнение към всичко казано дотук, няма никакви изисквания Европейският надзорен орган по защита на данните да бъде съдия или юрист, напротив той трябва да изпълнява и редица задачи от друго естество, но неговата независимост не трябва да подлежи на съмнение и той се избира между лица, за които е признато, че притежават необходимите опит и умения, за да изпълняват функциите на ЕНОЗД.

5. Защитата на личните данни според Договора от Лисабон

Накрая, едва ли е възможно настоящото изложение да претендира за изчерпателност, без да се посочи уредбата на защитата на личните данни в съответствие с Договора от Лисабон, подписан на 13 декември 2007 г. В съответствие с **Чл. 16 от Договора за функционирането на Европейския съюз**:

Всеки има право на защита на личните му данни.

Европейският парламент и Съветът, като действат в съответствие с обикновената законодателна процедура, определят правилата за защита на физическите лица по отношение на обработката на личните данни от страна на институциите, органите, службите и

[1] Case C-54/96, *Dorsch Consult*, [1997] ECR I-4961, решение от 17 септември 1997 г.

[2] Решение на СЕО от 17 март 2005 г. по обединени дела C-317 & 318/04, *European Parliament* v. Council and Commission.

[3] C-301/06 Ирландия срещу Европейския парламент и Съвета на Европейския съюз

агенциите на Съюза, както и от държавите членки при извършване на дейности, които попадат в обхвата на правото на Съюза, както и по отношение на тези данни. Спазването на тези правила е предмет на контрол от страна на независими органи.

Правилата, приети въз основа на настоящия член, не засягат специфичните правила, предвидени в чл. 39 от Договора за Европейския съюз.

Член 39 от ДЕС гласи следното:

В съответствие с Чл.16 от Договора за функционирането на Европейския съюз и чрез дерогация от §2 от него, Съветът приема решение, с което се определят правилата за защита на физическите лица по отношение на обработката на личните данни от държавите членки при извършване на дейности, попадащи в обхвата на настоящата глава, както и по отношение на свободното движение на тези данни. Спазването на тези правила е предмет на контрол от страна на независими органи.

Безспорно, редица са положителните моменти в новата правна уредба. На първо място, самият факт, че защитата на личните данни е припозната като основно човешко право в първичното законодателство на Европейския съюз, е от изключително значение. Освен това, усещане за повишена легитимност внася и текстът на Чл. 16, ДФЕС, според който правилата за защита на индивидите по отношение на обработката на личните данни се предвижда да се приемат в съответствие с обикновената законодателна процедура – т.е. в съответствие с процедурата по съвместно вземане на решение при по-активното участие на Европейския парламент. Фактът, че по силата на Чл.6, ДЕС Европейският съюз ще се присъедини към Европейската конвенция за защита правата на човека и основните свободи (ЕКПЧ) също има положително влияние, тъй като основните права, както са гарантирани от ЕКПЧ и както произтичат от общите конституционни традиции на държавите членки, се превръщат в част от правото на Съюза в качеството им на общи принципи. В **Декларация № 20**, приложена към Заключителния акт на междуправителствената конференция, се посочва, че при всяко приемане на правила за защита на личните данни въз основа на Чл. 16 от ДФЕС, които биха могли да окажат пряко влияние върху **националната сигурност**, това следва надлежно да се вземе предвид. А в **Декларация № 21** е записано, че специфични правила за защита на личните данни и за свободно движение на тези данни **в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество** въз основа на Чл. 16 ДФЕС могат да се окажат необходими поради специфичното естество на тези области.

6. Защита на личните данни в пространството на свобода, сигурност и правосъдие

Необходимо е да се направи уточнението, че проблемите, свързани със събирането и обработката на личните данни от правоприлагащите национални органи остава извън обхвата на Директива 46/95/ЕО. Член3, §2 от Директивата гласи:

*Настоящата директива **не се прилага** за обработването на лични данни:*

*при извършване на дейности, извън приложното поле на правото на Общността, например дейностите, предвидени в Дял V и Дял VI от Договора за Европейския съюз, и във всички случаи при дейности по **обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност** (включително икономическото благосъстояние на държавата, когато процесът на обработка е свързан с държавната сигурност) и **при***

дейности на държавата в областта на наказателното право.

През 2006 г. в своето становище за обмяна на информация въз основа на принципа на наличност[1] Европейският надзорен орган подчертава неотложната необходимост за изграждане на правна рамка за защита на личните данни впространството на свобода, сигурност и правосъдие, включително т.нар ШИС–II (Шенгенска информационна система–II) и предложенията, отнасящи се до Визовата информационна система. Представители на правната теория дори твърдят, че „когато Европейският съюз въведе правила за защитата на данните в полицейския сектор, те, в условията на глобализацията, ще отговарят на твърде ниски стандарти"[2]. Работата на Европейския съюз през последните пет години се основава на т.нар. „принцип на наличност", при който правоприлагащ орган от една държава-членка по време на изпълнение на служебните си задължения може да получи информация, когато такава е налична, от друга държава-членка.

През 2008 г. вече е прието Рамково решение на Съвета за защита на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси[3], в което са дадени допълнителни гаранции по отношение на обработката на личните данни в третия стълб. Проучване на общественото мнение през същата година, извършено от Евробарометър показва, че въпреки, че европейските граждани като цяло (64%) са загрижени за сигурността на личните им данни, но едва една трета (29%) знаят, специфични данни, като расова принадлежност или етнически произход, се ползват с особена защита[4].

В съобщение на Комисията от 10 юни 2009[5], даващо оценка на състоянието в пространството на свобода, сигурност и правосъдие от 2005 г. досега, е записано, че ЕС насърчава спазването на правото на защита на личните данни и на личния живот, като в същото време признава необходимостта правоприлагащите органи да обменят съответната информация в борбата срещу тероризма и престъпността. Насърчава се развитието на технологии за подобряване на защитата на личния живот[6] с цел създаването на информационни системи, които свеждат до минимум събирането и използването на лични данни.

Пакет от предложения на Комисията от 2008 г. определя новите етапи по пътя към интегрирано управление на границите: система за влизане/излизане[7], която подава автоматични известия, когато дадено лице пресрочи визата си, система за наблюдение на южните и източните външни граници на ЕС (известна като EUROSUR)[8] и оценка и бъдещо развитие на FRONTEX[9]. За целите на сигурността бяха определени условията за достъп до

---

[1] Opinion of EDPS of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005)490 final), OJ C 116, 17.05.2006, p. 8

[2] Hayes, Ben "A Failure to regulate: data protection and ethnic profiling in the police sector in Europe", in "Ethnic profiling by Police in Europe", ed. Open Society Justice Initiative, 2005 Вж. също и Eleni Kosta, Fanny Coudert & Prof. Jos Dumortier "Data Protection in third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive" BILETA 2007 Annual Conference, Hertfordshire, 16-17 April

[3] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

[4] The Gallup Organization (2008), "Data Protection in the European Union. Citzens' perceptions", Eurobarometer, p.5

[5] COM(2009) 263 окончателен

[6] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)', COM(2007) 228 final. e), OJ L 105, 13.4.2006, p. 1.

[7] 'Preparing the next steps in border management in the Europe an Union', COM(2008) 69 final.

[8] 'Examining the creation of a European border surveillance system (EUROSUR)', COM(2008) 68 final.

[9] 'Report on the evaluation and future development of the FRONTE

ВИС[1], която съдържа информация за всички лица, кандидатстващи за краткосрочен престой в ЕС.

Обменът на информация и на разузнавателни сведения бе опростен. Включването на **Конвенцията** от Прюм в законодателството на ЕС[2] осигури непряк достъп до базите данни на държавите-членки за пръстови отпечатъци и ДНК информация и пряк, контролиран достъп до данните за регистрация на превозни средства. Това може значително да подобри полицейското сътрудничество в рамките на ЕС, като предоставя на съответните органи информация за това какви данни са налични. Инициативата изисква събиране, съхранение и обмен на файлове с ДНК анализ и пръстови отпечатъци. Използването на биометрични данни при правоприлагането обаче води до специфични рискове за субектите на данни и изисква допълнителни предпазни мерки, за да се защитят техните права.

Следва да се има предвид, че ШИС I и II, EURODAC, ВИС, както и информационните системи на Европол и Евроюст, са централизирани европейски системи. Така например, Шенгенската информационна система представлява обща база данни, създадена и използвана от държавите, участнички в Шенгенското пространство. ШИС се състои от централна система в Страсбург и свързани с нея системи с национални данни на държавите-членки, които се използват за въвеждане на данни и извършване на справки. Приема се, че към момента ШИС съдържа близо 15 милиона сигнали, въвеждани от участващите държави. ШИС не е централен регистър на лицата, живеещи на територията на ЕС/Шенген, а съдържа данни (сигнали) за определени издирвани/контролирани лица и стоки с оглед запазването на Шенгенското пространство като територия на свобода, сигурност и правосъдие.

Всяка национална ШИС предоставя чрез автоматизирано търсене достъп на компетентните власти и органи до сигнали, касаещи издирвани/контролирани лица или стоки, с цел изпълнение на задачи в областта на граничния контрол, издаването на визи, разрешения за пребиваване, свидетелства за управление на МПС, митническия режим, полицейските и съдебните дейности, както и за защита на обществения ред и националната и европейска сигурност[3].

На заседание на Съвета "Правосъдие и вътрешни работи", проведен в

me, OJ L 210, 6.8.2008, p. 12.

[1] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 386, 29.12.2006, p. 89.

[2] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1 and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[3] Лицата, чиито данни се въвеждат в ШИС, са:
1. Лица, за които има молба за арест по силата на Европейска заповед за арест или екстрадиция;
2. Чужденци, на които е отказано влизане на територията на държавата;
3. Безследно изчезнали лица или лица, които в интерес на тяхната сигурност или за предотвратяване на заплаха е необходимо да бъдат поставени временно под полицейска охрана по молба на компетентен орган или компетентен съд на договарящата страна;
4. Данните за свидетели и лица, които са призовани в съдебен процес във връзка с наказателно производство, за да свидетелстват за деяния, за които са преследвани или за лица, на които следва да се връчи присъда или призовка за явяване с цел изтърпяване на наказание, свързано с лишаване от свобода;
5. Данните за лица за извършване на скрито наблюдение и специален контрол.
Министерство на вътрешните работи на Република България е централният орган, който ще администрира и отговаря за експлоатацията и функционирането на националната Шенгенска информационна система. МВР е и ведомството, което ще контролира въвеждането и обработката на личните данни в ШИС.

Люксембург, на 4 и 5 юни 2009 г., България (заедно с Румъния), в специално изявление, декларира намерението си да се присъедини към ШИС-I+ чрез SISone4ALL (ШИС "Една за всички"), като едновременно с това продължи подготовката за преминаването от ШИС-I+ към ШИС-II заедно с останалите държави-членки.

Въпреки, че всички посочени в изложението информационни системи са част от пространството на свобода, сигурност и правосъдие, някои от тях като ШИС и EURODAC са предмет на първия наднационален стълб, докато информационните системи, свързани с полицейското и правосъдно сътрудничество, спадат към обхвата на третия стълб. Това предполага различия в начина на вземане на решения, което се очаква да бъде преодоляно с влизането в сила на Договора от Лисабон и отпадането на стълбовата архитектура на Европейския съюз.

Друг съществуващ проблем са съществуващите различия на субектите с право на достъп до отделните информационни системи. По отношение на някои бази данни и механизми е възможен достъпът и обмяната на информация (при определени условия) с трети страни или международни организации. Държавите членки имат право да определят и съобщят на Секретариата на Съвета своите компетенти органи, които ще имат право на достъп до информационните баз данни. Практиката на отделните държави обаче се различава значително – т. напр. Латвия посочва в списъка на компетентните органи с право на достъп дори капитаните на плавателни съдове под латвийски флаг.

Различията по отношение на участващите държави най-ярко проличават на примера на ШИС. Исландия и Норвегия са страни по ШИС[1], докато България, Румъния и Кипър все още не са участнички по споразумението, а Великобритания и Ирландия, които също не са част от Шенгенското пространство, имат разрешен достъп до полицейското и наказателноправното съдържание на ШИС. **През м. декември 2008 г. и** Швейцария също се присъедини към Шенгенското пространство. Очаква се в скоро време, след привеждането на своите компютърни системи съобразно изискванията на ШИС, Лихтенщайн също да се присъедини към Шенген. По отношение на ШИС решенията се приемат в съответствие с процедурата по съвместно вземане на решения, с участието на Съвета и Европейския парламент. И докато страните, нечленуващи в ЕС, са ангажирани в работата на Съвета посредством т.нар. смесени комитети, то в работата на Европейския парламент Исландия и Норвегия не са представени. Великобритания и Ирландия участват в работата на Европейския парламент, независимо от факта, че правителствата им са лишени от правото на глас в Съвета на ЕС поради неучастието им в общата визова и миграционна политика[2].

7. Преглед на съдебната практика относно защитата на личните данни

А. Делото *Huber* - C-524/06

Интересна е практиката на СЕО по въпроси, свързани със защитата на личните данни. Съдът е имал възможност да се произнесе в решението си по делото *Huber*[3], като постановява:

[1] По съображения за запазването на Северния паспортен съюз чиито държави членки станаха част от Шенгенското пространство, с изкл. на Фарьорските острови.

[2] Geyer, Florian "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", Challenge: Liberty and Security Research Paper No 8, May 2008

[3] Решение на СЕО от 16 декември 2008 г. по дело C-524/06 (преюдициално запитване от Berverwaltungsgericht für das Land Nordrhein-Westfalen).

При всяко положение съхранението и обработването на поименни лични данни в рамките на регистър като централния регистър за чужденците за статистически цели не могат да се приемат за необходими по смисъла на член 7, буква "д" от Директива 95/46. Член 12, параграф 1 ДЕО следва да се тълкува в смисъл, че не допуска с оглед на целта за борба с престъпността държава-членка да създаде система за обработване на лични данни специално за гражданите на Съюза, които не са граждани на тази държава-членка.

В своето заключение по посоченото дело генералният адвокат П. Мадуро дори отива по-далеч, твърдейки, че национална база данни, съдържаща информация изключително за граждани на Съюза и на трети страни, но не и на собствени граждани на държавата членка, може да бъде окачествена като дискриминационна и в нарушение на Общностното право. "В действителност, правоприлагането и борбата с престъпността по принцип са легитимни основания в правото на Общността. Това, което държавата–членка не може да прави, е избирателно да ги прилага срещу граждани на ЕС, живеещи на нейната територия, но не и срещу своите собствени граждани. Ако наличието на централен регистър е от изключително значение за политиката на държавата членка, той трябва да включва всяко лице, живеещо на съответната територия, без оглед на неговата националност. Не е допустимо, компетентните национални органи да заявяват, че борбата срещу престъпността изисква систематична обработка на лични данни на граждани на ЕС извън собствените граждани. Предположението, че тези граждани биха представлявали по-голяма заплаха за сигурността и са по-склонни да извършват престъпления в сравнение със собствените граждани, също така е напълно неприемливо."[1]

Б. Съдебна практика на СЕО и съдебните органи на държавите членки по повод Директива 2006/24/ЕО

Съдебните органи на държавите членки също проявяват активност, в частност Конституционният съд на Федерална република Германия. В поредица от решения през м. февруари и марта 2008 г. Съдът в Карлсруе ограничава или отменя действието на някои особено чувствителни по отношение защитата на личните данни закони[2]. На 27 февруари 2008 г. Конституционният съд обявява за противоконституционен новият закон на провинция Северен Рейн-Вестфалия, който позволява проследяване на персонални компютри и ползването на Интернет услуги; на 11 март той отменя разпоредбите в Есен и Шлезвиг-Холщайн, даващи възможност за автоматична идентификация и пазене на номерата на автомобили, получени от видеокамери за контрол на движението по пътищата, както и тяхното сравняване с други полицейски бази данни; в същия ден Конституционният съд временно отменя някои положения на новия федерален закон, който въвежда в действие Директива 2006/24/ЕО[3].

Както е известно, с Директива 2006/24/ЕО бяха предвидени нови ограничения с оглед гарантирането, че "данните са достъпни за разследването, разкриването и преследването на сериозни престъпления, както те са определени в националното право на всяка държава". Създадени бяха задължения за запазване на т.нар.

[1] Заключение на Генерален адвокат П. Мадуро от 3 април 2008 г. по дело C-524/06 Heinz Huber v. Bundesrepublik Deutschland.

[2] 1 BvR 370/07; 1 BvR 2074/05; 1 BvR 256/08.

[3] Директива 2006/24/ЕО на Европейския парламент и 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.

трафични данни - данни, необходими за проследяване и идентифициране на източника на съобщението, на местоназначението на съобщението, датата, времето и продължителността на съобщението, вида съобщение и съобщителното оборудване на ползвателите. Приемането на директивата беше трудно. През 2004 г. Франция, Германия, Швеция и Великобритания предложиха рамково решение за запазване на данните, но не беше постигнато единодушие сред държавите членки. Затова беше предложена директива, която можеше да бъде приета (както и стана) без единодушие. Ирландия обаче атакува Директивата пред Съда на ЕО. В иска се твърдеше, че директивата няма правно основание в договорите, защото директивите се използват само за хармонизиране на националните мерки в полза на укрепването на единния вътешен пазар, докато тук става дума за борба с тероризма.

В решението си по дело С-301/06[1] Съдът на Европейските общности приема, че Директивата има годно правно основание, тъй като урежда само запазването на данните (което подлежи на хармонизиране), без да включва репресивна намеса на властите (дейност по третия стълб):

Тази директива не хармонизира нито въпроса за достъпа до данните от страна на компетентните национални органи в областта на наказателното преследване, нито този относно използването и обмена на тези данни между посочените органи. Тези въпроси, които по принцип попадат в обхвата на дял VI от Договора за ЕС, са изключени от обхвата на разпоредбите на Директива 2006/24.

Съдът не приема твърдението на Ирландия, подкрепяна от Словакия, според което: "*Директива 2006/24 не може да се основава на Член 95 ДЕО, тъй като нейният „център на тежестта" не засяга функционирането на вътрешния пазар, а има за единствена или поне за главна цел разследването, разкриването и преследването на престъпления*."

Важно е да се отбележи, че Съдът изрично указва в решението, че "*подадената от Ирландия жалба се отнася **само до избора на правно основание**, а не до евентуално нарушение на основните права, което произтича от съдържащата се в Директива 2006/24/ЕО намеса в упражняването на правото на лична неприкосновеност.*" Този въпрос не е предмет на разглеждане в съдебното решение.

Директивата предизвиква съпротива и по време на транспонирането ѝ в национални мерки, включително и в България. Наредба № 40 на МВР от м. януари 2008 година привежда в българското законодателство горепосочената Директива. Според нея т.нар. предприятия, предоставящи обществени електронни мрежи и услуги, са длъжни да запазват данните за всяко мобилно повикване: дата и час, място и страни по комуникацията, както и за всяко електронно съобщение (чрез интернет). Достъп до данните трябва да имат МВР, органите на досъдебното производство и съдът – за целите на наказателното производство, както и службите за сигурност и обществен ред – за целите на националната сигурност. На 11 декември 2008 г. Върховният административен съд на Република България в петчленен състав като касационна инстанция се произнесе по жалбата срещу Наредба № 40 за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за нуждите на националната сигурност и за разкриване на предстъпления. Решението на ВАС приема аргументите, че в Наредба № 40

[1] Дело С-301/06 - Ирландия срещу Европейския парламент и Съвета.

не са предвидени гаранции срещу злоупотребата с данните при предоставянето им на държавните органи и отменя изцяло разпоредбата на Чл. 5 на Наредбата, в който се регламентира възможността за предоставяне на достъп до събраните от операторите данни за потребителите. ВАС приема, че нормата на Чл. 5 не поставя никакви ограничения по отношение данните, до които се разрешава достъпът чрез компютърен терминал, а изразът "за нуждите на оперативно-издирвателната дейност" е твърде общ и не дава гаранции за спазване чл. 32, ал.1 от Конституцията на Република България, че личният живот на гражданите е неприкосновен. Така формулираният текст не поставя условия, препятстващи злоупотреба с възможността да се нарушават конституционно гарантирани права на гражданите. Не е предвидено препращане към специалните закони Наказателно-процесуален кодекс, Закон за специалните разузнавателни средства, Закон за защита на личните данни, в които са конкретизирани предпоставките за допускане достъп до определени данни, свързани с личния живот и личните данни на отделната личност. Върховният административен съд счита, че текстът на чл.5 от Наредба № 40/2008 г. противоречи на разпоредбата на чл.8 от ЕКПЧ. Също така липсва яснота по отношение гарантиране правото на защита срещу незаконна намеса в личния и семейния живот на гражданите, което обуславя противоречието на нормата с чл.8 от ЕКПЧ, с текстове от Директива 2006/24/ЕО, с чл.32 и чл.34 от Конституцията на Република България.

В проведените през м. юни 2009 г. избори за европейски парламент, Директива 2006/24 отново се оказа в центъра на вниманието чрез позицията на шведската "пиратска" партия (успяла да излъчи един евродепутат), която се обяви против Директивата и в защита на личното пространство на гражданите. Буквално дни преди изборите (в края на м. май) Европейската комисия заведе дело срещу Швеция за невъвеждане в срок на Директива 2006/24. Някои шведски политици съзряха в това възможност да поставят под въпрос съвместимостта на Директивата с Европейската конвенция за правата на човека. Те се съмняват доколко запазването на данни е съвместимо с нуждите на едно демократично общество и подчертават факта, че и други страни (Австрия, Гърция, Ирландия, Холандия и Полша) също не бързат да изостават с въвеждането на Директивата.

В. Практика на ЕСПЧ

Новите тенденции, свързани с ограничаването на съхранението на пръстови отпечатъци на индивидите, могат да бъдат откроени в решението на ЕСПЧ в Страсбург по делото *S.& Marper v. the United Kingdom*[1]. Европейският съд по правата на човека ограничава правото на европейските правителства да съхраняват неограничено генетичен материал, генетични профили и пръстови отпечатъци на лицата, обвинени в извършване на престъпление, но неосъдени впоследствие. Голямото отделение (*Grand Chamber*) на ЕСПЧ, състоящо се от 17 съдии, с единодушно решение от 4 декември 2008 г. заключава, че разпоредбите на Закона за полицията и доказателствата в наказателното производство (*Police and Criminal Evidence Act*) на Великобритания, които позволяват неограничено във времето съхранение на ДНК профили, клетъчни проби и пръстови отпечатъци, нарушават разпоредбата на Чл. 8 на Конвенцията за защита правата на човека и основните

[1] S. and Marper v. the United Kingdom, Judgment of 4 December 2008. Жалбоподателите С. и Майкъл Марпър са британски граждани, родени съответно през 1989 и 1963 г., и живущи в Шефилд, Великобритания. Случаят касае съхранението на пръстови отпечатъци, клетъчни проби и ДНК профили на жалбоподателите от страна на властите след прекратяване на наказателен процес срещу тях и сваляне на обвинението.

свободи, касаеща неприкосновеността на личния живот. Съдът още подчертава, че съхраняването на данни на неосъдени лица може да нанесе особени вреди в случаите на непълнолетни, предвид значението на бъдещото им развитие и интеграцията им в обществото. Такъв е случаят на първия жалбоподател. Според ЕСПЧ е недопустимо посочените лични данни да се съхраняват неограничено без оглед на обстоятелствата, дали лицето е оправдано, дали е непълнолетно, малолетно и др. ЕСПЧ още изтъква, че нивото на вмешателство в личния живот може да бъде различно, като съхраняването на данни от клетъчни проби е особено обезпокоително, взимайки предвид факта, че те са най-богати по съдържание на генетична и здравна информация.

В заключение Съдът смята, че всеобхватният и неограничен характер на властта да се запазват пръстови отпечатъци, клетъчни проби и ДНК профили на лицата, заподозрени, но неосъдени, не създава необходимия баланс между конкуриращи се частни и обществени интереси и че Великобритания е престъпила всякакви приемливи граници в това отношение. Следователно, събирането и съхранението на данни в случая представлява непропорционално вмешателство в личния живот на жалбоподателя и не може да бъде считано за необходимо в демократичното общество.

Интересен е фактът, че преди решението на ЕСПЧ по делото *Marper* в България Комисията за защита на личните данни (КЗЛД) в две свои решения[1] е установила нарушения от страна на органите на МВР при съхраняване на данни от полицейски регистрации. И в двата случая полицейската регистрация[2] не е била снета, въпреки че е отпаднало основанието за нейното съхраняване. И в двете свои решения КЗЛД счита обработването на лични данни от страна на МВР за незаконосъобразно и е задължила МВР да унищожи полицейските регистрации на жалбоподателите.

В заключение, авторът си позволява да отбележи изключителната активност както на европейските институции и органи, така и на държавите членки по проблеми, свързани ссъс защитата на личните данни. Внесени са и редица предложения за нови мерки, които да бъдат предприети, касаещи базите данни, видовете информация, продължителността на нейното съхраняване, начините за нейното предоставяне. Но основното, за което би следвало да се държи сметка е как тази архитектура на виртуална сигурност се отразява върху основните човешки права и върху демократичността на държавите членки.

[1] Решение № 8 от 21.03.2007 г. и Решение № 16 от 05.07.2006 г.

[2] Полицейската регистрация представлява вид обработване на лични данни за определени лица - български и чужди граждани и лица без гражданство, срещу които е започнало наказателно преследване за извършено умишлено престъпление от общ характер. Номерът от полицейския регистър, с който е осъществена регистрацията, се пренася върху изготвените карта за регистрация и дактилоскопна карта. Редът и условията за извършване на полицейска регистрация се определя с Наредба за реда за извършване на полицейска регистрация, издадена от МВР, в сила от 29.01.2004 г.