



Тематичен фиш

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Правото на защита на личните данни е основно право, чието спазване е важна цел за Европейския съюз.

То е закрепено в Харта на основните права на Европейския съюз (наричана по-нататък „Хартата“), член 8 от която гласи:

„1. Всеки има право на защита на неговите лични данни.

2. Тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им.

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

Това основно право е и тясно свързано с правото на зачитане на личния и семейния живот, закрепено в член 7 от Хартата.

Правото на защита на личните данни е предвидено и в член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС), разпоредбата, която замени по този въпрос член 286 ЕО.

Що се отнася до вторичното право, от средата на 90-те години Европейската общност започва да въвежда различни актове за гарантиране на защитата на личните данни. В това отношение Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни¹, която е приета на основание член 100А ЕО, е основният правен акт на Съюза в тази област. Тя установява общите условия за законност на обработването на лични данни, както и правата на съответните лица, и в частност предвижда създаването на независими надзорни органи в държавите членки.

¹ Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10), консолидиран текст от 20.11.2003 г., отменена, считано от 25 май 2018 г. (вж. бележка под линия 5).

Впоследствие към Директива 95/46/ЕО се добавя Директива 2002/58/ЕО², която хармонизира законодателните разпоредби на държавите членки относно защитата на правото на личен живот, що се отнася в частност до обработването на лични данни в сектора на електронните съобщения³.

Освен това в пространството на свобода, сигурност и правосъдие (старите членове 30 и 31 ДЕС) защитата на личните данни в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси е уредена с Рамково решение 2008/977/ПВР⁴ (до май 2018 г.).

Неотдавна Европейският съюз изготви нова обща правна рамка в тази област. За целта през 2016 г. бяха приети Регламент (ЕС) 2016/679⁵ относно защитата на данните, който отменя Директива 95/46/ЕО и ще е пряко приложим от 25 май 2018 г., както и Директива (ЕС) 2016/680⁶ за защита на данните в наказателната област, която отменя Рамково решение 2008/977/ПВР и трябва да бъде транспонирана в държавите членки до 6 май 2018 г.

Накрая, защитата на личните данни, обработвани от институциите и органите на ЕС, е гарантирана с Регламент (ЕО) № 45/2001⁷. Въз основа на този регламент през 2004 г. бе създаден Европейският надзорен орган по защита на данните. През януари 2017 г. Комисията представи предложение⁸ за нов регламент, който да отмени Регламент № 45/2001 и Решение № 1247/2002/ЕО с цел осъвременяване на правилата в тази област и съгласуването им с новия режим по Регламент (ЕС) 2016/679.

2 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронните комуникации) (ОВ L 201, 31.7.2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63), консолидиран текст от 19.12.2009 г.

3 Директива 2002/58/ЕО е изменена с Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на общественодостъпни електронни съобщителни услуги или на електронни съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 13.4.2006 г., стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51). С решение от 8 април 2014 г., Digital Rights Ireland и Seitlinger и др. (С-293/12 и С-594/12, ЕУ:С:2014:238), Съдът обявява тази директива за невалидна, тъй като създава тежко посягателство върху правото на неприкосновеност на лични живот и защитата на личните данни (вж. рубрика I.1 от този фиш, „Съвместимост на вторичното право на Съюза с правото на защита на личните данни“).

4 Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси (ОВ L 350, 30.12.2008 г., стр. 60), отменено, считано от 6 май 2018 г. (вж. бележка под линия 6).

5 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (ОВ L 119, 4.5.2016 г., стр. 1), приложим, считано от 25 май 2018 г.

6 Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

7 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 30, стр. 142).

8 Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (СОМ (2017) 8 окончателен).

I. Правото на защита на личните данни, признато с Хартата на основните права на Европейския съюз

1. Съвместимост на вторичното право на Съюза с правото на защита на личните данни

Решение от 9 ноември 2010 г. (голям състав), Volker und Markus Schecke и Eifert (C-92/09 и C-93/09, EU:C:2010:662)⁹

В главното производство по това дело се разглеждат спорове между земеделски производители и провинция Хесен по повод на публикуването на уебсайта на Bundesanstalt für Landwirtschaft und Ernährung (Федерална агенция по земеделие и храни) на лични данни, относещи се до тези земеделски производители в качеството им на получатели на средства от Европейския фонд за гарантиране на земеделието (ЕФГЗ) и Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР). Земеделските производители възразяват срещу публикуването на данните, като в частност изтъкват, че няма по-висш обществен интерес, който да го оправдава. Провинция Хесен поддържа, че публикуването на данните се изисква от регламенти (ЕО) № 1290/2005¹⁰ и № 259/2008¹¹, които уреждат финансирането на Общата селскостопанска политика и предвиждат задължително публикуване на информация за физическите лица — бенефициери на ЕФГЗ и ЕЗФРСР.

В този контекст Verwaltungsgericht Wiesbaden (Административен съд Висбаден, Германия) отправя до Съда няколко въпроса за валидността на отделни разпоредби от Регламент (ЕО) № 1290/2005 и на Регламент (ЕО) № 259/2008, които изискват публичното оповестяване на такава информация в частност на уебсайтовете на националните агенции.

Що се отнася до съвместимостта на закрепеното в Хартата право на защита на личните данни и задължението за прозрачност във връзка с европейските фондове, Съдът отбелязва, че поради свободния достъп на трети лица до уебсайта публикуването на този сайт на поименни данни за получателите на средства и за отпуснатите им суми накърнява правото им на зачитане на техния личен живот като цяло и правото на защита на техните лични данни в частност (т. 56—64).

За да е обосновано, накърняването на тези права трябва да е предвидено в закон, да зачита основното съдържание на посочените права и в съответствие с принципа на пропорционалност да е необходимо и действително да отговаря на признати от Съюза цели от общ интерес, а дерогациите и ограниченията на тези права трябва да се въвеждат в границите на строго необходимото (т. 65). В този контекст Съдът приема, че макар наистина в едно демократично общество данъкоплатците да имат право да бъдат информирани за използването на публичните средства, също така е вярно, че Съветът и Комисията са длъжни да претеглят балансирано различните разглеждани интереси, поради което е било необходимо преди приемането на спорните разпоредби да проверят дали публикуването на тези данни посредством отделен

⁹ Това решение е представено в Годишния доклад за 2010 г., стр. 11.

¹⁰ Регламент (ЕО) № 1290/2005 на Съвета от 21 юни 2005 година относно финансирането на Общата селскостопанска политика (ОВ L 209, 11.8.2005 г., стр. 1; Специално издание на български език, 2007 г., глава 14, том 1, стр. 193), отменен с Регламент (ЕС) № 1306/2013 на Европейския парламент и на Съвета от 17 декември 2013 година относно финансирането, управлението и мониторинга на общата селскостопанска политика (ОВ L 347, 20.12.2013 г., стр. 549).

¹¹ Регламент (ЕО) № 259/2008 на Комисията от 18 март 2008 година за установяване на подробни правила за прилагане на Регламент (ЕО) № 1290/2005 относно публикуването на информация за получателите на средства от Европейския фонд за гарантиране на земеделието (ЕФГЗ) и Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) (ОВ L 76, 19.3.2008 г., стр. 28), отменен с Регламент за изпълнение (ЕС) № 908/2014 на Комисията от 6 август 2014 година за определяне на правила за прилагането на Регламент (ЕС) № 1306/2013 на Европейския парламент и на Съвета по отношение на разплащателните агенции и други органи, финансовото управление, уравниването на сметките, правилата за проверките, обезпеченията и прозрачността (ОВ L 255, 28.8.2014 г., стр. 59).

уебсайт за всяка държава членка не надхвърля необходимото за осъществяване на легитимно преследваните цели (т. 77, 79, 85 и 86).

Затова Съдът обявява за невалидни някои разпоредби на Регламент (ЕО) № 1290/2005, както и целия Регламент (ЕО) № 259/2008, доколкото, що се отнася до физическите лица — бенефициери на помощи от ЕФГЗ и ЕЗФРСР, тези разпоредби налагат публикуването на лични данни относно всеки бенефициер, без да се прави разграничение въз основа на релевантни критерии като периодите, през които те са получавали подобни помощи, честотата или още вида и размера на помощите (т. 92; т. 1 от диспозитива). Съдът обаче не допуска оспорване на последиците от публикуването на списъците на бенефициерите на тези помощи, извършено от националните органи през периода, предшестваш датата на постановяване на решението му (т. 94; т. 2 от диспозитива).

Решение от 17 октомври 2013 г., Schwarz (C-291/12, EU:C:2013:670)

Г-н Schwarz подава молба до общинските власти на град Бохум (Германия) да му бъде издаден паспорт, като същевременно отказва да бъдат снети в тази връзка пръстовете му отпечатьци. След като общината отхвърля молбата му, г-н Schwarz подава жалба пред *Verwaltungsgericht Gelsenkirchen* (Административен съд Гелзенкирхен, Германия), за да бъде разпоредено на компетентните органи да му издадат паспорт без снемане на пръстовете отпечатьци. Пред тази юрисдикция г-н Schwarz оспорва валидността на Регламент (ЕО) № 2252/2004¹², който въвежда задължението за снемане на пръстовете отпечатьци на лицата, които искат да им бъде издаден паспорт, като в частност изтъква, че този регламент нарушава правото на защита на личните данни и правото на зачитане на личния живот.

В този контекст *Verwaltungsgericht Gelsenkirchen* (Административен съд Гелзенкирхен) отправя преюдициално запитване до Съда, за да установи дали Регламентът е валиден, в частност от гледна точка на Хартата, при положение че задължава лицата, които искат да им бъде издаден паспорт, да дадат пръстовете си отпечатьци и предвижда съхраняването на тези отпечатьци в паспорта.

Съдът отговаря утвърдително, като постановява, че наистина снемането и съхраняването на пръстови отпечатьци от националните власти, уредено в член 1, параграф 2 от Регламент (ЕО) № 2252/2004, съставляват засягане на правото на зачитане на личния живот и на защита на личните данни, но това е обосновано от целта за защита на паспортите срещу незаконно използване.

Най-напред, това предвидено в закона ограничение има призната от Съюза цел от общ интерес, доколкото цели да попречи по-конкретно на незаконното влизане на лица на територията на Съюза (т. 35—38). По-нататък, снемането и съхраняването на пръстови отпечатьци са в състояние да осъществят тази цел. Всъщност, от една страна, въпреки че методът на проверка на самоличността посредством пръстови отпечатьци не е напълно надежден, той снижава значително риска от допускането на неоторизирани лица. От друга страна, липсата на съвпадение на пръстовите отпечатьци на притежателя на паспорта с данните, въведени в този документ, не означава, че на въпросното лице автоматично ще бъде отказано влизане на територията на Съюза, а ще има за единствена последица извършването на задълбочен контрол, целящ да установи по категоричен начин самоличността на посоченото лице (т. 42—45).

¹² Регламент (ЕО) № 2252/2004 на Съвета от 13 декември 2004 година относно стандартите за отличителните знаци за сигурност и биометричните данни в паспортите и документите за пътуване, издавани от държавите членки (ОВ L 385, 29.12.2004 г., стр. 1; Специално издание на български език, 2007 г., глава 1, том 5, стр. 155), изменен с Регламент (ЕО) № 444/2009 на Европейския парламент и на Съвета от 6 май 2009 г. (ОВ L 142, 6.6.2009 г., стр. 1).

Най-сетне, що се отнася до необходимостта от такова обработване, на Съда не е известно да съществуват мерки, които да са достатъчно ефикасни, а същевременно да засягат в по-малка степен правата, признати от членове 7 и 8 от Хартата, в сравнение с мерките, произтичащи от метода, основан на пръстовите отпечатьци (т. 53). Член 1, параграф 2 от Регламент (ЕО) № 2252/2004 не изисква обработване на снетите пръстови отпечатьци, което да надхвърля необходимото за постигането на търсената цел. Всъщност този регламент уточнява изрично, че пръстовите отпечатьци могат да бъдат използвани само с цел проверка на автентичността на паспорта и самоличността на неговия притежател. Освен това член 1, параграф 2 от Регламента осигурява защита срещу риска от четене на данните, съдържащи пръстови отпечатьци, от неоторизирани лица и предвижда съхраняването на пръстови отпечатьци само в същия паспорт, който остава в изключително държане на своя притежател (т. 54—57, 60 и 63).

Решение от 8 април 2014 г. (голям състав), Digital Rights Ireland и Seitlinger и др. (съединени дела C-293/12 и C-594/12, EU:C:2014:238)¹³

Това решение е постановено по запитвания от ирландски и от австрийски съд за преценка на валидността на Директива 2006/24/ЕО за запазването на данните от гледна точка на основното право на зачитане на личния живот и основното право на защита на личните данни. По дело C-293/12 High Court (Висш съд, Ирландия) разглежда спор между дружеството Digital Rights и ирландските власти по въпроса за законосъобразността на определени национални мерки за запазване на данни относно електронните съобщения. По дело C-594/12 Verfassungsgerichtshof (Конституционен съд, Австрия) разглежда няколко конституционни жалби, с които се иска отмяна на националната разпоредба за транспониране на Директива 2006/24/ЕО в австрийското право.

С преюдициалните си запитвания ирландската и австрийската юрисдикция молят Съда да се произнесе по валидността на Директива 2006/24/ЕО от гледна точка на членове 7, 8 и 11 от Хартата. По-конкретно, тези юрисдикции питат Съда дали установеното в Директивата задължение на доставчиците на обществено достъпни електронни съобщителни услуги или обществени съобщителни мрежи да запазват за определен период данни, свързани с личния живот на дадено лице и с неговите съобщения, и да дават достъп на компетентните национални органи до тях, води до неоправдана намеса в посочените основни права. Става дума в частност за данните, необходими за проследяване и идентифициране на източника на съобщението и неговото местоназначение, за определяне на датата, времето, продължителността и вида на съобщението, съобщителното оборудване на ползвателите, както и за локализиране на мобилното съобщително оборудване, данни, сред които са по-специално името и адресът на абоната или на регистрирания ползвател, телефонният номер на викащата страна и номерът на виканата страна, както и IP адрес за интернет услугите. Именно тези данни дават възможност да се установи кое е лицето, с което даден абонат или регистриран ползвател се е свързал, и по какъв начин, като същевременно се определят времето на съобщението и мястото, от което то е направено. Освен това те дават възможност да се разбере честотата на съобщенията на абоната или на регистрирания ползвател с определени лица през определен период.

Най-напред Съдът постановява, че с налагането на подобни задължения на тези доставчици разпоредбите на Директива 2006/24/ЕО създават особено тежка намеса в основното право на зачитане на личния живот и основното право на защита на личните данни, които са гарантирани с членове 7 и 8 от Хартата. В този контекст Съдът констатира, че наистина тази намеса би могла да бъде оправдана от цел от общ интерес като борбата с организираната престъпност. В това отношение, на първо място, Съдът отбелязва, че изискваното от Директивата запазване на данните не би могло да засегне същественото съдържание на основното право на зачитане на

¹³ Това решение е представено в Годишния доклад за 2014 г., стр. 60.

личния живот и основното право на защита на личните данни, доколкото Директивата не позволява да се разкрива самото съдържание на електронните съобщения и предвижда, че доставчиците на услуги или мрежи трябва да спазват някои принципи във връзка със защитата и сигурността на данните. На второ място, Съдът посочва, че запазването на данните с оглед на евентуалното им предаване на компетентните национални органи действително отговаря на цел от общ интерес, а именно борба с тежките престъпления и в крайна сметка обществена сигурност (т. 38—44).

Съдът обаче намира, че с приемането на Директивата за запазването на данните законодателят на Съюза е надхвърлил границите, които налага зачитането на принципа на пропорционалност. Затова Съдът обявява Директивата за невалидна и постановява, че създаваната от нея силно изразена и особено тежка намеса в основните права не е достатъчно точно уредена, за да се гарантира, че ще е ограничена до строго необходимото (т. 65). Всъщност Директива 2006/24/ЕО се прилага общо за всички лица, за всички електронни съобщителни средства, както и за всички данни за трафик, без да въвежда никакво разграничение, ограничение или изключение с оглед на целта за борба с тежките престъпления (т. 57—59). Освен това Директивата не предвижда никакъв обективен критерий, позволяващ да се гарантира, че компетентните национални органи няма да имат достъп до данните и няма да могат да ги използват, освен за целите на предотвратяването, разкриването или преследването на престъпления, които могат да се считат за достатъчно тежки, за да обосновават подобна намеса, а и не предвижда материалните и процесуалните условия за такъв достъп и такова използване на данните (т. 60—62). Накрая, що се отнася до периода на съхранение на данните, Директивата изисква запазването им за период, не по-кратък от шест месеца, без да се прави каквато и да било разлика между категориите данни според засегнатите лица или според евентуалната полза от данните с оглед на преследваната цел (т. 63 и 64).

Освен това, що се отнася до изискванията по член 8, параграф 3 от Хартата, Съдът констатира, че Директива 2006/24/ЕО не предвижда достатъчно гаранции за ефикасна защита на данните срещу рисковете от злоупотреби, както и срещу всякакъв незаконен достъп или незаконно използване на тези данни, нито пък изисква данните да се съхраняват на територията на Съюза.

Ето защо въпросната директива не гарантира напълно, че спазването на изискванията за защита и сигурност ще подлежи на контрол от независим орган, какъвто обаче изрично се изисква от Хартата (т. 66—68).

2. Спазване на правото на защита на личните данни при прилагането на правото на Съюза

Решение от 21 декември 2016 г. (голям състав), Tele2 Sverige (съединени дела C-203/15 и C-698/15, EU:C:2016:970)¹⁴

След като с решение Digital Rights Ireland и Seitlinger и др. обявява за невалидна Директива 2006/24/ЕО (вж. по-горе), Съдът е сезиран с две дела относно предвиденото в Швеция и в Обединеното кралство задължение на доставчиците на електронни съобщителни услуги да запазват данните за електронните съобщения, както е предвидено в обявената за невалидна директива.

¹⁴ Това решение е представено в Годишния доклад за 2016 г., стр. 62.

В деня след обявяването на решение Digital Rights Ireland и Seitlinger и др. далекосъобщителното предприятие Tele2 Sverige уведомява шведския надзорен орган за пощите и далекосъобщенията, че преустановява запазването на данни и ще изтрие вече записаните данни (дело C-203/15). Всъщност шведското право задължава доставчиците на електронни съобщителни услуги системно и постоянно да запазват, без никакво изключение, всички данни за трафика и данните за местонахождението на всички техни абонати и регистрирани ползватели за всички електронни съобщителни средства. По дело C-698/15 се обсъждат жалбите на три лица срещу британската уредба на запазването на данните, съгласно която министърът на вътрешните работи има право да задължи обществените далекосъобщителни оператори да запазват всички данни относно съобщенията за максимален срок от 12 месеца, без обаче да е възможно запазване на съдържанието на тези съобщения.

Сезиран от Kammarrätten i Stockholm (Апелативен административен съд Стокхолм, Швеция) и Court of Appeal (England and Wales) (Civil Division) (Апелативен съд на Англия и Уелс, гражданско отделение, Обединеното кралство), Съдът се произнася по тълкуването на член 15, параграф 1 от Директива 2002/58/ЕО, известна като „Директивата за правото на неприкосновеност на личния живот и електронните комуникации“, разпоредба, която позволява на държавите членки да въвеждат някои изключения от предвиденото в тази директива задължение за осигуряване на поверителността на електронните съобщения и свързаните с тях данни за трафика.

В решението си Съдът най-напред постановява, че член 15, параграф 1 от Директива 2002/58/ЕО във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата не допуска национална правна уредба като шведската, която за целите на борбата с престъпността предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства. Според Съда такава правна уредба надхвърля границите на строго необходимото и не може да се счита за обоснована в едно демократично общество, както изисква член 15, параграф 1 от Директивата във връзка с упоменатите членове от Хартата (т. 99—105, 107 и 112; т. 1 от диспозитива).

Същата разпоредба във връзка със същите членове от Хартата не допуска и национална правна уредба, която регламентира защитата и сигурността на данните за трафик и на данните за местонахождение, и по-специално достъпа на компетентните национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза (т. 118—122 и 125; т. 2 от диспозитива).

За сметка на това Съдът приема, че член 15, параграф 1 от Директива 2002/58/ЕО допуска правна уредба, която позволява целево запазване на такива данни като превантивна мярка за целите на борбата с тежката престъпност, при условие че запазването на данни е ограничено до строго необходимото, що се отнася до подлежащите на запазване категории данни, визираните съобщителни средства, съответните лица, както и установения период на запазване. За да отговаря на тези изисквания, националната правна уредба трябва, на първо място, да предвижда ясни и точни правила, които да позволяват ефикасна защита на данните срещу рискове от злоупотреби. Тя трябва в частност да посочва обстоятелствата и условията, при които превантивно може да се приложи мярка за запазване на данни, като по този начин гарантира ограничаването ѝ до строго необходимото. На второ място, що се отнася до материалните условия, на които трябва да отговаря националната правна уредба, за да се гарантира, че ще е ограничена до строго необходимото, запазването на данните трябва да отговаря винаги на обективни критерии, установяващи връзка между подлежащите на запазване данни и преследваната с това цел. Такива условия трябва по-специално да се явяват на практика реално ограничаващи обхвата на мярката, а следователно и засегнатите лица. Що се отнася до посоченото ограничаване, националната правна уредба трябва да е основана на обективни

обстоятелства, които да правят възможно с нея да се визират лица, чиито данни могат да имат връзка, макар и непряка, с тежки престъпления, като по един или друг начин допринася за борбата с тежката престъпност или за предотвратяването на сериозен риск за обществената сигурност (т. 108—111).

II. Обработването на лични данни по смисъла на Директива 95/46/ЕО

1. Обработване на лични данни, което е извън приложното поле на Директива 95/46/ЕО

Решение от 30 май 2006 г. (голям състав), Парламент/Съвет (С-317/04 и С-318/04, EU:C:2006:346)

След терористичните нападения от 11 септември 2001 г. САЩ приемат законодателство, съгласно което въздушните превозвачи, които обслужват линии към, от или през територията на САЩ, са длъжни да предоставят на американските власти електронен достъп до данните в системите им за резервации и контрол при заминаване, или т.нар. резервационни данни на пътниците (Passenger Name Records, PNR данни).

Тъй като смята, че тези разпоредби могат да влязат в противоречие с европейското законодателство и със законодателствата на държавите членки в областта на защитата на данните, Комисията започва преговори с американските власти. В резултат от преговорите на 14 май 2004 г. Комисията приема Решение 2004/535/ЕО¹⁵, в което констатира, че служба „Митници и гранична защита“ на САЩ (United States Bureau of Customs and Border Protection, наричана по-нататък „СВР“) гарантира достатъчна степен на защита на предаваните от Общността PNR данни (наричано по-нататък „решението относно адекватността“). След това, на 17 май 2004 г., Съветът приема Решение 2004/496/ЕО¹⁶, с което одобрява сключването на споразумение между Европейската общност и САЩ относно обработването и предаването на СВР на резервационни данни за пътниците от страна на въздушните превозвачи, установени на територията на държавите — членки на Общността.

Европейският парламент моли Съда да отмени тези две решения, като в частност поддържа, че решението относно адекватността е прието *ultra vires*, че член 95 ЕО (понастоящем член 114 ДФЕС) не е подходящо правно основание за решението за одобряване на сключването на споразумението и че двете решения са приети в нарушение на основните права.

Що се отнася до решението относно адекватността, Съдът най-напред проверява дали Комисията е можела надлежно да приеме това решение на основание на Директива 95/46/ЕО. В този контекст Съдът констатира, че видно от решението относно адекватността, предаването на PNR данни на СВР представлява обработване на тези данни за целите на обществената сигурност и дейностите

¹⁵ Решение 2004/535/ЕО на Комисията от 14 май 2004 година относно адекватността на защитата на личните данни, съдържащи се в резервационните данни на пътниците във въздушния транспорт, предавани на служба „Митници и гранична защита“ на Съединените американски щати (ОВ L 235, 6.7.2004 г., стр. 11).

¹⁶ Решение 2004/496/ЕО на Съвета от 17 май 2004 година относно сключването на споразумение между Европейската общност и Съединените американски щати относно обработването и предаването на резервационни данни за пътниците от страна на въздушните превозвачи към служба „Митници и гранична защита“ на министерството на вътрешната сигурност на Съединените американски щати (ОВ L 183, 20.5.2004 г., стр. 83).

на държавата в областта на наказателното право. Според Съда наистина PNR данните първоначално се събират от авиокомпаниите в рамките на дейност, която попада в обхвата на правото на Съюза, а именно продажбата на самолетен билет, даващ право на определена доставка на услуги, но обработването на данните, което се разглежда в решението относно адекватността, е от съвсем друго естество. Всъщност това решение се отнася не до обработване на данни, което е необходимо за осъществяването на доставка на услуги, а до обработване на данни, което се счита за необходимо за защитата на обществената сигурност и за наказателни цели (т. 56 и 57).

В това отношение Съдът посочва, че PNR данните се събират от частни оператори за търговски цели и именно тези оператори организират предаването им на трета държава, но това не е пречка предаването на данните да се смята за обработване на данни, което е изключено от приложното поле на Директивата. Всъщност това предаване на данни се извършва в установена от публичните власти рамка, отнасяща се до обществената сигурност. Ето защо Съдът заключава, че решението относно адекватността не попада в приложното поле на Директивата, тъй като се отнася до обработване на данни, което е изключено от нейното приложно поле. Поради това Съдът отменя решението относно адекватността (т. 58 и 59).

Що се отнася до решението на Съвета, Съдът констатира, че член 95 ЕО във връзка с член 25 от Директива 95/46/ЕО не овластява Общността да сключи въпросното споразумение със САЩ. Всъщност споразумението се отнася до същото предаване на данни, до което се отнася и решението относно адекватността, и следователно до обработване на данни, което е изключено от приложното поле на Директивата. Поради това Съдът отменя решението на Съвета за одобряване на сключването на споразумението (т. 67—69).

Решение от 11 декември 2014 г., Ryneš (C-212/13, EU:C:2014:2428)

Поради неколкочратни посегателства срещу имота му г-н Ryneš инсталира на къщата си камера за видеонаблюдение. След поредното посегателство срещу къщата му записите от камерата дават възможност за идентифицирането на двама заподозрени, спрямо които са образувани наказателни производства. След като единият от заподозрените оспорва законосъобразността на обработката на записаните с камерата за видеонаблюдение данни пред чешката служба за защита на личните данни, същата констатира, че г-н Ryneš е нарушил правилата в областта на защитата на личните данни, и му налага глоба.

Сезиран с жалба от г-н Ryneš срещу решението, с което Městský soud v Praze (Окръжен съд Прага, Чешка република) потвърждава решението на тази служба, Nejvyšší správní soud (Върховен административен съд) отправя запитване до Съда дали записите, направени от г-н Ryneš, за да защити живота, здравето и имота си, представляват обработка на данни извън обхвата на Директива 95/46/ЕО, поради това че тези записи са направени от физическо лице в хода на изцяло лични или домашни занимания по смисъла на член 3, параграф 2, второ тире от тази директива.

Съдът постановява, че използването на система за видеонаблюдение, извършваща видеозаснемане на хора, съхранявано върху устройство за дълготрайно запаметяване, а именно твърд диск, която е инсталирана от физическо лице в семейната му къща за защита на собствеността, здравето и живота на собствениците на къщата, като системата покрива и обществени места, не представлява обработване на лични данни при извършване на изцяло лични или домашни занимания (т. 35 и диспозитива).

В това отношение Съдът напомня, че зачитането основното право на личен живот, гарантирано в член 7 от Хартата, изисква изключенията и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото. Доколкото разпоредбите на Директива 95/46/ЕО, уреждащи обработването на лични данни, което може да засегне основните свободи, и по-

специално правото на личен живот, по необходимост трябва да се тълкуват с оглед на основните права, които са закрепени в Хартата, предвиденото в член 3, параграф 2, второ тире от тази директива изключение трябва да се тълкува стриктно (т. 27—29). Нещо повече, самият текст на тази разпоредба изключва от приложното поле на Директива 95/46/ЕО обработването на лични данни, извършвано в хода на „изцяло“ лични или домашни занимания. Доколкото видеонаблюдението покрива, макар и частично, публични места и поради това е насочено извън личната сфера на лицето, което извършва по този начин обработване на данни, то не може да се счита за дейност, която е изцяло „лична или домашна“ по смисъла на посочената разпоредба (т. 30, 31 и 33).

2. Понятие за лични данни

Решение от 19 октомври 2016 г., Breyer (C-582/14, EU:C:2016:779)¹⁷

Г-н Breyer води дело пред германските граждански съдилища с искане да се забрани на Федерална република Германия да съхранява или да възлага на трети лица да съхраняват компютърните данни, предавани при всяко ползване на уебсайтовете на германските федерални служби. Всъщност с цел защита от атаки и осигуряване на възможност за наказателно преследване на „пиратите“ доставчикът на онлайн медийни услуги за германските федерални служби записва данните, състоящи се от „динамичния“ IP адрес, който се променя при всяко ново свързване с интернет, както и датата и часа на влизане в сайта. За разлика от статичните IP адреси, динамичните IP адреси по принцип не позволяват да се направи връзка посредством общодостъпни файлове между даден компютър и физическото включване към мрежата, използвано от доставчика на интернет услуги. Сами по себе си записаните данни не позволяват на доставчика на онлайн медийни услуги да идентифицира ползвателя. За сметка на това доставчикът на интернет услуги разполага с допълнителна информация, която, ако бъде комбинирана с този IP адрес, би позволила да бъде идентифициран ползвателят.

В този контекст Bundesgerichtshof (Федерален върховен съд, Германия), сезиран с ревизионна жалба по делото, отправя запитване до Съда дали IP адресът, записан от доставчик на онлайн медийни услуги при всяко влизане на неговия уебсайт, представлява за него лични данни.

Съдът най-напред отбелязва, че за да могат определени данни да се квалифицират като „лични данни“ по смисъла на член 2, буква а) от Директива 95/46/ЕО, не се изисква цялата информация, позволяваща идентифицирането на съответното лице, да се намира в ръцете на едно-единствено лице. Затова фактът, че допълнителната информация, необходима за идентифицирането на ползвател на интернет сайт, се притежава не от доставчика на онлайн медийни услуги, а от доставчика на интернет услуги на този ползвател, видимо не изключва възможността динамичните IP адреси, запазвани от доставчика на онлайн медийни услуги, да представляват за него лични данни по смисъла на член 2, буква а) от Директива 95/46/ЕО (т. 43 и 44).

Ето защо Съдът констатира, че динамичен IP адрес, запазен от доставчик на онлайн медийни услуги по повод на ползването от дадено лице на уебсайт, до който този доставчик предоставя достъп, представлява по отношение на въпросния доставчик лични данни по смисъла на член 2, буква а) от Директива 95/46/ЕО, когато същият разполага със законни средства, позволяващи му да идентифицира съответното лице благодарение на допълнителната информация, с която разполага доставчикът на интернет услуги на това лице (т. 49; т. 1 от диспозитива).

¹⁷ Това решение е представено в Годишния доклад за 2016 г., стр. 61.

Решение от 20 декември 2017 г., Nowak (C-434/16, EU:C:2017:582)

Г-н Nowak, стажант експерт-счетоводител, не издържа изпита, организиран от ирландската професионална организация на експерт-счетоводителите. На основание член 4 от Закона за защита на данните той подава молба за достъп до всички негови лични данни, съхранявани от професионалната организация на експерт-счетоводителите. Тази организация изпраща на г-н Nowak няколко документа, но отказва да му предостави неговата писмена изпитна работа, с довода че тя не съдържа негови лични данни по смисъла на Закона за защита на данните.

По същите съображения и комисарят за защита на данните не уважава искането за достъп на г-н Nowak и същият отнася случая до националните съдилища. Supreme Court (Върховен съд, Ирландия), който разглежда касационната жалба на г-н Nowak, отправя запитване до Съда дали член 2, буква а) от Директива 95/46/ЕО трябва да се тълкува в смисъл, че при условия като тези в главното производство писмените отговори, дадени от кандидат по време на изпит за професионални умения, и евентуалните коментари на проверителя по тези отговори представляват лични данни на кандидата по смисъла на тази разпоредба.

На първо място, Съдът отбелязва, че за да могат определени данни да се квалифицират като „лични данни“ по смисъла на член 2, буква а) от Директива 95/46/ЕО, не се изисква цялата информация, позволяваща идентифицирането на съответното лице, да се намира в ръцете на едно-единствено лице. Освен това, ако проверителят не знае самоличността на кандидата при оценяването на дадените от него отговори на изпит, организиращият изпита субект — в разглеждания случай професионалната организация на експерт-счетоводителите — все пак разполага с необходимата информация, позволяваща му да идентифицира без затруднения или съмнения този кандидат чрез неговия идентификационен номер, отбелязан върху писмената изпитна работа или заглавната ѝ страница, и съответно да му припише неговите отговори.

На второ място, Съдът констатира, че писмените отговори, дадени от кандидат на изпит за професионални умения, представляват информация, свързана с личността му. Всъщност съдържанието на тези отговори отразява равнището на знания и умения на кандидата в определена област, както евентуално и мисловния процес, преценката и критичното му мислене. Освен това крайната цел на събирането на тези отговори е да се оценят професионалните способности на кандидата и уменията му за упражняване на съответната професия. Също така, използването на тази информация, което по-специално намира отражение в издържането или неиздържането от кандидата на съответния изпит, може да има последици за неговите права и интереси, тъй като може да предопредели или повлияе например на шансовете му за достъп до желаната професия или работа. Констатацията, че писмените отговори, дадени от кандидат на изпит за професионални умения, представляват информация, която засяга този кандидат поради нейното съдържание, крайна цел и последици, освен това се отнася и за хипотезата на изпит „с отворена книга“.

На трето място, що се отнася до коментарите на проверителя по отговорите на кандидата, Съдът приема, че също както отговорите, дадени от кандидата на изпита, тези коментари представляват информация за кандидата, като се има предвид, че отразяват становището или преценката на проверителя относно индивидуалните резултати, постигнати от кандидата по време на изпита, и по-специално относно неговите знания и умения в съответната област. Крайната цел на тези коментари освен това е именно да се документира извършеното от проверителя оценяване на постигнатите резултати от кандидата и те могат да имат последици за последния.

На четвърто място, Съдът постановява, че е възможно писмените отговори, дадени от кандидат по време на изпит за професионални умения, и евентуалните коментари на проверителя по тях да бъдат подложени на проверка — по-специално, що се отнася до тяхната точност и до необходимостта от съхраняването им по смисъла на член 6, параграф 1, букви г) и д) от Директива

95/46/ЕО — и да бъдат поправени или изтрети на основание член 12, буква б) от същата директива. Предоставянето на кандидат на право на достъп до тези отговори и коментари по силата на член 12, буква а) от същата директива служи на целта на последната, а именно да гарантира защитата на правото на кандидата на личен живот при обработването на засягащите го данни, при това независимо дали въпросният кандидат разполага с такова право на достъп и по силата на националната правна уредба, приложима към изпитната процедура. Съдът обаче подчертава, че правата на достъп и на поправяне по член 12, букви а) и б) от Директива 95/46/ЕО не обхващат изпитните въпроси, които сами по себе си не представляват лични данни на кандидата.

По тези съображения Съдът заключава, че при условия като тези в главното производство писмените отговори, дадени от кандидат по време на изпит за професионални умения, и евентуалните коментари на проверителя по тези отговори представляват лични данни на кандидата по смисъла на член 2, буква а) от Директива 95/46/ЕО.

3. Понятие за обработване на лични данни

Решение от 6 ноември 2003 г. (пленум), Lindqvist (C-101/01, EU:C:2003:596)

Г-жа Lindqvist е доброволка към енория на протестантската църква в Швеция и чрез личния си компютър създава уебсайтове, в които публикува лични данни на други хора, които като нея са доброволци в енорията. Г-жа Lindqvist е осъдена и ѝ е наложено наказание глоба за това, че е използвала лични данни чрез автоматична обработка, без преди това да подаде писмена декларация до шведската Datainspektion (службата за защита на предаваните по компютърен път данни), че ги е прехвърляла без разрешение в трети страни и че е обработвала чувствителни лични данни.

Г-жа Lindqvist обжалва присъдата пред Göta hovrätt (Апелативен съд, Швеция), който отправя преюдициално запитване до Съда в частност за да установи дали г-жа Lindqvist е извършвала „пълна или частична обработка на лични данни с автоматизирани средства“ по смисъла на Директива 95/46/ЕО.

Съдът констатира, че операцията, състояща се в споменаването на различни лица в даден уебсайт и идентифицирането им по име или по друг начин, например чрез телефонния им номер или чрез информация за условията им на работа или за тяхното хоби, представлява „пълна или частична обработка на лични данни с автоматизирани средства“ по смисъла на Директивата (т. 27; т. 1 от диспозитива). Всъщност подобно обработване на лични данни за целите на доброволческа или религиозна дейност не попада в хипотезата на нито едно от изключенията от приложното поле на Директивата, доколкото не спада към нито една от категориите дейности, които са извън приложното поле на Директивата — нито към дейностите, отнасящи се до обществената сигурност, нито към изцяло личните или домашни занимания (т. 38 и 43—48; т. 2 от диспозитива).

Решение от 13 май 2014 г. (голям състав), Google Spain и Google (C-131/12, EU:C:2014:317)

През 2010 г. испански гражданин подава жалба до Agencia Española de Protección de Datos (Испанска агенция за защита на данните, наричана по-нататък „AEPD“) срещу La Vanguardia Ediciones SL, дружеството издател на широко разпространяван в Испания всекидневник, както и срещу Google Spain и Google. Той твърди, че когато интернет потребител въведе името му в търсачката на групата Google, списъкът с резултатите съдържа линкове към две страници на всекидневника на La Vanguardia от 1998 г., съдържащи в частност обява за публична продажба на недвижимо имущество във връзка с принудително изпълнение на негови задължения. С жалбата

си той иска, от една страна, да се разпорежи на La Vanguardia да премахне посочените страници или да измени съдържанието им или да използва някои от предоставяните от интернет търсачките средства за защита на тези данни. От друга страна, той иска да се разпорежи на Google Spain или на Google да заличи или да скрие тези лични данни, така че те да не се появяват повече в резултатите от търсенето и да не се съдържат във връзките към La Vanguardia.

AEPD отхвърля жалбата срещу La Vanguardia, тъй като приема, че издателят законно е публикувал тази информация, но уважава жалбата в частта ѝ относно Google Spain и Google, като задължава тези две дружества да вземат необходимите мерки, за да премахнат данните от своя индекс и да направят достъпа до тях невъзможен занапред. Тези дружества подават две жалби до Audiencia Nacional (Национален съд, Испания), с които искат да се отмени решението на AEPD, във връзка с което този испански съд отправя редица въпроси до Съда.

Това дава повод на Съда да изясни понятието „обработване на лични данни“ в интернет по смисъла на Директива 95/46/ЕО.

Съдът постановява, че дейността на интернет търсачка, изразяваща се в намиране на публикувана или въведена в интернет от трети лица информация, автоматичното ѝ индексване, временно съхраняване и накрая, предоставянето ѝ на разположение на потребителите на интернет в определен ред на предпочитание, трябва да се квалифицира като обработване на лични данни, когато тази информация съдържа лични данни (т. 1 от диспозитива). Освен това Съдът припомня, че посочените в Директивата операции трябва да се квалифицират като обработване включително когато се отнасят само до информация, която вече е публикувана в медиите в същия вид. Евантуална обща дерогация от прилагането на Директивата в тази хипотеза до голяма степен би лишила посочената директива от смисъл (т. 29 и 30).

4. Условия за законност на обработването на лични данни съгласно член 7 от Директива 95/46/ЕО

Решение от 16 декември 2008 г. (голям състав), Huber (C-524/06, EU:C:2008:724)¹⁸

Федералната служба за миграцията и бежанците (Bundesamt für Migration und Flüchtlinge, Германия) води централен регистър на чужденците, в който се съхраняват някои лични данни на чужденците, пребиваващи на германска територия за повече от три месеца. Регистърът се използва за статистически цели, както и при упражняването от службите за сигурност, от полицейските служби и от съдебните органи на правомощията им в областта на преследването и разследването във връзка с действия, които са наказуеми или създават заплаха за обществената сигурност.

Австрийският гражданин г-н Huber се установява през 1996 г. в Германия, за да упражнява там професията на независим застрахователен агент. Тъй като смята, че е дискриминиран поради обработването, на което подлежат свързаните с него данни в регистъра, доколкото за германските граждани не съществува подобна база данни, г-н Huber моли тези данни да бъдат заличени.

В този контекст сезираният със спора Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Висш административен съд на провинция Северен Рейн Вестфалия, Германия) отправя запитване

¹⁸ Това решение е представено в Годишния доклад за 2008 г., стр. 45.

до Съда дали обработването на лични данни във въпросния регистър е съвместимо с правото на Съюза.

Най-напред Съдът припомня, че правото на гражданите на Съюза да пребивават на територията на държави членки, на които не са граждани, не е безусловно, а може да бъде ограничавано. Затова използването на подобен регистър, за да се подпомагат органите, отговарящи за прилагането на нормативната уредба относно правото на пребиваване, по принцип е законосъобразно и предвид естеството му е съвместимо със забраната за дискриминация според гражданството, предвидена в член 12, параграф 1 ЕО (понастоящем член 18, първа алинея ДФЕС). Такъв регистър обаче не може да съдържа друга информация освен необходимата за тази цел по смисъла на Директивата за защита на личните данни (т. 54, 58 и 59).

Що се отнася до понятието за необходимост от обработването на данните по смисъла на член 7, буква д) от Директива 95/46/ЕО, Съдът най-напред припомня, че това е самостоятелно понятие на правото на Съюза, което трябва да бъде тълкувано в пълно съответствие с целта на Директива 95/46/ЕО, определена в член 1, параграф 1 от нея. По-нататък Съдът констатира, че дадена система за обработване на лични данни е съвместима с правото на Съюза, ако съдържа единствено данните, които са необходими на посочените органи, за да прилагат тази нормативна уредба, и ако централизиращият ѝ характер позволява по-ефективното прилагане на тази нормативна уредба, що се отнася до правото на пребиваване на гражданите на Съюза, които не са граждани на тази държава членка.

При всяко положение съхранението и обработването на поименни лични данни в рамките на подобен регистър за статистически цели не могат да се приемат за необходими по смисъла на член 7, буква д) от Директива 95/46/ЕО (т. 52, 66 и 68).

Освен това, що се отнася до въпроса за използването на съдържащите се в регистъра данни за целите на борбата с престъпността, Съдът в частност отбелязва, че тази цел предполага наказване на престъпленията независимо от гражданството на извършителите. Следователно от гледна точка на целта за борба с престъпността за държавата членка положението на гражданите ѝ не може да се различава от положението на гражданите на Съюза, които не са граждани на тази държава членка и пребивават на нейна територия. Ето защо с оглед на целта за борба с престъпността различното третиране на тези граждани и посочените граждани на Съюза, изведено от рутинното обработване на лични данни само на гражданите на Съюза, които не са граждани на съответната държава членка, представлява дискриминация, забранена от член 12, параграф 1 ЕО (т. 78—80).

Решение от 24 ноември 2011 г., ASNEF и FECEMD (C-468/10 и C-469/10, EU:C:2011:777)

Asociación Nacional de Establecimientos Financieros de Crédito (Национално сдружение на кредитните институции, ASNEF) и Federación de Comercio Electrónico y Marketing Directo (Федерация за електронна търговия и директен маркетинг, FECEMD) подават жалби до Tribunal Supremo (Върховен съд, Испания), с които искат да бъдат отменени редица членове на Кралски указ 1720/2007 за прилагането на Устройствен закон 15/1999, с който се транспонира Директива 95/46/ЕО.

По-конкретно, ASNEF и FECEMD поддържат, че испанското право предвижда несъществуващо в Директива 95/46/ЕО условие за обработването на лични данни без съгласието на съответното лице, а именно условието тези данни да се съдържат в „общодостъпни източници“ като изброените в член 3, буква j) от Устройствен закон 15/1999. В това отношение те изтъкват, че този закон и Кралски указ 1720/2007 ограничават действието на член 7, буква е) от Директива 95/46/ЕО, който предвижда само едно условие за обработването на лични данни без съгласието на

съответното лице, а именно обработването на данните да е необходимо за целите на законните интереси, преследвани от администратора или от третото лице, на което се разкриват данните.

В това отношение Съдът най-напред отбелязва, че член 7 от Директива 95/46/ЕО изчерпателно изброява случаите, в които обработването на лични данни може да се счита за законно при липсата на съгласие от страна на съответното лице. Ето защо държавите членки не могат на основание член 5 от тази директива нито да въвеждат други критерии за законност на обработването на лични данни, различни от прогласените в член 7, нито чрез допълнителни изисквания да изменят обхвата на предвидените в член 7 критерии. Всъщност член 5 дава право на държавите членки единствено да уточнят — в границите на глава II от Директивата, а следователно и на член 7 от последната — условията, при които обработването на лични данни е законно (т. 30, 32 и 33).

По-конкретно, държавите членки могат да установяват критерии за извършване на необходимото съгласно член 7, буква е) от Директивата претегляне на съответните противоположни права и интереси. Те също така могат да вземат предвид обстоятелството, че тежестта на засягане на основните права на лицето, до което се отнасят съответните данни, може да е различна според това дали тези данни се съдържат или не в общодостъпни източници (т. 44 и 46).

Съдът обаче приема, че когато националната правна уредба изключва възможността за обработване на някои категории лични данни, като спрямо тях определя окончателно резултата от претеглянето на противоположните права и интереси, без да допуска различен резултат в зависимост от обстоятелствата на конкретния случай, това вече не представлява по-точно определяне по смисъла на член 5 от Директива 95/46/ЕО. Затова Съдът заключава, че член 7, буква е) от Директива 95/46/ЕО не допуска държава членка да изключи категорично и безусловно възможността за обработване на някои категории лични данни, без да позволи претегляне във всеки конкретен случай на съответните противоположни права и интереси (т. 47 и 48).

Решение от 19 октомври 2016 г., Breyer (C-582/14, EU:C:2016:779)

В това решение (вж. също рубрика II.2, „Понятие за лични данни“) Съдът се произнася и по въпроса дали член 7, буква е) от Директива 95/46/ЕО допуска разпоредба от националното право, съгласно която доставчикът на онлайн медийни услуги може да събира и използва лични данни за ползвател без неговото съгласие само доколкото това е необходимо, за да се даде възможност за конкретното ползване на електронната медия от съответния ползвател и за да се отчете това ползване, и съгласно която целта за осигуряване на общата функционална способност на електронната медия не може да оправдае използването на данните след края на съответното действие на ползване.

Съдът постановява, че член 7, буква е) от Директива 95/46/ЕО не допуска такава правна уредба. Всъщност съгласно тази разпоредба обработването на лични данни е законно само когато е необходимо за целите на законните интереси, преследвани от администратора или от трето лице или 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. В случая обаче германската правна уредба изключва категорично и безусловно възможността за обработване на някои категории лични данни, без да позволи претегляне във всеки конкретен случай на съответните противоположни права и интереси. По този начин тази правна уредба недопустимо ограничава обхвата на критерия по член 7, буква е) от Директива 95/46/ЕО, като изключва възможността за претегляне на целта за осигуряване на общата функционална способност на сайтовете на електронната медия спрямо интереса или основните права и свободи на ползвателите (т. 62—64; т. 2 от диспозитива).

Решение от 4 май 2017 г., Rīgas satiksme (C-13/16, EU:C:2017:336)

Това дело е свързано със спор между латвийската национална полиция и Rīgas satiksme, дружеството за тролейбусен транспорт на град Рига, по повод на искане за съобщаване на идентификационните данни на лице, причинило пътно-транспортно произшествие. В конкретния случай при пътно-транспортно произшествие таксиметров шофьор паркира автомобила си край пътя. При преминаването на тролейбус на Rīgas satiksme покрай това такси пътникът на задната седалка на таксито отваря вратата, която се удря в каросерията на тролейбуса, нанасяйки ѝ вреда. За да може да предяви иск за обезщетение за тези вреди, Rīgas satiksme в частност отправя искане до националната полиция да му съобщи идентификационните данни на лицето, причинило произшествието. Полицията отказва да съобщи идентификационния номер и адреса на пътника, както и документите, съдържащи изявленията на участвалите в произшествието лица, по съображение че само страните в административнонаказателното производство могат да получат достъп до събраната в него информация, а и законът за защита на данните на физическите лица забранява разкриването на идентификационния номер и адреса на частни лица.

При тези условия Augstākās tiesas Administratīvo lietu departaments (Върховен съд, административно отделение, Латвия) решава да отправи до Съда въпроса дали член 7, буква е) от Директива 95/46/ЕО създава задължение за разкриване на лични данни пред трето лице, за да може то да предяви пред гражданските съдилища иск за обезщетение за вредите, причинени му от лицето, ползващо се от защитата на тези данни, и дали фактът, че последното не е навършило пълнолетие, има значение за тълкуването на тази разпоредба.

Съдът постановява, че член 7, буква е) от Директива 95/46/ЕО трябва да се тълкува в смисъл, че не създава задължение за разкриване на лични данни пред трето лице, за да може то да предяви пред гражданските съдилища иск за обезщетение за вредите, причинени му от лицето, ползващо се от защитата на тези данни. Тази разпоредба обаче допуска разкриване на такива данни, в случай че то се извършва въз основа на националното право при спазване на предвидените в тази разпоредба условия (т. 27 и 34, както и диспозитива).

В този контекст Съдът отбелязва, че освен ако националният съд не установи друго в това отношение, не е оправдано при обстоятелства като тези по главното производство на пострадалия да не бъдат разкрити — само защото причинителят на вредите не е навършил пълнолетие — личните данни, необходими, за да предяви иск за обезщетение за вреди срещу този причинител или евентуално срещу лицата, упражняващи родителските права (т. 33).

Решение от 27 септември 2017 г., Puškár (C-73/16, EU:C:2017:725)

В главното производство Najvyšší súd Slovenskej republiky (Върховен съд на Словашката република) разглежда жалба от г-н Puškár, който иска да бъде разпоредено на Finančné riaditeľstvo (дирекция „Финанси“), на всички подчинени на дирекцията данъчни служби и на Kriminálny úrad finančnej správy (отдел за разследване на финансови престъпления) да не включват името му в списъка на лицата, които дирекцията счита за подставени лица, списък, който дирекцията съставя във връзка със събирането на данъците и който се води съвместно от тази дирекция и от отдела за разследване на финансови престъпления (наричан по-нататък „спорният списък“). Освен това г-н Puškár иска да бъдат заличени всички отнасящи се до него данни в тези списъци и в информационната система на финансовата администрация.

При тези условия Najvyšší súd (Върховният съд) отправя запитване до Съда в частност дали правото на зачитане на личния и семейния живот, на жилището и тайната на съобщенията, предвидено в член 7, както и правото на защита на личните данни, предвидено в член 8 от Хартата, могат да се тълкуват в смисъл, че не допускат държавите членки да създават без

съгласието на заинтересованото лице списъци с лични данни за целите на събирането на данъците, тоест че само по себе си събирането на лични данни от публичните органи с цел борба с данъчните измами представлява риск.

Съдът заключава, че член 7, буква д) от Директива 95/46/ЕО допуска обработване на лични данни от органите на държава членка за целите на събирането на данъци и на борбата с данъчните измами като произтичащото от съставянето на списък на лица като този в главното производство без съгласието на заинтересованите лица, при условие, от една страна, че националното законодателство е възложило на тези органи задачи, които се осъществяват в обществен интерес по смисъла на тази разпоредба, че съставянето на този списък и включването в него на имената на заинтересованите лица са подходящи и необходими за осъществяване на преследваните цели и че съществуват достатъчно улики, даващи основание да се предположи, че заинтересованите лица са включени основателно в посочения списък, и от друга страна, че са изпълнени всички изисквания за законосъобразност на това обработване на лични данни, предвидени в Директива 95/46/ЕО (т. 117; т. 3 от диспозитива).

В това отношение Съдът отбелязва, че запитващата юрисдикция трябва да провери дали съставянето на спорния списък е необходимо за изпълнението на обсъжданите в главното производство задачи в обществен интерес, като вземе предвид по-специално точната цел на съставянето на спорния списък, правните последици за посочените в него лица и това дали този списък е публичен или не. Освен това от гледна точка на принципа на пропорционалност националната юрисдикция следва да провери дали съставянето на спорния списък и включването в него на имената на заинтересованите лица са подходящи за осъществяване на преследваните с тях цели и дали не са налице други, по-малко ограничителни способности за постигането на тези цели (т. 111, 112 и 113).

Също така Съдът констатира, че с включването на дадено лице в спорния списък може да бъдат засегнати някои от правата на това лице. Всъщност включването в списъка би могло да увреди репутацията му и да повлияе на отношенията му с данъчните органи. Също така включването би могло да засегне презумпцията за невинност на това лице, закрепена в член 48, параграф 1 от Хартата, както и закрепената в член 16 от Хартата свобода на стопанска инициатива на юридическите лица, свързани със физическите лица, включени в спорния списък. Ето защо такава намеса може да е подходяща само ако съществуват достатъчно улики, даващи основание да се подозира, че заинтересованото лице има фиктивни ръководни функции в юридическите лица, свързани с него, и по този начин засяга събирането на данъци и борбата с данъчните измами (т. 114).

Освен това Съдът приема, че ако съществуват причини за ограничаване по смисъла на член 13 от Директива 95/46/ЕО на някои от правата, предвидени в членове 6 и 10—12 от тази директива, като правото на информация на заинтересованото лице, това ограничение трябва да е необходимо за гарантиране на посочените в член 13, параграф 1 интереси, и по-специално на важни икономически и финансови интереси в данъчната сфера, и да се основава на законодателни мерки (т. 116).

III. Предаване на лични данни на трети страни

Решение от 6 ноември 2003 г. (пленум), Lindqvist (C-101/01, EU:C:2003:596)¹⁹

По това дело (вж. също рубрика II.3, „Понятие за обработване на лични данни“) запитващата юрисдикция задава в частност въпроса дали г-жа Lindqvist е предавала данни на трети страни по смисъла на посочената директива.

Съдът постановява, че не е налице „предаване на лични данни на трети страни“ по смисъла на член 25 от Директива 95/46/ЕО, когато намиращо се в държава членка лице записва лични данни върху уебстраница, съхранявана от физическо или юридическо лице, което хоства уебсайта, от който може да бъде отворена страницата, и което е установено в същата държава или в друга държава членка, като по този начин данните стават достъпни за всяко свързано с интернет лице, в това число за лица, които се намират в трети страни (т. 71; т. 4 от диспозитива).

Всъщност, като се имат предвид, от една страна, етапът на развитието на интернет към момента на изготвянето на Директива 95/46/ЕО и от друга, липсата на приложими за използването на интернет критерии в глава IV, която включва член 25, предназначен да осигури контрол от страна на държавите членки върху предаването на лични данни към трети страни и да забрани предаването им, ако не е гарантирана достатъчна степен на защита, не може да се презюмира, че волята на общностния законодател е била изпреварващо да включи този вид записване на данни върху уебстраница в обхвата на понятието „предаване на лични данни на трети страни“, въпреки че по този начин данните стават достъпни за лицата от трети страни, разполагащи с техническите средства за достъп до тях (т. 63, 64 и 68).

Решение от 6 октомври 2015 г. (голям състав), Schrems (C-362/14, EU:C:2015:650)²⁰

Австрийският гражданин г-н Schrems, потребител на социалната мрежа Facebook, подава жалба до Data Protection Commissioner (Комисар за защита на личните данни, Ирландия), поради това че Facebook Ireland прехвърля в САЩ личните данни на своите потребители и ги съхранява на разположение в тази страна сървъри, където те се подлагат на обработка. Според г-н Schrems правото и практиките в САЩ не гарантират достатъчна защита срещу извършваните от публичните органи дейности по наблюдение на прехвърляните в тази страна данни. Комисарят за защита на личните данни отказва да започне разследване по твърденията в жалбата, в частност защото според него в Решение 2000/520/ЕО²¹ Комисията е приела, че в рамките на т.нар. схема за „сфера на неприкосновеност на личния живот“ (на английски „safe harbour“)²² САЩ гарантират достатъчна степен на защита на прехвърляните лични данни.

В този контекст High Court (Висш съд, Ирландия) отправя до Съда запитване за тълкуването на член 25, параграф 6 от Директива 95/46/ЕО, съгласно който Комисията може да констатира, че трета страна гарантира достатъчна степен на защита на прехвърляните данни, както и по същество запитване за валидността на Решение 2000/520/ЕО, което Комисията е приела на основание член 25, параграф 6 от Директива 95/46/ЕО.

¹⁹ Това решение е представено в Годишния доклад за 2003 г., стр. 67.

²⁰ Това решение е представено в Годишния доклад за 2015 г., стр. 53.

²¹ Решение 2000/520/ЕО на Комисията от 26 юли 2000 година съгласно Директива 95/46/ЕО относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ (ОВ L 215, 25.8.2000 г., стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64).

²² Схемата за сфера на неприкосновеност на личния живот включва няколко правила за защита на личните данни, които американските предприятия могат да прилагат на доброволен принцип.

Съдът обявява решението на Комисията за невалидно в неговата цялост, като най-напред подчертава, че приемането му е изисквало надлежно мотивирана констатация от страна на Комисията, че съответната трета страна ефективно гарантира степен на защита на основните права, която по същество е равностойна на гарантираната в правния ред на Съюза. Тъй като обаче в своето Решение 2000/520/ЕО Комисията не прави такава констатация, член 1 от това решение не отговаря на изискванията, установени в член 25, параграф 6 от Директива 95/46/ЕО, разглеждан във връзка с Хартата, и поради това е невалиден. Всъщност принципите за „сфера на неприкосновеност на личния живот“ се прилагат единствено за американски самосертифицирани организации, получаващи лични данни от Съюза, като не се изисква американските публични органи да спазват тези принципи. Освен това Решение 2000/520/ЕО прави възможна намесата в упражняването на основните права на лицата, чиито лични данни се прехвърлят или биха могли да се прехвърлят от Съюза към САЩ, без в него да се съдържа констатация относно наличието в посочената страна на правила с етичен характер, предназначени за ограничаване на евентуалната намеса, засягаща тези права, и без да се отбелязва наличието на ефективна правна защита срещу този вид намеса (т. 82, 87—89 и 96—98; т. 2 от диспозитива).

Съдът обявява за невалиден и член 3 от Решение 2000/520/ЕО, доколкото тази разпоредба лишава националните надзорни органи от правомощията, които те черпят от член 28 от Директива 95/46/ЕО, в случай че съответното лице посочи обстоятелства, които могат да поставят под въпрос съвместимостта със защитата на личния живот и на основните права и свободи на лицата на решение на Комисията, с което тя констатира, че трета страна гарантира достатъчна степен на защита (т. 102—104). Съдът заключава, че невалидността на членове 1 и 3 от Решение 2000/520/ЕО засяга валидността на цялото решение (т. 105 и 106).

Що се отнася до невъзможността да се обоснове подобна намеса, Съдът най-напред отбелязва, че съответната правна уредба на Съюза, в която се предвижда намеса в гарантираните с членове 7 и 8 от Хартата основни права, трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито лични данни са били засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби, както и срещу всякакъв незаконен достъп или използване на тези данни. Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматична обработка и съществува значителен риск от незаконен достъп до тях (т. 91).

Освен това и преди всичко, защитата на основното право на зачитане на личния живот на равнището на Съюза изисква дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото (т. 92). В този смисъл не се ограничава до строго необходимото правна уредба, която общо разрешава съхраняването на всички лични данни на всички лица, чиито данни са били прехвърлени от Съюза, без да въвежда никакво разграничение, ограничение или изключение с оглед на преследваната цел и без да предвижда обективен критерий, позволяващ да се ограничи достъпът на публичните органи до данните и тяхното последващо използване за конкретни цели, които са строго ограничени и могат да обосноват намесата, каквато съдържа достъпът и използването на тези данни (т. 93). По-конкретно, правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, засяга същественото съдържание на основното право на зачитане на личния живот. Също така правна уредба, в която не се предвижда никаква възможност правният субект да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни, не зачита същественото съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата (т. 94 и 95).

**Становище 1/15 (Споразумение PNR ЕС—Канада) от 26 юли 2017 г. (голям състав)
(EU:C:2017:592)**

На 26 юли 2017 г. Съдът се произнася за първи път по съвместимостта на проект за международно споразумение с Хартата на основните права на Европейския съюз, и в частност с разпоредбите относно зачитането на личния живот и защитата на личните данни.

Европейският съюз и Канада се договарят по споразумение относно предаването и обработката на резервационни данни на пътниците (споразумението PNR), което е подписано през 2014 г. Съветът на Европейския съюз внася искане в Европейския парламент за одобряване на споразумението и Парламентът решава да поиска становище от Съда относно съвместимостта на предвиденото споразумение с правото на Съюза.

Предвиденото споразумение допуска резервационните данни (т.нар. „PNR данни“) на всички пътници във въздушния транспорт систематично и непрекъснато да се предават на компетентния канадски орган с оглед на тяхното използване и съхраняване, както и с оглед на евентуалното им последващо предаване на други органи и други трети страни, с цел борба с тероризма и тежката транснационална престъпност. Затова споразумението предвижда в частност петгодишен срок на съхранение на данните и установява особени изисквания във връзка със сигурността и целостта на PNR данните, например незабавно маскиране на чувствителните данни, а също така предвижда право на достъп до данните, право на коригиране и право на заличаването им и правни средства за защита по административен и съдебен ред.

Визираните с предвиденото споразумение PNR данни включват в частност името и наличната информация за контакт на пътника или пътниците, необходимата информация, за да се направи резервация, например датите на заплануваното пътуване и маршрута на пътуването, информация за билетите, групите лица, регистрирани под един и същ номер на резервация, информация относно средствата за плащане или фактуриране, информация за багажа, както и общи бележки за пътниците.

В становището си Съдът постановява, че споразумението PNR не може да бъде сключено в настоящия му вид поради несъвместимостта на редица негови разпоредби с основните права, признати в Съюза.

На първо място, Съдът констатира, че както предаването на PNR данните от Съюза на канадския компетентен орган, така и договорената от Съюза с Канада уредба на условията, свързани със запазването на тези данни, тяхното използване и евентуалното им по-нататъшно предаване на други канадски органи, Европол, Евроюст, на съдебните или полицейските органи на държавите членки или пък на органите на други трети държави, представляват форми на намеса в гарантираното от член 7 от Хартата право. Тези операции представляват и намеса в основното право на защита на личните данни, гарантирано от член 8 от Хартата, тъй като са видове обработка на лични данни (т. 125 и 126).

Наред с това Съдът подчертава, че макар да изглежда, че някои PNR данни, разгледани самостоятелно, не могат да разкрият важна информация за личния живот на засегнатите лица, все пак, взети заедно, те могат по-специално да разкрият пълния маршрут на пътуването, навигиците при пътуване, съществуващите отношения между две или повече лица, както и информация относно финансовото положение на пътниците във въздушния транспорт, техните хранителни навици или здравословно състояние и дори биха могли да предоставят чувствителна информация за пътниците съгласно дефиницията в член 2, буква д) от предвиденото споразумение (данни, които разкриват расов или етнически произход, политически възгледи, религиозни убеждения и пр.) (т. 128).

В това отношение Съдът приема, че макар тези форми на намеса да могат да бъдат обосновани с цел от общ интерес (гарантиране на обществената сигурност в контекста на борбата с терористичните престъпления и тежките транснационални престъпления), редица разпоредби на споразумението не се изчерпват със строго необходимото и не предвиждат ясни и точни правила.

По-конкретно, Съдът отбелязва, че предвид риска данните да бъдат обработвани в противоречие с принципа за недопускане на дискриминация, евентуалното предаване на чувствителните данни към Канада би изисквало точна и особено солидна обосновка, изведена от мотиви, различни от защитата на обществената сигурност от тероризъм и тежка транснационална престъпност. В конкретния случай обаче липсва подобна обосновка. Затова Съдът заключава, че разпоредбите на споразумението относно предаването на чувствителни данни към Канада и относно обработването и запазването на тези данни са несъвместими с основните права (т. 165 и 232).

На второ място, Съдът приема, че след отпътуването на съответните пътници от Канада разрешеното от споразумението продължаващо съхраняване на PNR данните на всички пътници във въздушния транспорт не се свежда до строго необходимото. Всъщност, що се отнася до пътниците във въздушния транспорт, за които при пристигането им в Канада и до заминаването им от тази държава не е бил установен риск във връзка с тероризма или тежката транснационална престъпност, след отпътуването им не се установява наличието дори на индиректна връзка между PNR данните им и преследваната с предвиденото споразумение цел, която би обосновала запазването на посочените данни. Обратно, съхраняването на PNR данните на пътниците във въздушния транспорт, за които са установени обективни обстоятелства, позволяващи да се приеме, че дори след заминаването си от Канада те биха могли да представляват такъв риск, е допустимо и след престоя им в тази страна, включително за период от пет години (т. 205—207 и 209).

На трето място, Съдът констатира, че основното право на зачитане на личния живот, закрепено в член 7 от Хартата на основните права на Европейския съюз, предполага съответното физическо лице да може да се убеди, че личните му данни се обработват по точен и законосъобразен начин. За да може да извърши необходимите проверки, това лице трябва да разполага с право на достъп до данните, които се отнасят до него и които са предмет на обработка.

В това отношение Съдът подчертава, че в предвиденото споразумение е важно пътниците във въздушния транспорт да бъдат информирани за предаването на техните PNR данни в съответната трета страна и за използването на същите веднага щом това вече не може да попречи на извършването от визираните в предвиденото споразумение публични органи разследване. В действителност тази информация фактически се оказва необходима, за да даде възможност на пътниците във въздушния транспорт да упражнят правото си да поискат достъп до засягащите ги PNR данни и евентуално тяхното поправяне, както и в съответствие с член 47, първа алинея от Хартата да подадат ефективна жалба пред съда.

В този смисъл в хипотезите, в които са налице обективни обстоятелства, обосноваващи използването на резервационните данни на пътниците за целите на борбата с тероризма и тежката транснационална престъпност и изискващи предварително разрешение от юрисдикция или независима административна структура, се оказва необходимо пътниците във въздушния транспорт да бъдат информирани лично. Същото се отнася за случаите, в които резервационните данни на пътниците във въздушния транспорт се разкриват на други публични органи или на частни лица. Същевременно подобна информация трябва да се дава едва след като това вече не може да попречи на извършването от визираните в предвиденото споразумение публични органи разследване (т. 219, 220, 223 и 224).

IV. Защита на личните данни в интернет

1. Право на възражение срещу обработването на лични данни („право на забравя“)

Решение от 13 май 2014 г. (голям състав), Google Spain и Google (C-131/12, EU:C:2014:317)

В това решение (вж. също рубрика II.3, „Понятие за обработване на лични данни“) Съдът изяснява обхвата на предвидените в Директива 95/46/ЕО права на достъп и на възражение срещу обработването на лични данни в интернет.

Така, произнасяйки се по въпроса за обхвата на отговорността на субекта, който управлява интернет търсачка, Съдът по същество постановява, че за да спази правата на достъп и възражение, гарантирани с член 12, буква б) и член 14, първа алинея, буква а) от Директива 95/46/ЕО и стига да са налице предвидените в тези членове условия, този субект е длъжен при определени условия да заличава връзки към уебстраници, които са публикувани от трети лица и съдържат информация относно дадено лице, от списъка на резултатите, който се показва след търсене въз основа на името на това лице. Съдът пояснява, че това задължение може да е налице и в хипотезата, в която това име или тази информация не са заличени предварително или едновременно от тези уебстраници, при това дори когато евентуално самото им публикуване на посочените страници е законосъобразно (т. 88; т. 3 от диспозитива).

Освен това по въпроса дали Директивата позволява на съответното лице да иска връзките към някои уебстраници да бъдат заличени от списъка с резултати, тъй като би желало съдържащата се там информация за него да бъде „забравена“ след известно време, Съдът най-напред постановява, че дори обработване на точни данни, което първоначално е било законосъобразно, може с времето да стане несъвместимо с тази директива, когато данните вече не са необходими за целите, за които са събирани или обработвани, по-специално когато е видно, че тези данни не са адекватни, че не са или вече не са релевантни или че са прекомерни по отношение на целите и на изтеклия срок (т. 93). Ето защо ако вследствие на искане от съответното лице се установи, че включването на тези връзки в списъка с резултатите към настоящия момент е несъвместимо с Директивата, информацията и съответните връзки в посочения списък трябва да бъдат изтрети (т. 94). В този контекст констатацията за наличие на право на съответното лице отнасящата се до него информация да не се свързва повече с името му посредством списък на резултатите, не предполага, че включването на въпросната информация в списъка на резултатите причинява вреда на съответното лице (т. 96; т. 4 от диспозитива).

Накрая Съдът пояснява, че тъй като с оглед на основните си права по членове 7 и 8 от Хартата съответното лице може да поиска въпросната информация да не се предоставя повече на разположение на широката общественост посредством включването ѝ в подобен списък на резултатите, тези права имат по принцип предимство не само пред икономическия интерес на субекта, който управлява интернет търсачката, но и пред интереса на тази общественост да намери посочената информация при търсене, отнасящо се до името на въпросното лице. Такъв не би бил случаят обаче, ако по конкретни причини, като ролята на посоченото лице в обществения живот, е видно, че вмешателството в неговите основни права е обосновано поради приоритетния интерес на посочената общественост да има вследствие на това включване достъп до въпросната информация (т. 97; т. 4 от диспозитива).

2. Обработване на лични данни и право на интелектуална собственост

*Решение от 29 януари 2008 г. (голям състав), Promusicae (C-275/06, EU:C:2008:54)*²³

Испанското сдружение с нестопанска цел Promusicae, което обединява продуценти и издатели на музикални и аудиовизуални записи, се обръща към испанските съдилища с искане да осъдят Telefónica de España SAU (търговско дружество, чийто предмет на дейност включва и доставката на интернет услуги) да разкрие самоличността и физическия адрес на някои лица, на които е доставяло интернет услуги и за които са известни използваният IP адрес и датата и часа на свързване с интернет. Според Promusicae тези лица са използвали програма за обмен на файлове, известна като „peer-to-peer“ или „P2P“ (самостоятелно и децентрализирано прозрачно средство за споделяне на съдържание с разширени функции за търсене и сваляне), която дава възможност за достъп до звукозаписи в споделената директория на личния им компютър, записи, върху които членовете на Promusicae притежават имуществени права на използване. Ето защо то моли да му се съобщят посочените по-горе сведения, за да може да предяви граждански иски срещу заинтересованите лица.

При тези обстоятелства Juzgado de lo Mercantil no 5 de Madrid (Съд по търговски дела № 5, Мадрид, Испания) отправя запитване до Съда дали европейското законодателство задължава държавите членки да предвидят задължение за съобщаване на лични данни в рамките на гражданско производство, за да осигурят ефективна защита на авторското право.

Според Съда това запитване повдига въпроса за необходимото съчетаване на изискванията, свързани със защитата на различните основни права, а именно, от една страна, правото на зачитане на личния живот и от друга страна, правото на защита на собствеността и правото на ефективни правни средства за защита.

В това отношение Съдът заключава, че Директива 2000/31/ЕО за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директивата за електронната търговия)²⁴, Директива 2001/29/ЕО относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество²⁵, Директива 2004/48/ЕО относно упражняването на права върху интелектуалната собственост²⁶ и Директива 2002/58/ЕО не задължават държавите членки в хипотеза като тази в главното производство да предвидят задължение за съобщаване на лични данни, за да осигурят ефективна защита на авторското право в рамките на гражданско производство. Правото на Съюза обаче изисква при транспониране на тези директиви посочените държави да следят за тълкуване на директивите, което позволява да се осигури подходящо равновесие между различните основни права, защитени от общностния правен ред. На следващо място, при въвеждане на мерките за транспониране на посочените директиви органите и юрисдикциите на държавите членки са длъжни не само да тълкуват националното си право в съответствие с тези директиви, но и да не се основават на тълкуване на последните, което би влязло в конфликт с посочените основни права или с другите общи принципи на общностното право като принципа на пропорционалност (т. 70 и диспозитива).

²³ Това решение е представено в Годишния доклад за 2008 г., стр. 46.

²⁴ Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 17.7.2000 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 29, стр. 257).

²⁵ Директива 2001/29/ЕО на Европейския парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество (ОВ L 167, 22.6.2001 г., стр. 10; Специално издание на български език, 2007 г., глава 17, том 1, стр. 230).

²⁶ Директива 2004/48/ЕО на Европейския парламент и на Съвета от 29 април 2004 година относно упражняването на права върху интелектуалната собственост (ОВ L 157, 30.4.2004 г., стр. 45; Специално издание на български език, 2007 г., глава 17, том 2, стр. 56).

Решение от 24 ноември 2011 г., Scarlet Extended (C-70/10, EU:C:2011:771)²⁷

Société belge des auteurs, compositeurs et éditeurs SCRL (Белгийско дружество за защита на правата на авторите, композиторите и издателите, наричано по-нататък „SABAM“) установява, че някои интернет потребители, използващи услугите на доставчика на интернет достъп Scarlet Extended SA (наричано по-нататък „Scarlet“), качват в интернет произведения от неговия каталог чрез мрежи „peer-to-peer“, без да имат разрешение за това и без да плащат авторски възнаграждения. SABAM се обръща към националните съдилища и първоинстанционният съд разпорежда на Scarlet да преустанови тези посегателства върху авторското право, като направи невъзможна всяка форма на изпращане или приемане от неговите клиенти посредством софтуери „peer-to-peer“ на електронни файлове, възпроизвеждащи музикално произведение от репертоара на SABAM.

Scarlet обжалва пред Cour d'appel de Bruxelles (Брюкселски апелативен съд, Белгия), който спира производството, за да отправи преюдициално запитване до Съда дали такова разпореждане е съвместимо с европейското право.

Съдът постановява, че директиви 95/46/ЕО, 2000/31/ЕО, 2001/29/ЕО, 2002/58/ЕО и 2004/48/ЕО, разгледани заедно и във връзка с изискванията, произтичащи от защитата на приложимите основни права, трябва да се тълкуват в смисъл, че не допускат разпореждането до Scarlet да въведе система за филтриране на всички електронни съобщения, пренасяни посредством предлаганите от него услуги, по-специално чрез използването на софтуери „peer-to-peer“, която да прилага без разграничение към всички свои клиенти превантивно, изцяло на свои разноси и без ограничение във времето, и с която да може да се идентифицира в мрежата на този доставчик движението на електронни файлове, съдържащи музикално, кинематографско или аудио-визуално произведение, върху което ищецът твърди, че притежава права на интелектуална собственост, за да се блокира прехвърлянето на файлове, чийто обмен нарушава авторското право (т. 54 и диспозитива).

Всъщност според Съда подобно разпореждане не е съобразено нито със забраната по член 15, параграф 1 от Директива 2000/31/ЕО да се налага на тези доставчици общо задължение за контрол, нито с изискването за осигуряване на справедливо равновесие между правото на интелектуална собственост, от една страна, и свободата на стопанска инициатива и правото на защита на личните данни и свободата за получаване и разпространяване на информация, от друга (т. 40 и 49).

В този контекст Съдът отбелязва, че от една страна, разпореждането за въвеждане на спорната система за филтриране би предполагало систематичен анализ на цялото съдържание, както и събирането и идентифицирането на IP адресите на ползвателите, които са започнали изпращането на незаконното съдържание в мрежата, като тези адреси са защитени лични данни, тъй като позволяват точното идентифициране на ползвателите (т. 51). От друга страна, посоченото разпореждане създава опасност от нарушаване на свободата на информация, тъй като е възможно тази система да не разграничава в достатъчна степен незаконното от законното съдържание, така че прилагането ѝ може да доведе до блокиране на съобщения със законно съдържание. Въсъщност не се спори по това, че отговорът на въпроса за законността на дадено пренасяне на данни зависи и от прилагането на законовите изключения от авторското право, които се различават в различните държави членки. Освен това в някои държави членки някои произведения могат да спадат към публичната сфера или да са предмет на безплатно предоставяне онлайн от страна на съответните автори (т. 52).

²⁷ Това решение е представено в Годишния доклад за 2011 г., стр. 37.

Ето защо Съдът приема, че ако постанови разпореждане, задължаващо Scarlet да въведе спорната система за филтриране, съответната национална юрисдикция няма да спази изискването да осигури справедливо равновесие между правото върху интелектуална собственост, от една страна, и свободата на стопанската инициатива, правото на защита на личните данни и свободата на получаване или разпространяване на информация, от друга страна (т. 53).

Решение от 19 април 2012 г., Bonnier Audio и др. (C-461/10, EU:C:2012:219)

Högsta domstolen (Върховен съд, Швеция) отправя преюдициално запитване до Съда за тълкуването на директиви 2002/58/ЕО и 2004/48/ЕО във връзка със спор между Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB и Storyside AB (наричани по-нататък „Bonnier Audio и др.“), от една страна, и Perfect Communication Sweden AB (наричано по-нататък „ePhone“), от друга, по повод на възражението на последното срещу искане на Bonnier Audio и др. за издаване на съдебно разпореждане за разкриване на информация.

Bonnier Audio и др. са издателски дружества, които притежават по-конкретно изключителни права да възпроизвеждат, разпространяват и предоставят публичен достъп до 27 произведения под формата на аудиокниги. Те твърдят, че изключителните им права са били нарушени поради предоставения без тяхно съгласие публичен достъп до тези 27 произведения чрез FTP сървър („file transfer protocol“), който позволява обмен на файлове и прехвърляне на данни между компютри по интернет. Затова те искат от шведските съдилища да издадат разпореждане за разкриване на името и адреса на лицето, използвало IP адреса, от който се смята, че са изпращани въпросните файлове.

Сезиран с касационна жалба по делото, Högsta domstolen (Върховният съд) отправя запитване до Съда дали правото на Съюза допуска прилагането на въведена въз основа на член 8 от Директива 2004/48/ЕО разпоредба на националното право, която с цел да се идентифицира даден абонат, позволява доставчикът на интернет услуги да бъде задължен в рамките на гражданско производство да предостави на носителя на авторското право или на негов наследник информация за абоната с предоставен IP адрес, за който се твърди, че е използван за извършване на нарушението. Презюмира се, че лицето, което иска издаването на разпореждането, е представило доказателства за нарушаването на конкретно авторско право и че тази мярка е пропорционална.

Съдът най-напред припомня, че член 8, параграф 3 от Директива 2004/48/ЕО във връзка с член 15, параграф 1 от Директива 2002/58/ЕО допуска държавите членки да установяват задължение за предаване на лични данни на частноправни лица, за да могат те да предявят граждански иски за защита от нарушенията на авторското право, но същевременно не задължава държавите членки да предвидят такова задължение. Органите и юрисдикциите на държавите членки обаче са длъжни не само да тълкуват националното си право в съответствие с тези директиви, но и да не се основават на тълкуване на последните, което би влязло в конфликт с посочените основни права или с другите общи принципи на общностното право като принципа на пропорционалност (т. 55 и 56).

В това отношение Съдът констатира, че за да може да се издаде разпореждане за разкриване на разглежданите данни, въпросното национално законодателство изисква по-специално да има достатъчно данни за наличието на нарушение на право на интелектуална собственост, исканата информация да може да улесни разследването на нарушението на авторското право и целта на разпореждането да е по-значима от неудобствата или вредите, които то може да причини на засегнатото лице или на други лица с противоположни интереси (т. 58).

Затова Съдът стига до извода, че директиви 2002/58/ЕО и 2004/48/ЕО допускат национално законодателство като разглежданото в главното производство, доколкото това законодателство позволява на националната юрисдикция, която е сезирана с подадено от надлежна страна искане да се издаде разпореждане за разкриване на лични данни, да претегли съответните противоположни интереси, като съобрази обстоятелствата на конкретния случай и надлежно отчете изискванията, произтичащи от принципа на пропорционалност (т. 61 и диспозитива).

V. Национални надзорни органи

1. Обхват на изискването за независимост

Решение от 9 март 2010 г. (голям състав), Комисия/Германия (C-518/07, EU:C:2010:125)²⁸

С исковата си молба Комисията моли Съда да установи, че като е подчинила на контрола на държавата надзорните органи, които отговарят за наблюдението и контрола на обработването на лични данни извън публичния сектор в различните провинции и по този начин е транспонирила неправилно изискването за „пълна независимост“ на органите, натоварени да гарантират защитата на тези данни, Федерална република Германия не е изпълнила задълженията си по член 28, параграф 1, втора алинея от Директива 95/46/ЕО.

От своя страна Федерална република Германия поддържа, че член 28, параграф 1, втора алинея от Директива 95/46/ЕО изисква функционална независимост на надзорните органи, в смисъл че тези органи трябва да бъдат независими от контролирания от тях непубличен сектор и че те не трябва да бъдат изложени на външни влияния. Според нея обаче упражняваният в германските провинции контрол от страна на държавата не представлява такова външно влияние, а вътрешен за администрацията механизъм за наблюдение и контрол, осъществявани от органи, числящи се към същия административен апарат, към който спадат и надзорните органи, и длъжни, също както последните, да се съобразяват с целите на Директива 95/46/ЕО.

Съдът постановява, че предвидената в Директива 95/46/ЕО гаранция за независимост на националните надзорни органи цели да осигури ефективността и надеждността на надзора за спазване на разпоредбите в областта на защитата на физическите лица при обработване на лични данни и трябва да се тълкува в светлината на тази цел. Тя е установена не за да осигури особен статут на самите органи, както и на техните служители, а с цел да засили защитата на засегнатите от техните решения лица и организации, доколкото вследствие от нея надзорните органи трябва да действат обективно и безпристрастно при упражняването на своите функции (т. 25).

Според Съда тези надзорни органи, компетентни да наблюдават и контролират обработването на лични данни извън публичния сектор, трябва да се ползват с независимост, която да им дава възможност да изпълняват функциите си без външно влияние. Тази независимост изключва не само всяко упражнявано от контролираните организации влияние, а и всяко предписание и всяко друго външно влияние, независимо дали последното е пряко или косвено, които биха могли да застрашат изпълнението на задачата на посочените органи, състояща се в постигането на баланс между защитата на правото на личен живот и свободното движение на личните данни. Самата опасност органите, упражняващи контрол, да могат да упражняват политическо влияние върху решенията на компетентните надзорни органи е достатъчна, за да попречи на независимостта при

²⁸ Това решение е представено в Годишния доклад за 2010 г., стр. 34.

изпълнението на техните функции. От една страна, би могло да има „изпреварващо послушание“ на тези органи с оглед на практиката на контролния орган при взимане на решения. От друга страна, ролята на пазители на правото на личен живот, която посочените надзорни органи изпълняват, изисква по отношение на техните решения, и следователно на самите тях, да бъде изключено всякакво подозрение за пристрастност. Затова според Съда контролът, упражняван от държавата върху националните надзорни органи, не е съвместим с изискването за независимост (т. 30, 36, 37 и диспозитива).

Решение от 16 октомври 2012 г. (голям състав), Комисия/Австрия (С-614/10, EU:C:2012:631)

С исковата си молба Комисията моли Съда да установи, че като не е взела всички необходими мерки, за да съобрази действащото законодателство в Австрия с критерия за независимост, що се отнася до Datenschutzkommission (Комисия за защита на данните), създадена като надзорен орган за защита на личните данни, Австрия не е изпълнила задълженията си по член 28, параграф 1, втора алинея от Директива 95/46/ЕО.

Съдът установява, че Австрия не е изпълнила задълженията си, като по същество приема, че зададеният от Директива 95/46/ЕО критерий за независимост на надзорния орган не е изпълнен, когато държавата членка е въвела нормативна уредба, съгласно която управителният член на надзорния орган е държавен служител, подлежащ на административен контрол, секретариатът на надзорния орган е включен към службите на националното правителство, а ръководителят на правителството разполага с безусловно право на информация по всички аспекти от работата на надзорния орган (т. 66 и диспозитива).

Съдът най-напред припомня, че изразът „пълна независимост“ по член 28, параграф 1, втора алинея от Директива 95/46/ЕО означава, че надзорните органи трябва да се ползват с независимост, която да им дава възможност да изпълняват функциите си без външно влияние. В това отношение обстоятелството, че съответният орган разполага с функционална независимост, доколкото членовете му са независими и не са обвързани от никакви инструкции при изпълнението на своите функции, не е достатъчно само по себе си, за да предпази надзорния орган от всякакво външно влияние. Същевременно изискваната в този контекст независимост предполага да е изключено не само прякото влияние под формата на инструкции, но и всяка форма на косвено влияние, което би могло да насочва решенията на надзорния орган. Освен това ролята на пазители на правото на личен живот, която надзорните органи изпълняват, изисква по отношение на техните решения и следователно на самите тях да бъде изключено всякакво подозрение за пристрастност (т. 41—43 и 52).

Съдът пояснява, че не е необходимо националният надзорен орган да разполага с отделна бюджетна линия подобно на предвидената в член 43, параграф 3 от Регламент (ЕО) № 45/2001, за да може да отговаря на критерия за независимост по упоменатата разпоредба от Директива 95/46/ЕО. Всъщност държавите членки не са длъжни да възпроизведат в националното си законодателство аналогични на предвидените в глава V от Регламент (ЕО) № 45/2001 разпоредби, за да гарантират пълна независимост на своите надзорни органи, и в този смисъл могат за бюджетни цели да зачислят надзорния орган към някое министерство. Въпреки това осигуряването на този орган с персонал и материално оборудване не трябва да съставлява пречка за упражняването на функциите му при „пълна независимост“ по смисъла на член 28, параграф 1, втора алинея от Директива 95/46/ЕО (т. 58).

Решение от 8 април 2014 г. (голям състав), Комисия/Унгария (C-288/12, EU:C:2014:237)²⁹

По това дело Комисията моли Съда да установи, че с предсрочното прекратяване на мандата на надзорния орган за защита на личните данни Унгария е допуснала неизпълнение на задълженията си по Директива 95/46/ЕО.

Съдът постановява, че държава членка, която прекратява предсрочно мандата на надзорния орган за защита на личните данни, не изпълнява задълженията си по Директива 95/46/ЕО (т. 62; т. 1 от диспозитива).

Всъщност според Съда независимостта, с която трябва да се ползват надзорните органи, компетентни да наблюдават обработването на лични данни, изключва по-специално всяко предписание и всяко друго външно влияние под каквато и да е форма, независимо дали последното е пряко или косвено, които биха могли да насочат решенията им и по този начин биха могли да застрашат изпълнението на задачата на посочените органи, състояща се в постигането на справедлив баланс между защитата на правото на личен живот и свободното движение на личните данни (т. 51).

Съдът също така припомня, че функционална независимост сама по себе си не е достатъчна, за да предпази надзорните органи от всякакво външно влияние, доколкото самата опасност органите, упражняващи държавен контрол, да могат да упражняват политическо влияние върху решенията на надзорните органи, е достатъчна, за да попречи на независимостта при изпълнението на техните функции. Ако беше допустимо всяка държава членка да прекратява мандата на надзорния орган преди изтичането на първоначално предвидения краен срок, без да спазва правилата и гаранциите, предварително установени за тази цел от приложимото законодателство, заплахата от подобно предсрочно прекратяване, която би съществувала за този орган през целия период на упражнявания от него мандат, би могла да доведе до някаква форма на послушание на този орган към политическата власт, несъвместимо с посоченото изискване за независимост. Освен това при такава хипотеза не би могло да се счита, че надзорният орган може винаги да функционира извън всякакво подозрение за пристрастност (т. 52—55).

2. Определяне на приложимото право и на компетентния надзорен орган**Решение от 1 октомври 2015 г., Weltimmo (C-230/14, EU:C:2015:639)³⁰**

Nemzeti Adatvédelmi és Információszabadság Hatóság (национален орган за защита на данните и за свободата на информацията, Унгария) налага глоба на регистрираното в Словакия дружество Weltimmo, което управлява уебсайтове с обяви за недвижими имоти, отнасящи се до имоти в Унгария, по съображение че това дружество не е заличавало личните данни на подателите на обявите въпреки техните искания в този смисъл и е съобщавало тези данни на дружества за събиране на вземания с оглед на заплащането на неплатени фактури. Според унгарския надзорен орган по този начин дружеството Weltimmo е нарушило унгарския закон, с който се транспонира Директива 95/46/ЕО.

Сезиран с касационна жалба, Kúria (Върховен съд, Унгария) изразява съмнения относно определянето на приложимото право и правомощията на унгарския надзорен орган предвид член 4, параграф 1 и член 28 от Директива 95/46/ЕО. Затова той отправя няколко преюдициални въпроса до Съда.

²⁹ Това решение е представено в Годишния доклад за 2014 г., стр. 62.

³⁰ Това решение е представено в Годишния доклад за 2015 г., стр. 55.

Що се отнася до приложимото национално право, Съдът постановява, че член 4, параграф 1, буква а) от Директива 95/46/ЕО допуска законодателството на дадена държава членка относно защитата на личните данни да бъде приложено в друга държава членка, различна от държавата по регистрацията на администратора на тези данни, доколкото последният упражнява на територията на тази държава членка, посредством постоянен обект, дори минимална ефективна и действителна дейност, в чийто контекст се извършва разглежданото обработване на данни. За да определи дали конкретният случай е такъв, запитващата юрисдикция може по-специално да вземе предвид факта, че от една страна, дейността на администратора, в чийто контекст се извършва посоченото обработване на данни, се състои в експлоатирането на уебсайтове със съставени на езика на тази държава членка обяви за недвижими имоти, намиращи се на територията на тази държава членка, поради което тази дейност е предимно или изцяло насочена към посочената държава членка. От друга страна, запитващата юрисдикция може да вземе предвид и факта, че този администратор има представител в посочената държава членка, на когото е възложено да събира вземанията, произтичащи от тази дейност, както и да представлява администратора в административните и съдебните производства относно обработването на разглежданите данни. За сметка на това Съдът приема, че е ирелевантен въпросът какво е гражданството на лицата, засегнати от това обработване (т. 41; т. 1 от диспозитива).

Що се отнася до компетентността и правомощията на надзорния орган, сезиран с жалби в съответствие с член 28, параграф 4 от Директива 95/46/ЕО, Съдът приема, че този орган може да разглежда тези жалби независимо от приложимото право и дори преди да бъде установено кое е националното право, приложимо към разглежданото обработване на данни (т. 54). Въпреки това, ако този орган стигне до заключението, че е приложимо правото на друга държава членка, той няма право да налага санкции извън територията на собствената си държава членка. Ако случаят е такъв, този орган е длъжен, в изпълнение на задължението за сътрудничество по член 28, параграф 6 от тази директива, да поиска от надзорния орган на тази друга държава членка да установи евентуалното нарушение на това право и да наложи съответните санкции, ако националното му право допуска това, позовавайки се при необходимост на предоставената му информация (т. 57 и 60; т. 2 от диспозитива).

3. Правомощия на националните надзорни органи

Решение от 6 октомври 2015 г. (голям състав), Schrems (C-362/14, EU:C:2015:650)

По това дело (вж. също рубрика III, „Предаване на лични данни на трети страни“) Съдът в частност постановява, че националните надзорни органи са компетентни да контролират предаването на лични данни към трети страни.

В това отношение Съдът най-напред констатира, че националните надзорни органи разполагат с широк набор от правомощия, които са изброени неизчерпателно в член 28, параграф 3 от Директива 95/46/ЕО и които представляват необходимите средства, за да изпълняват органите своите задължения. Така органите разполагат по-специално с правомощия по разследване, като например правомощия за събиране на цялата информация, необходима за изпълнението на функциите по надзора; с ефективни правомощия за намеса, като например правомощия за въвеждане на временна или окончателна забрана върху обработването на данни, и с правомощия да водят съдебни дела (т. 43).

Що се отнася до правомощията за контрол върху предаването на лични данни към трети страни, Съдът постановява, че безспорно от член 28, параграфи 1 и 6 от Директива 95/46/ЕО следва, че правомощията на националните надзорни органи се отнасят до обработването на лични данни, извършвано на територията на държавата членка, към която принадлежат тези органи, и

съответно член 28 не им предоставя правомощия по отношение на обработването на тези данни, извършвано на територията на трета страна (т. 44).

Същевременно операцията по прехвърляне на лични данни от държава членка към трета страна сама по себе си представлява обработване на лични данни, извършвано на територията на държава членка. Тъй като в съответствие с член 8, параграф 3 от Хартата и член 28 от Директива 95/46/ЕО националните надзорни органи са натоварени с осъществяването на контрола по спазването на правилата на Съюза относно защитата на физическите лица при обработването на лични данни, всеки от тях съответно разполага с правомощия да проверява дали дадено прехвърляне на лични данни от държавата членка, към която спада съответният орган, към трета страна отговаря на въведените с тази директива изисквания (т. 45 и 47).

VI. Териториална приложимост на европейското законодателство

Решение от 13 май 2014 г. (голям състав), Google Spain и Google (C-131/12, EU:C:2014:317)

В това решение (вж. също рубрика II.3, „Понятие за обработване на лични данни“, и рубрика IV.1, „Право на възражение срещу обработването на лични данни („право на забравя“)) Съдът се произнася и относно териториалния обхват на Директива 95/46/ЕО.

Съдът постановява, че обработването на лични данни се извършва в контекста на дейностите на установен на територията на държава членка обект на администратора по смисъла на Директива 95/46/ЕО, когато лицето, което управлява интернет търсачка, макар да е със седалище в трета държава, създава в държава членка клон или дъщерно дружество, чието предназначение е да осигури рекламирането и продажбата на рекламните пространства, предлагани от търсачката, и чиято дейност е насочена към жителите на тази държава членка (т. 55 и 60; т. 2 от диспозитива).

Всъщност при подобни обстоятелства дейностите на лицето, което управлява интернет търсачката, и тези на неговия обект, установен в държава членка, макар и различни, са неразделно свързани, тъй като дейностите, свързани с рекламните пространства, представляват средството, даващо икономическа рентабилност на разглежданата търсачка, и тази търсачка е същевременно средството, което позволява осъществяването на тези дейности (т. 56).

VII. Право на публичен достъп до документите на институциите на Европейския съюз и защита на личните данни

Решение от 29 юни 2010 г. (голям състав), Комисия/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Дружеството Bavarian Lager, което е създадено с цел внос на германска бира, предназначена за продажба в заведения за консумация на място в Обединеното кралство, не успява да продаде стоката си, тъй като голяма част от лицата, които стопанисват и управляват заведения за консумация на място в Обединеното кралство, са обвързани с договори за продажба с изключителни права, които ги задължават да се снабдяват с бира от определени пивоварници.

Съгласно действащата в Обединеното кралство уредба на доставките на бира (Guest Beer Provision, наричана по-нататък „GBP“) британските пивоварници са длъжни да предоставят на управителите на заведенията възможността да закупуват бира от други пивоварници, при условие че тя е наливна. Повечето от произведените извън Обединеното кралство видове бира обаче не могат да се считат за „наливна бира“ по смисъла на GBP и следователно не попадат в приложното поле на тази уредба. Тъй като смята, че въпросната уредба е мярка с равностоеен на количествено ограничение на вноса ефект, Bavarian Lager подава жалба до Комисията.

На 11 октомври 1996 г. в хода на воденото срещу Обединеното кралство производство пред Комисията за установяване на неизпълнение на задължения се провежда събрание, в което участват представители на общността и британската администрация и на Конфедерацията на пивоварите от общия пазар (КПОП). След като е уведомена от британските власти за изменение на спорната правна уредба, което има за цел да позволи продажбата на бутилирана бира като бира с различен произход, подобно на наливната бира, Комисията информира Bavarian Lager за спирането на производството за неизпълнение на задължения.

Bavarian Lager подава заявление да получи пълния протокол от събранието от октомври 1996 г. с имената на всички участници, но Комисията отхвърля това заявление с решение от 18 март 2004 г., като се позовава в частност на защитата на личния живот на участниците, гарантирана от регламента за защита на личните данни.

Тогава Bavarian Lager обжалва решението на Комисията пред Общия съд, като иска то да бъде отменено. С решение от 8 ноември 2007 г. Общият съд отменя решението на Комисията, като приема, че самото включване на името на съответните лица в списъка на лицата, които са участвали в събранието от името на представляваната от тях организация, не представлява засягане и не поставя в опасност личния живот на тези лица. Комисията, подпомагана от Обединеното кралство и Съвета, подава жалба до Съда против това решение на Общия съд.

Съдът най-напред отбелязва, че когато е подадено заявление на основание на Регламент (ЕО) № 1049/2001³¹ за получаване на достъп до документи, които съдържат лични данни, разпоредбите на Регламент (ЕО) № 45/2001 се прилагат изцяло, в това число разпоредбата, която задължава получателя на лични данни да удостовери необходимостта от тяхното оповестяване, както и разпоредбата, която предоставя на субекта на данни възможността по всяко време, позовавайки се на непреодолими легитимни основания, свързани с конкретното му положение, да възрази срещу обработката на свързани с него данни (т. 63).

По-нататък Съдът констатира, че включеният в протокола от събрание списък с участниците в това събрание, проведено в рамките на производство за установяване на неизпълнение на задължения, съдържа лични данни по смисъла на член 2, буква а) от Регламент (ЕО) № 45/2001, тъй като лицата, които са могли да присъстват на това събрание, могат да бъдат идентифицирани (т. 70).

Накрая Съдът заключава, че като е изисквала да е установена необходимостта от предаване на личните данни относно лицата, които не са дали изрично съгласие за разкриването на съдържащите се в протокола техни лични данни, Комисията се е съобразила с разпоредбите на член 8, буква б) от този регламент (т. 77).

Всъщност, при положение че във връзка с подаденото заявление за достъп до протокола на основание на Регламент (ЕО) № 1049/2001 не са предоставени никаква изрична и легитимна

31 Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 година относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43; Специално издание на български език, 2007 г., глава 1, том 3, стр. 76).

обосновка, нито убедителен довод, за да се докаже необходимостта от предаване на тези лични данни, Комисията не може да претегли различните интереси на съответните страни. Тя не може и да провери дали няма основания да се предполага, че това предаване би могло да засегне легитимните интереси на субектите на данните, както е предвидено в член 8, буква б) от Регламент (ЕО) № 45/2001 (т. 78)³².

Решение от 16 юли 2015 г., ClientEarth и PAN Europe/ЕОБХ (С-615/13 Р, ЕУ:С:2015:489)

Европейският орган за безопасност на храните (ЕОБХ) създава работна група, която да изготви насоки за прилагането на член 8, параграф 5 от Регламент (ЕО) № 1107/2009³³, който гласи, че заявителят за разрешение за търговия с продукт за растителна защита трябва да приложи към досието експертно проверената актуална научна литература, както е определена от ЕОБХ, относно активното вещество и съответните му метаболити, свързана със страничните ефекти върху здравето, околната среда и неприцелни видове.

Проектът за насоки е подложен на обществени консултации, при което ClientEarth и Pesticide Action Network Europe (PAN Europe) представят становища по него. В този контекст те подават съвместно до ЕОБХ заявление за достъп до няколко документа относно изготвянето на проекта за насоки, в това число становищата на външните експерти.

ЕОБХ разрешава достъп на ClientEarth и PAN Europe в частност до отделните становища на външните експерти по проекта за насоки. ЕОБХ обаче посочва, че е заличил имената на експертите в съответствие с член 4, параграф 1, буква б) от Регламент (ЕО) № 1049/2001, както и в съответствие със законодателството на Съюза относно защитата на личните данни, в частност Регламент (ЕО) № 45/2001. В това отношение ЕОБХ изтъква, че оповестяването на имената на експертите представлява предаване на лични данни по смисъла на член 8 от Регламент (ЕО) № 45/2001 и че посочените в този член условия за предаване на данни не са налице в настоящия случай.

Тогава ClientEarth и PAN Europe подават жалба до Общия съд, като искат да отмени това решение на ЕОБХ. Тъй като Общият съд отхвърля жалбите им, ClientEarth и PAN Europe обжалват решението му³⁴ пред Съда.

На първо място, Съдът отбелязва, че доколкото исканата информация би позволила да се направи връзка между определен експерт и дадено становище, тя се отнася до физически лица с установена самоличност и следователно представлява съвкупност от лични данни по смисъла на член 2, буква а) от Регламент (ЕО) № 45/2001. Тъй като понятията „лични данни“ по смисъла на член 2, буква а) от Регламент (ЕО) № 45/2001 и „данни, свързани с личния живот“ не се сливат, Съдът също така приема, че твърдението на ClientEarth и PAN Europe, че спорната информация не попада в обхвата на личния живот на съответните експерти, е неотнормимо (т. 29 и 32).

На второ място, Съдът разглежда довода на ClientEarth и PAN Europe, че е налице атмосфера на недоверие спрямо ЕОБХ, често обвиняван в пристрастие поради факта, че прибегва до експерти, които имат лични интереси, диктувани от връзките им с промишлените среди, както и че е необходимо да се гарантира прозрачността на процеса на вземане на решения на този орган. Този довод е подкрепен от проучване, което установява поддържаните връзки от по-голямата част от експертите, членове на работна група на ЕОБХ, с групи за натиск в промишлеността. В това

32 Това решение е представено в Годишния доклад за 2010 г., стр. 14.

33 Регламент (ЕО) № 1107/2009 на Европейския парламент и на Съвета от 21 октомври 2009 година относно пускането на пазара на продукти за растителна защита и за отмяна на директиви 79/117/ЕИО и 91/414/ЕИО на Съвета (ОВ L 309, 24.11.2009 г., стр. 1).

34 Решение на Общия съд от 13 септември 2013 г., ClientEarth и PAN Europe/ЕОБХ (Т-214/11, ЕУ:Т:2013:483).

отношение Съдът постановява, че получаването на спорната информация се оказва необходимо, за да се провери конкретно безпристрастността на всеки от тези експерти при изпълнение на научното им задание в служба на ЕОБХ. Затова Съдът отменя решението на Общия съд, като констатира, че той неправилно е постановил, че въпросният довод на ClientEarth и PAN Europe не е достатъчен, за да се докаже необходимостта от предаване на спорната информация (т. 57—59).

На трето място, за да прецени законосъобразността на спорното решение на ЕОБХ, Съдът проверява дали има основание или не да се предполага, че предаването би могло да засегне легитимните интереси на субектите на данните. В това отношение той констатира, че твърдението на ЕОБХ, че оповестяването на спорната информация би могло да накърни личния живот и неприкосновеността на посочените експерти, представлява общо съображение, което иначе не е подкрепено от каквото и да е доказателство в конкретния случай. Съдът приема, че напротив, подобно оповестяване би позволило само по себе си да се разсеят съмненията за пристрастие в случая или би предоставило на евентуално засегнатите експерти възможността да оспорят, ако е необходимо посредством наличните средства за защита, основателността на твърденията за пристрастие. По тези съображения Съдът отменя и решението на ЕОБХ (т. 69 и 73).

* * *

Всички упоменати в този фиш решения са индексирани в Справочника на съдебната практика, рубрики 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 и 4.11.07.