СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
ДИРЕКЦИЯ „ИЗСЛЕДВАНИЯ И ДОКУМЕНТАЦИЯ“

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 данни[1], която е приета на основание член 100А ЕО, по онова време е основният правен акт на Съюза в тази област. Тя

[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, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10), консолидиран текст към 20.11.2003 г., отменена, считано от 25 май 2018 г. (вж. бележка под линия 5).

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.

Впоследствие към Директива 95/46 се добавя Директива 2002/58/ЕО[2], 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 съобщения[3]. Следва да се отбележи, че законодателят на Съюза планира да преразгледа тази директива. Във връзка с това на 10 януари 2017 г. Комисията внася предложение за заместването ѝ с регламент за неприкосновеността на личния живот и електронните съобщения[4].

Освен това в пространството на свобода, сигурност и правосъдие (старите членове 30 ДЕС и 31 ДЕС) до май 2018 г. защитата на личните данни в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси е уредена с Рамково решение 2008/977/ПВР[5].

През 2016 г. Европейският съюз реформира общата правна рамка в тази област. За целта са приети Регламент (ЕС) 2016/679[6] относно защитата на данните (наричан по-нататък „ОРЗД“), който отменя Директива 95/46 и е пряко приложим от 25 май 2018 г., както и Директива (ЕС) 2016/680[7] за защита на данните в наказателната област, която отменя Рамково решение 2008/977/ПВР, а крайният срок за транспонирането ѝ в държавите членки е 6 май 2018 г.

Накрая, защитата на личните данни, обработвани от институциите и органите на ЕС, първо е гарантирана с Регламент (ЕО) № 45/2001[8]. Въз основа на този регламент през 2004 г. е създаден Европейският надзорен орган по защита на данните. През 2018 г.

---

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, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63), консолидиран текст към 19 декември 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, 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. (C-293/12 и C-594/12, EU:C:2014:238), Съдът обявява тази директива за невалидна, тъй като създава тежко посегателство 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 Предложение за Регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения), COM/2017/010 final — 2017/03 (COD).

5 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, 2008 г., стр. 60), отменено, считано от 6 май 2018 г. (вж. бележка под линия 6).

6 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, 2016 г., стр. 1).

7 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 119,2016 г., стр. 89).

8 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, 2001 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 30, стр. 142).

Европейският съюз се сдобива с нова правна рамка в тази област вследствие на приемането на Регламент (ЕС) 2018/1725[9], който отменя Регламент № 45/2001 и Решение № 1247/2002/ЕО[10] и се прилага от 11 декември 2018 г. С новия регламент правилата в тази област се привеждат в съответствие, доколкото е възможно, с новия режим по ОРЗД в интерес на постигането на съгласуван подход към защитата на личните данни навсякъде в Съюза.

[9] Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 година 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.

[10] Решение № 1247/2002/ЕО на Европейския парламент, на Съвета и на Комисията от 1 юли 2002 година относно статута и общите условия, регулиращи изпълнението на задълженията на Европейския надзорен орган по защита на данните (ОВ L 183, 2002 г., стр. 1; Специално издание на български език, 2007 г., глава 1, том 3, стр. 194).

Съдържание

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)[11]

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, отнасящи 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) № 1290/2005[12] и № 259/2008[13], 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 № 1290/2005 и на Регламент № 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).

---

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

12 Регламент (ЕО) № 1290/2005 на Съвета от 21 юни 2005 година относно финансирането на Общата селскостопанска политика (ОВ L 209, 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, 2013 г., стр. 549).

13 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, 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, уравняването на сметките, правилата за проверките, обезпеченията и прозрачността (ОВ L 255, 2014 г., стр. 59).

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 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 № 1290/2005, както и целия Регламент № 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 и 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, предшестващ датата на постановяване на решението му (т. 94 и 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 властите на град Бохум (Германия) да му бъде издаден паспорт, като същевременно отказва да бъдат снети в тази връзка пръстовите му отпечатъци. 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 пръстовите отпечатъци. Пред тази юрисдикция г-н Schwarz оспорва валидността на Регламент (ЕО) № 2252/2004[14], който въвежда задължението за снемане на пръстовите отпечатъци 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 пръстовите си отпечатъци и предвижда съхраняването на тези отпечатъци в паспорта.

[14] 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, 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, 2009 г., стр. 1).

Съдът отговаря утвърдително, като постановява, че наистина снемането и съхраняването на пръстови отпечатъци от националните власти, уредено в член 1, параграф 2 от Регламент № 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 отпечатъци са в състояние да осъществят тази цел. Всъщност, от една страна, въпреки че методът на проверка на самоличността посредством пръстови отпечатъци не е напълно надежден, той снижава значително риска от допускането на неоторизирани лица. От друга страна, липсата на съвпадение на пръстовите отпечатъци 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).

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 отпечатъци (т. 53). Член 1, параграф 2 от Регламент № 2252/2004 не изисква обработване на снетите пръстови отпечатъци, което да надхвърля необходимото за постигането на търсената цел. Всъщност този регламент уточнява изрично, че пръстовите отпечатъци 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 отпечатъци, от неоторизирани лица и предвижда съхраняването на пръстови отпечатъци 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)[15]

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 в австрийското право.

[15] Това решение е представено в Годишния доклад за 2014 г., стр. 63.

С преюдициалните си запитвания ирландската и австрийската юрисдикция молят Съда да се произнесе по валидността на Директива 2006/24 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 общественодостъпни 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 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 изискването от Директивата запазване на данните не би могло да засегне съществото съдържание на основното право на зачитане на 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 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 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)[16]

След като с решение Digital Rights Ireland и Seitlinger и др. обявява за невалидна Директива 2006/24 (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.

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.

[16] Това решение е представено в Годишния доклад за 2016 г., стр. 62.

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, 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 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 и 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 и т. 2 от диспозитива).

За сметка на това Съдът приема, че член 15, параграф 1 от Директива 2002/58 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 общата уредба в тази област

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 (C-317/04 и C-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/ЕО[17], в което констатира, че служба „Митници и гранична защита“ на САЩ (United States Bureau of Customs and Border Protection, наричана по-нататък „CBP“) 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/ЕО[18], с което одобрява сключването на споразумение между Европейската общност и САЩ относно обработването и предаването на CBP 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.

---

[17] 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, 2004 г., стр. 11).

[18] 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, 2004 г., стр. 83).

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 CBP представлява обработване на тези данни за целите на обществената сигурност и дейностите 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 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 неколкократни 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 (Пражки градски съд, Чехия) потвърждава решението на тази служба, Nejvyšší správní soud (Върховен административен съд, Чехия) 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, 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, 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)[19]

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.

[19] Това решение е представено в Годишния доклад за 2016 г., стр. 61.

В този контекст Bundesgerichtshof (Федерален върховен съд, Германия), сезиран с ревизионна жалба по делото, отправя запитване до Съда дали IP адресът, записван 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, 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 уебсайт, 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 и т. 1 от диспозитива).

Решение от 20 декември 2017 г., Nowak (C-434/16, EU:C:2017:994)

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 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, 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“ (т. 31 и 36—40).

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 (т. 42 и 43).

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 — и да бъдат поправени или изтрити 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 не обхващат изпитните въпроси, които сами по себе си не представляват лични данни на кандидата (т. 56 и 58).

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 (т. 62 и диспозитива).

3. Понятие за обработване на лични данни

Решение от 6 ноември 2003 г. (голям състав), 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.

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 и 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 и 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 продан на недвижимо имущество във връзка с принудително изпълнение на негови задължения. С жалбата си той иска, от една страна, да се разпореди 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 разпореди 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.

Съдът постановява, че дейността на интернет търсачка, изразяваща се в намиране на публикувана или въведена в интернет от трети лица информация, автоматичното ѝ индексиране, 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. Евентуална обща дерогация от прилагането на Директивата в тази хипотеза до голяма степен би лишила посочената директива от смисъл (т. 29 и 30).

Решение от 10 юли 2018 г. (голям състав), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)[20]

Финландският орган по защита на данните издава решение, с което забранява на религиозната общност „Свидетели на Йехова“ да събира и обработва лични данни при извършваната от членовете ѝ проповедническа дейност „от врата на врата“, доколкото не са изпълнени изискванията на финландското законодателство относно обработването на лични данни. Всъщност при проповедническата си дейност „от врата на врата“ членовете на тази общност водят записки за направените посещения на лица, които самите те или посочената общност не познават. Тези данни са събирани като напомнителни бележки, за да може информацията да бъде намерена при следващи посещения, като съответните лица нито са давали съгласие, нито са били уведомявани за това. Религиозната общност „Свидетели на Йехова“ е дала на членовете си указания за воденето на такива записки, като тези указания са фигурирали в поне един от информационните ѝ бюлетини, посветени на проповедническата дейност.

Съдът постановява, че събирането на лични данни, извършвано от членове на религиозна общност при проповедническата им дейност „от врата на врата“, и по-нататъшното обработване на тези данни не попадат в обхвата на изключенията от приложното поле на Директива 95/46, тъй като не представляват нито обработване на лични данни при извършване на дейности, посочени в член 3, параграф 2, първо тире от тази директива, нито обработване на лични данни, извършвано от физически лица в хода

[20] Това решение е представено в Годишния доклад за 2018 г., стр. 93.

на изцяло лични или домашни занимания по смисъла на член 3, параграф 2, второ тире от същата директива (т. 51 и т. 1 от диспозитива).

Решение от 14 февруари 2019 г., Buivids (C-345/17, EU:C:2019:122)

По това дело Съдът се спира на тълкуването на приложното поле на Директива 95/46, от една страна, и на понятието „обработване на лични данни единствено за целите на журналистическа дейност“ по член 9 от тази директива, от друга.

Решението му е постановено по преюдициално запитване от латвийския върховен съд във връзка със спор между г-н Buivids (наричан по-нататък „жалбоподателят“) и националния орган за защита на данните по повод на искане да се обяви за незаконосъобразно решението, с което този орган приема, че г-н Buivids е нарушил националното законодателство в областта на защитата на данните, като е публикувал в уебсайт заснет от самия него видеозапис със снемането на показанията му от служители на полицията в помещенията на участък на националната полиция в рамките на административно-наказателно производство. След като двете предходни съдебни инстанции отхвърлят жалбата му, жалбоподателят подава касационна жалба до Върховния съд. Пред него той се позовава на правото си на свобода на словото и изтъква, че въпросният видеозапис показва служители на националната полиция, тоест публични личности, на общественодостъпно място и че поради това за тези лица не се прилагат разпоредбите на законодателството за защита на данните.

На първо място, що се отнася до приложното поле на Директива 95/46, Съдът отбелязва, че образите на заснетите на видеозаписа полицейски служители представляват лични данни и че видеозаписът на тези лица, запазен в паметта на използваната от жалбоподателя камера, представлява обработване на лични данни. Съдът добавя, че публикуването на видеозапис с лични данни в уебсайт за видеоматериали, които потребителите могат да гледат и споделят, представлява изцяло или частично автоматизирано обработване на тези данни. Освен това Съдът подчертава, че посоченият видеозапис и публикуването му не попадат в обхвата на предвидените изключения от приложното поле на Директива 95/46, които се отнасят по-конкретно до обработването на лични данни при упражняването на дейности, които не попадат в приложното поле на Директивата, и до обработването на такива данни в хода на изцяло лични или домашни занимания. Затова Съдът заключава, че в приложното поле на Директивата попада видеозаснемането на полицейски служители в полицейски участък при снемане на показания и публикуването на заснетия видеозапис в уебсайт за видеоматериали, на който потребителите могат да изпращат, гледат и споделят такива материали (т. 31, 32, 35, 39, 42 и 43 и т. 1 от диспозитива).

На второ място, що се отнася до обхвата на понятието „обработване на лични данни единствено за целите на журналистическа дейност“, Съдът най-напред припомня, че доколкото е необходимо широко тълкуване на понятието „журналистическа дейност“, предвидените в член 9 от Директива 95/46 изключения и дерогации се прилагат към всяко лице, което упражнява журналистическа дейност. В този смисъл Съдът постановява, че макар жалбоподателят да не е журналист по професия, това обстоятелство не изключва възможността заснемането на спорния видеозапис и предаването му да могат да се

квалифицират като „обработване на лични данни единствено за целите на журналистическа дейност“. Наред с това Съдът подчертава, че изключенията и дерогациите, предвидени в член 9 от Директива 95/46, трябва да се прилагат само доколкото са необходими за съгласуване на две основни права, а именно правото на защита на личния живот и свободата на словото. В това отношение Съдът пояснява, че не би могло да се изключи вероятността заснемането и публикуването на спорния видеозапис, без показаните на него полицейски служители да са информирани за заснемането и неговите цели, да представляват намеса в основното право на зачитане на личния живот на тези лица. Затова той заключава, че заснемането на въпросния видеозапис и публикуването му в уебсайт за видеоматериали може да представляват обработване на лични данни единствено за целите на журналистическа дейност, при условие че от посочения запис е видно, че заснемането и публикуваното имат за цел единствено публичното разгласяване на информация, мнения или идеи, което запитващата юрисдикция следва да провери (т. 51, 52, 55, 63, 67 и т. 2 от диспозитива).

Решение от 22 юни 2021 г. (голям състав), Latvijas Republikas Saeima (Наказателни точки) (C-439/19, EU:C:2021:504)

В е физическо лице, на което са наложени точки за едно или няколко пътнотранспортни нарушения. Наказателните точки са вписани от Ceļu satiksmes drošības direkcija (Дирекция „Безопасност на движението по пътищата“, Латвия) (наричана по-нататък „CSDD“) в националния регистър на превозните средства и техните водачи.

Съгласно латвийските правна уредба относно движението по пътищата[21] информацията за наказателните точки, наложени на водачи на превозни средства, вписани в този регистър, е достъпна за обществеността и се съобщава от CSDD на всяко лице, което я поиска, без да е необходимо това лице да обосновава конкретен интерес от получаването ѝ, включително на икономически оператори с цел повторна употреба. Тъй като изпитва съмнения относно законосъобразността на тази уредба, В подава конституционна жалба до Latvijas Republikas Satversmes tiesa (Конституционен съд, Латвия) с искане да разгледа съответствието ѝ с правото на зачитане на личния живот.

Конституционният съд приема, че при преценката на това конституционно право трябва да вземе предвид ОРЗД. В тази връзка той иска от Съда да изясни обхвата на няколко разпоредби на ОРЗД, за да определи съвместимостта на латвийската правна уредба относно движението по пътищата с този регламент.

В решението си, постановено от голям състав, Съдът приема, че обработването на лични данни относно наказателните точки представлява „обработване на лични данни, свързани с присъди и нарушения“ [22], за което ОРЗД предвижда засилена защита поради особената чувствителност на съответните данни (т. 10, 46, 74, 94 и т. 1 от диспозитива).

[21] Член 14[1], параграф 2 от Ceļu satiksmes likums (Закон за движението по пътищата) от 1 октомври 1997 г. (Latvijas Vēstnesis, 1997 г., бр. 274/276).

[22] Член 10 от ОРЗД.

В този контекст той отбелязва като начало, че данните относно наказателните точки са лични данни и че съобщаването им от CSDD на трети лица представлява обработване, което попада в материалното приложно поле на ОРЗД. Всъщност това приложно поле е много широко и посоченото обработване не спада към изключенията от приложимостта на този регламент (т. 60, 61 и 72).

Така, от една страна, разглежданото обработване не попада в обхвата на изключението, свързано с неприлагане на ОРЗД към обработване в хода на дейност, която е извън приложното поле на правото на Съюза[23]. Това изключение следва да се разглежда като имащо за единствен предмет изключването от приложното поле на посочения регламент обработването на лични данни, извършвано от държавните органи в рамките на дейност, насочена към запазване на националната сигурност, или на дейност, която може да бъде причислена към същата категория. Тези дейности обхващат по-специално защитата на съществените функции на държавата и на основните интереси на обществото. Дейностите, свързани с безопасността на движението по пътищата, обаче не преследват такава цел и следователно не могат да бъдат причислени към категорията на дейностите, чиято цел е защитата на националната сигурност (т. 62 и 66—68).

От друга страна, съобщаването на личните данни относно наказателните точки не съставлява и обработване, което попада в приложното поле на изключението, предвиждащо неприлагане на ОРЗД към обработване на лични данни от компетентните органи в наказателната сфера[24]. Всъщност Съдът приема, че в рамките на посоченото съобщаване CSDD не може да се счита за такъв „компетентен орган“ (т. 69—71)[25].

За да определи дали достъпът до личните данни относно точките за пътнотранспортни нарушения като наказателните точки представлява обработване на лични данни, отнасящо се до „нарушения“ [26], което се ползва със засилена защита, Съдът констатира, като се основава по-специално на процеса на създаването на ОРЗД, че това понятие се позовава изключително на престъпленията. При все това фактът, че в латвийската правна система пътнотранспортните нарушения са квалифицирани като административни, не е определящ при преценката дали тези нарушения попадат в обхвата на понятието за престъпление, доколкото става въпрос за самостоятелно понятие на правото на Съюза, което изисква самостоятелно и еднакво тълкуване навсякъде в Съюза. Така, след като припомня трите релевантни критерия за преценка на наказателноправния характер на дадено нарушение, а именно правната квалификация на нарушението във вътрешното право, естеството на нарушението и степента на строгост на наложената санкция, Съдът приема, че разглежданите пътнотранспортни нарушения попадат в обхвата на понятието „нарушение“ по смисъла на ОРЗД. Що се отнася до първите два критерия, Съдът констатира, че макар разглежданите нарушения да не са квалифицирани в националното право като „престъпления“, подобен характер може да произтича от естеството на нарушението и по-специално от репресивната цел на санкцията, до налагането на която

[23] Член 2, параграф 2, буква а) ОРЗД.
[24] Член 2, параграф 2, буква г) ОРЗД.
[25] Член 3, параграф 7 от 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, 2016 г., стр. 89).
[26] Член 10 ОРЗД.

може да доведе то. В случая налагането на точки за пътнотранспортни нарушения, както и другите санкции, които могат да бъдат наложени в резултат от извършването на подобни нарушения, наред с останалото, преследват и такава репресивна цел. Що се отнася до третия критерий, Съдът отбелязва, че само пътнотранспортните нарушения с определена тежест предполагат налагането на точки и следователно могат да доведат до налагане на санкции с известна строгост. Освен това налагането на такива точки по принцип се добавя към наложената санкция и кумулирането на посочените точки има правни последици, които могат да стигнат дори до забрана за управление (т. 77, 80, 85, 87—90 и 93).

4. Понятие за файл с лични данни

Решение от 10 юли 2018 г. (голям състав), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

В това решение (вж. също рубрика II.3, „Понятие за обработване на лични данни“) Съдът изяснява понятието „файл“ по смисъла на член 2, буква в) от Директива 95/46.

След като припомня, че тази директива се прилага за ръчното обработване на лични данни само ако обработваните данни съставляват или са предназначени да съставляват част от файл, Съдът постановява, че това понятие обхваща съвкупността от лични данни, събирани в рамките на проповедническа дейност „от врата на врата“ и състоящи се от имена и адреси и други сведения за посетените лица, при положение че тези данни са структурирани според определени критерии, позволяващи на практика лесното им откриване с цел последващо използване. За да бъде такава съвкупност обхванатата от това понятие, не е необходимо тя да включва картотеки, специфични списъци или други подобни класификационни системи (т. 62 и т. 2 от диспозитива).

5. Понятие за администратор на лични данни

Решение от 10 юли 2018 г. (голям състав), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

По това дело (вж. също рубрика II.3, „Понятие за обработване на лични данни“, и рубрика II.4, „Понятие за файл с лични данни“) Съдът се произнася дали съответната религиозна общност се явява администратор на лични данни, когато такива данни се обработват в рамките на проповедническа дейност „от врата на врата“, организирана, съгласувана и насърчавана от тази общност.

Съдът приема, че задължението на всяко лице да спазва нормите на правото на Съюза относно защитата на личните данни не може да се счита за намеса в организационната самостоятелност на религиозните общности. В това отношение той заключава, че член 2, буква г) от Директива 95/46, разглеждан във връзка с член 10, параграф 1 от Хартата, трябва да се тълкува в смисъл, че религиозна общност, съвместно с проповядващите нейни членове, може да бъде квалифицирана като администратор на личните данни, обработвани от последните в рамките на проповедническа дейност „от врата на врата“,

организирана, съгласувана и насърчавана от тази общност, без да е необходимо въпросната общност да има достъп до данните или да е установено, че тя е дала на членовете си писмени указания или нареждания във връзка с обработването (т. 74 и 75; т. 3 от диспозитива).

Решение от 5 юни 2018 г. (голям състав), Wirtschaftsakademie Schleswig Holstein (C-210/16, ECLI:EU:C:2018:388)[27]

В качеството си на надзорен орган по смисъла на член 28 от Директива 95/46 германският орган за защита на данните разпорежда на специализирано в образователната област германско дружество, което предлага услуги за обучение чрез фен страница, хоствана от социалната мрежа Facebook, да деактивира тази фен страница. Според органа нито посоченото дружество, нито Facebook предоставят информация на посетителите на фен страницата, че на нея се събират личните им данни с помощта на бисквитки и че впоследствие дружеството и Facebook обработват тези данни.

Във връзка с това Съдът изяснява понятието „администратор“ на лични данни. Той приема, че администраторът на фен страница, хоствана от Facebook, какъвто е участващото в главното производство дружество, чрез действията си по параметриране (с оглед най-вече на неговата целева аудитория, както и на целите, които си поставя във връзка с управлението и рекламата на своята дейност) участва при определянето на целите и средствата за обработването на личните данни на посетителите на своята фен страница. Поради това според Съда такъв администратор на страница следва да се квалифицира като администратор по смисъла на член 2, буква г) от Директива 95/46 в рамките на Съюза, отговарящ за тази обработка съвместно с Facebook Ireland (установеното в Съюза дъщерно дружество на американското дружество Facebook) (т. 39).

Решение от 29 юли 2019 г., Fashion ID (C-40/17, EU:C:2019:629)

Това дело дава повод на Съда да изясни понятието за администратор на данни във връзка с интегрирането на „социална приставка“ в уебстраница.

Случаят се отнася до германското предприятие за онлайн продажба на модни дрехи Fashion ID, което интегрира в уебсайта си социалната приставка „харесва ми“ на социалната мрежа „Фейсбук“. Когато дадено лице посети уебсайта на Fashion ID, в резултат от интегрирането на приставката негови лични данни се предават на Facebook Ireland. Става ясно, че това се случва без знанието на посетителя и без значение дали същият е член на социалната мрежа „Фейсбук“ и дали е натиснал фейсбук бутона „харесва ми“.

Verbraucherzentrale NRW, действащо в обществена полза германско сдружение за защита на интересите на потребителите, упреква Fashion ID, че е предало на Facebook Ireland лични данни на посетителите на уебсайта му без тяхното съгласие, от една страна, и в нарушение на задълженията за предоставяне на информация, предвидени в

[27] Това решение е представено в Годишния доклад за 2018 г., стр. 92.

разпоредбите за защита на личните данни, от друга. Сезираният със спора Oberlandesgericht Düsseldorf (Висш областен съд Дюселдорф, Германия) отправя запитване до Съда за тълкуването на няколко разпоредби на Директива 95/46.

Съдът най-напред констатира, че оператор на уебсайт като Fashion ID може да се счита за администратор по смисъла на член 2, буква г) от Директива 95/46. Тази администраторска отговорност обаче е ограничена — само за операцията или набора от операции по обработване на лични данни, чиито цели и средства той действително определя, а именно събирането на въпросните данни и разкриването им чрез предаване. За сметка на това според Съда на пръв поглед е изключено Fashion ID да определя целите и средствата за последващите операции по обработване на лични данни, които Facebook Ireland извършва, след като данните са му предадени, така че Fashion ID не може да се счита за администратор на така обработваните данни, по смисъла на този член 2, буква г) (т. 76 и 85 и т. 2 от диспозитива).

Освен това Съдът подчертава, че е необходимо и операторът на уебсайта, и доставчикът на социалната приставка, какъвто е Facebook Ireland, да преследват с тези операции по обработване законни интереси по смисъла на член 7, буква е) от Директива 95/46, за да имат право да извършват въпросните операции (т. 97 и т. 3 от диспозитива).

Накрая Съдът уточнява, че операторът на уебсайта трябва да получи съгласието на съответното лице по смисъла на член 2, буква з) и член 7, буква а) от Директива 95/46 само за операциите по обработване на лични данни, чиито цели и средства той действително определя. В такъв случай предвиденото в член 10 от Директивата задължение за предоставяне на информация е в тежест и на въпросния оператор, като обаче информацията, която той дължи на съответното физическо лице, се отнася само до операцията или набора от операции по обработване на лични данни, чиито цели и средства този оператор действително определя (т. 10 и; т. 4 от диспозитива).

Решение от 9 юли 2020 г., Land Hessen (C-272/19, EU:C:2020:535)

Гражданин, който е подал петиция до Комисията по петициите на парламента на провинция Хесен (Германия), иска от същата да му предостави достъп до свързаните с него лични данни, които тя е съхранила във връзка с разглеждането на неговата петиция. Като основание за искането си сочи ОРЗД, който предвижда право на субекта на данни да получи от администратора достъп до свързаните с него лични данни.

Председателят на парламента на провинция Хесен решава да отхвърли това искане, тъй като процедурата за разглеждането на петиции е задача на парламента, а посоченият парламент не попада в приложното поле на ОРЗД.

Verwaltungsgericht Wiesbaden (Административен съд Висбаден, Германия), сезиран от гражданина, счита, че германското законодателство не предоставя право на достъп до лични данни в контекста на петиция като разглежданата. Въпреки това Verwaltungsgericht Wiesbaden (Административен съд Висбаден) счита, че такова право на достъп може да произтича от ОРЗД, и отправя запитване до Съда на ЕС по този въпрос. Освен това, тъй като се съмнява в собствената си независимост и следователно в качеството си на съд,

който има право да отправя преюдициални запитвания до Съда, Verwaltungsgericht Wiesbaden (Административен съд Висбаден) отправя запитване до Съда и по този въпрос.

В решението си Съдът отговаря, че доколкото комисия по петиции на парламент на федерална провинция на държава членка сама или съвместно с други определя целите и средствата за обработването на лични данни, тази комисия трябва да се квалифицира като „администратор“ по смисъла на ОРЗД[28]. Поради това извършваното от такава комисия обработване на лични данни попада в приложното поле на посочения регламент, и по-специално на разпоредбата, която дава на субектите на данни право на достъп до свързаните с тях лични данни[29].

По-специално Съдът констатира, че дейностите на Комисията по петициите на парламента на Хесен не попадат в някое от изключенията, предвидени в ОРЗД. Той приема, че тези дейности са от публично естество и присъщи на провинцията, тъй като посочената комисия косвено допринася за парламентарната дейност, но отбелязва, че те също така са от политически и административен характер. Освен това от доказателствата на разположение на Съда по никакъв начин не следва, че посочените дейности в случая съответстват на някое от предвидените в ОРЗД изключения (т. 71—74 и диспозитива).

6. Условия за допустимост на обработването

Решение от 16 декември 2008 г. (голям състав), Huber (C-524/06, EU:C:2008:724)[30]

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

---

28 Член 4, точка 7 от ОРЗД.
29 Член 15 от ОРЗД.
30 Това решение е представено в Годишния доклад за 2008 г., стр. 48.

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, 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, 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 централизираният 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 (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.

По-конкретно, ASNEF и FECEMD поддържат, че испанското право предвижда несъществуващо в Директива 95/46 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, 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 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. Затова Съдът заключава, че член 7, буква е) от Директива 95/46 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 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 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, 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 и 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 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 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 Slovenskej republiky (Върховен съд на Словашката република) 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 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 (т. 117 и 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 способи 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 невиновност 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 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).

Решение от 11 ноември 2020 г., Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA е доставчик на мобилни далекосъобщителни услуги на румънския пазар. На 28 март 2018 г. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Национален орган за надзор върху обработването на лични данни, Румъния) му налага глоба за това, че е събирало и съхранявало копия от документите за самоличност на своите клиенти без изрично съгласие от тяхна страна.

Според ANSPDCP в периода от 1 до 26 март 2018 г. Orange România е сключил договори за предоставяне на мобилни далекосъобщителни услуги, които съдържат клауза, съгласно която клиентите са били информирани и са се съгласили със събирането и съхраняването на копие от техния документ за самоличност с цел идентификация. Полето относно тази клауза е отметнато от администратора на лични данни преди подписването на договора.

При тези условия Tribunalul București (Градски съд Букурещ, Румъния) иска от Съда да уточни условията, при които съгласието на клиентите за обработване на лични данни може да се счита за валидно.

На първо място Съдът припомня, че правото на Съюза[31] предвижда списък от случаи, в които обработването на лични данни може да се счита за законосъобразно. По-специално, съгласието на субекта на данните трябва да бъде свободно, конкретно,

[31] Член 7 от Директива 95/46 и член 6 от ОРЗД.

информирано и недвусмислено[32]. В това отношение съгласието не е валидно дадено в случаите на мълчание, предварително отметнати полета или липса на действие (т. 34, 36, 37 и 39).

Освен това, когато съгласието на субекта на данните е дадено в рамките на писмена декларация, която се отнася и до други въпроси, тази декларация трябва да се представи в разбираема и леснодостъпна форма, като използва ясен и прост език. За да се осигури на субекта на данни истински свободен избор, клаузите на договора не трябва да въвеждат субекта на данни в заблуждение, що се отнася до възможността да сключи договора, дори да отказва да даде съгласие за обработване на неговите данни (т. 34, 36, 37, 39 и 41).

Съдът уточнява, че тъй като Orange România е администратор на лични данни, то трябва да може да докаже законосъобразността на обработването на тези данни и следователно, в конкретния случай, наличието на валидно съгласие от страна на своите клиенти. В това отношение, тъй като не изглежда засегнатите клиенти сами да са правили отметка в полето относно събирането и съхраняването на копия от техните документи за самоличност, самият факт, че това поле е отметнато, не е от естество да докаже изразено с потвърждаващо действие съгласие. Запитващата юрисдикция следва да направи необходимите в това отношение проверки (т. 42 и 46).

Според Съда националният съд трябва също така да прецени дали разглежданите договорни клаузи са могли да подведат засегнатите клиенти относно възможността за сключване на договора въпреки отказа за даване на съгласие за обработване на техните данни, при липсата на уточнения относно тази възможност. Освен това в случай на отказ на клиента да даде съгласие за обработването на своите данни Orange România е изисквало той да заяви писмено, че не е съгласен със събирането и съхраняването на копие от документа си за самоличност. Според Съда подобно допълнително изискване може неоправдано да наруши свободния избор за противопоставяне срещу това събиране и съхраняване. При всички положения, тъй като посоченото дружество трябва да докаже, че неговите клиенти с активно поведение са изразили съгласието си за обработване на техните лични данни, то не е имало основание да изисква от тях активно да изразят отказа си (т. 49—51).

В заключение Съдът посочва, че договор за предоставяне на далекосъобщителни услуги, съдържащ клауза, че субектът на данни е информиран за и се е съгласил със събирането и съхраняването с идентификационна цел на копие от документа му за самоличност, не е годен да докаже, че субектът на данни е дал надлежно по смисъла на тези разпоредби съгласие за събирането и съхраняването, когато полето относно тази клауза е отметнато от администратора на данни преди подписването на договора, когато уговорките в посочения договор могат да въведат субекта на данни в заблуждение относно възможността да сключи договора дори ако отказва да даде съгласие за обработването на неговите лични данни, или когато този администратор неоправдано е нарушил свободния избор на субекта на данни да се противопостави на събирането и съхраняването, като е изисквал от него, за да откаже да даде съгласието си за обработването, да попълни допълнителен формуляр, отразяващ този отказ (т. 52 и диспозитива).

---

[32] Член 2, буква з) от Директива 95/46 и член 4, параграф 11 от ОРЗД.

Решение от 12 май 2021 г. (голям състав), Bundesrepublik Deutschland (Червена бюлетина на Интерпол) (C-505/19, EU:C:2021:376)

През 2012 г. Международната организация на криминалната полиция (наричана по-нататък „Интерпол“) публикува, по искане на Съединените американски щати и на основание издадена от властите на тази държава заповед за задържане, червена бюлетина относно WS, германски гражданин, с оглед на евентуалната му екстрадиция. Когато е установено, че местонахождението на лице, за което е издадена такава бюлетина, е в държава — членка на Интерпол, тази държава по принцип трябва временно да задържи това лице или да наблюдава или ограничи придвижването му.

Още преди да бъде публикувана тази червена бюлетина обаче, срещу WS в Германия е образувано производство по разследване, което според запитващата юрисдикция се отнася до същите деяния като тези, които са довели до въпросната бюлетина. Това производство е окончателно прекратено през 2010 г., след като WS превежда определена парична сума в съответствие с особена процедура за постигане на споразумение, предвидена в германското наказателно право. Впоследствие Bundeskriminalamt (Федерална криминална полиция, Германия) уведомява Интерпол, че поради споменатото предходно производство според нея принципът ne bis in idem е приложим в случая. Този принцип, прогласен както в член 54 от Конвенцията за прилагане на споразумението от Шенген[33], така и в член 50 от Хартата, по-специално забранява лицето, спрямо което вече е бил постановен окончателен съдебен акт, да бъде отново преследвано за същото деяние.

През 2017 г. WS подава пред Verwaltungsgericht Wiesbaden (Административен съд Висбаден, Германия) жалба срещу Федерална република Германия, за да бъде разпоредено тя да предприеме всички необходими мерки за заличаване на червената бюлетина. В тази насока WS твърди, наред с нарушение на принципа ne bis in idem, и нарушение на гарантираното му с член 21 ДФЕС право на свободно движение, защото той не може да отиде в държава, страна по Споразумението от Шенген, или в държава членка, без да се излага на риска да бъде задържан. Той смята също, че поради тези нарушения обработването на неговите лични данни, съдържащи се в червената бюлетина, е в разрез с Директива 2016/680 относно защитата на личните данни в областта на наказателното право[34].

При тези обстоятелства Verwaltungsgericht Wiesbaden (Административен съд Висбаден) решава да отправи до Съда въпрос за приложимостта на принципа ne bis in idem, и по-конкретно за възможността в случай като разглеждания временно да бъде задържано

---

[33] Конвенция за прилагане на споразумението от Шенген от 14 юни 1985 година между правителствата на държавите от Икономическия съюз Бенелюкс, Федерална република Германия и Френската република за постепенното премахване на контрола по техните общи граници (ОВ L 239, 2000 г., стр. 3; Специално издание на български език, 2007 г., глава 19, том 1, стр. 183) (наричана по-нататък „КПСШ“).

[34] 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, 2016 г., стр. 89).

лице, за което е издадена червена бюлетина. В допълнение, ако този принцип е приложим, запитващата юрисдикция иска да се установи какви са последиците за обработването от държавите членки на личните данни, съдържащи се в такава бюлетина.

В решението си Съдът (голям състав) постановява по-специално, че разпоредбите на Директива 2016/680, разглеждани през призмата на член 54 от КПСШ и на член 50 от Хартата, трябва да се тълкуват в смисъл, че допускат обработването на личните данни, съдържащи се в издадена от Интерпол червена бюлетина, докато с влязъл в сила съдебен акт не е било установено, че принципът ne bis in idem се прилага за деянията, на които се основава тази бюлетина, стига посоченото обработване да отговаря на предвидените от тази директива условия (т. 121 и т. 2 от диспозитива).

По въпроса за личните данни, съдържащи се в червена бюлетина на Интерпол, Съдът посочва, че всяка операция, приложена към тези данни, като записването им в базите данни за издирвани лица на държава членка, представлява „обработване“, което попада в обхвата на Директива 2016/680[35]. По-нататък, според Съда, от една страна, това обработване има легитимна цел, и от друга, то няма как да се приеме за незаконосъобразно просто поради съображението че принципът ne bis in idem би могъл да се прилага към деянията, на които се основава червената бюлетина[36]. Впрочем това обработване от органите на държавите членки може да се окаже задължително именно за да се провери дали този принцип е приложим (т. 111, 114, 116, 117 и 119).

При това положение Съдът постановява също, че Директива 2016/680 във връзка с член 54 от КПСШ и с член 50 от Хартата допуска обработването на личните данни, съдържащи се в червена бюлетина, докато с влязъл в сила съдебен акт не е било установено, че в случая се прилага принципът ne bis in idem. Това обработване обаче трябва да отговаря на предвидените от цитираната директива условия. В този смисъл то по-специално трябва да е необходимо за изпълнението на задача, осъществявана от компетентен национален орган, за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания[37] (т. 121 и т. 2 от диспозитива).

От друга страна, когато се прилага принципът ne bis in idem, записът в базите данни на държавите членки за издирвани лица на личните данни, съдържащи се в червена бюлетина на Интерпол, вече не е необходим, защото спрямо съответното лице повече не може да се води наказателно преследване за деянията, предмет на споменатата бюлетина, и следователно то да бъде задържано за същите деяния. Ето защо съответното лице трябва да може да поиска засягащите го данни да бъдат заличени. Ако обаче този запис остане, той трябва да бъде придружен от указанието, че съответното лице повече не може да бъде преследвано в държава членка или в договаряща държава за същите деяния, на основание на принципа ne bis in idem (т. 120).

35 Вж. член 2, параграф 1 и член 3, точка 2 от Директива 2016/680.

36 Вж. член 4, параграф 1, буква б) и член 8, параграф 1 от Директива 2016/680.

37 Вж. член 1, параграф 1 и член 8, параграф 1 от Директива 2016/680.

Решение от 22 юни 2021 г. (голям състав), Latvijas Republikas Saeima (Наказателни точки) (C-439/19, EU:C:2021:504)

В това решение (вж. също раздел II, точка 3, „Понятие за обработване на лични данни“) Съдът постановява, че ОРЗД не допуска правна уредба, която задължава Ceļu satiksmes drošības direkcija (Дирекция „Безопасност на движението по пътищата“, Латвия) (наричана по-нататък „CSDD“) да предоставя на обществеността достъп до данните относно наказателните точки, наложени на водачите на превозни средства за извършването на пътнотранспортни нарушения, без да е необходимо лицето, поискало достъп, да доказва наличието на специфичен интерес от получаването им. Той констатира, че не е доказана необходимостта, по-специално с оглед на целта за подобряването на безопасността на движението по пътищата, посочена от латвийското правителство, от съобщаване на лични данни относно точките за пътнотранспортни нарушения. Освен това според Съда нито правото на достъп на обществеността до официални документи, нито правото на свобода на информация обосновават подобна правна уредба (т. 113 и 120—122 и т. 2 от диспозитива).

В този контекст Съдът подчертава, че подобряването на безопасността на движението по пътищата, посочено в латвийската правна уредба, представлява призната от Съюза цел от общ интерес и следователно държавите членки могат да квалифицират пътната безопасност като „задача от обществен интерес“[38]. При все това не е доказано, че латвийският режим за съобщаване на лични данни относно точките за пътнотранспортни нарушения е необходим за постигане на преследваната цел. Всъщност, от една страна, латвийският законодател разполага с множество способи за действие, които биха му позволили да постигне тази цел по друг начин и които нарушават в по-малка степен основните права на засегнатите лица. От друга страна, следва да се има предвид чувствителността на данните, свързани с точките за пътнотранспортни нарушения, както и фактът, че публичното им съобщаване може да съставлява сериозна намеса в правата на неприкосновеност на личния живот и на защита на личните данни, тъй като може да предизвика неодобрение на обществото и да доведе до заклеймяване на съответното лице (т. 109—113).

Освен това Съдът счита, че предвид чувствителността на посочените данни и сериозността на разглежданата намеса в тези две основни права, последните имат предимство както пред обществения интерес от достъп до официални документи, какъвто например е националният регистър на превозните средства и техните водачи, така и пред правото на свобода на информацията (т. 120 и 121).

По тези причини Съдът приема също, че ОРЗД не допуска латвийската правна уредба и доколкото тя разрешава на CSDD да съобщава данните относно точките, наложени на водачите на превозни средства за пътнотранспортни нарушения, на икономически оператори, за да могат последните да ги използват повторно и да ги съобщават на обществеността (т. 126 и т. 3 от диспозитива).

---

[38] По силата на член 6, параграф 1, буква д) от ОРЗД обработването на лични данни е законосъобразно, когато „е необходимо за изпълнението на задача от обществен интерес [...]“.

Накрая, Съдът уточнява, че принципът на предимство на правото на Съюза не допуска запитващата юрисдикция, сезирана с жалба срещу латвийското законодателство, което е квалифицирано от Съда като несъвместимо с правото на Съюза, да реши да запази правните последици на това законодателство до датата на обявяване на окончателното си решение (т. 137 и т. 4 от диспозитива).

III. Обработване на лични данни по Директива 2002/58/ЕО

Решение от 2 октомври 2018 г. (голям състав), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788)[39]

По това дело става дума за отказа на испански съдия следовател да разреши достъп до лични данни във връзка с разследване на грабеж, при който са отнети портфейл и мобилен телефон. По-конкретно, съдебната полиция подава до този съдия искане за достъп до данните за самоличността на ползвателите на телефонните номера, активирани от откраднатия телефон в период от 12 дни, считано от датата на грабежа. Съдията мотивира отказа си с това, че наказателното дело не се води за „тежко“ престъпление, каквито съгласно испанското право са престъпленията, които се наказват с лишаване от свобода над пет години, а достъп до данните за самоличността може да се разреши само във връзка с тежки престъпления.

След като припомня, че достъпът на публичните органи до личните данни, съхранявани от доставчиците на електронни съобщителни услуги, в рамките на досъдебното наказателно производство попада в приложното поле на Директива 2002/58, Съдът постановява, че достъпът до данни с цел установяването на самоличността на притежатели на СИМ карти, активирани с откраднат мобилен телефон, като името, фамилията и евентуално адреса на тези притежатели, съставлява намеса в основните им права на зачитане на личния живот и защита на данните, закрепени в Хартата, дори да не са налице обстоятелства, които дават основание тази намеса да се квалифицира като „тежка“, като при това е без значение дали данните за личния живот имат чувствителен характер и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса. Съдът обаче подчертава, че тази намеса не е толкова тежка, че посоченият достъп да трябва да бъде ограничен — в областта на превенцията, разследването, разкриването и преследването на престъпления — до борбата с тежката престъпност. Наистина Директива 2002/58 изброява изчерпателно целите, които могат да обосноват национална правна уредба, регламентираща достъпа на публични органи до разглежданите данни и съответно дерогираща принципа на поверителност на електронните съобщения, поради което при този достъп трябва действително и строго да се преследва някоя от тези цели, но все пак Съдът отбелязва, че що се отнася до целта за превенция, разследване, разкриване и преследване на престъпления, текстът на Директива 2002/58 не ограничава тази цел само до борбата с тежките престъпления, а се отнася общо до „[престъпления]“ (т. 38, 42 и 59—63 и диспозитива).

---

[39] Това решение е представено в Годишния доклад за 2018 г., стр. 94.

В този контекст Съдът пояснява, че наистина в решение Tele2 Sverige и Watson и др.[40] е приел, че само в случаите на борба с тежката престъпност може да е обоснован достъпът на публичните органи до лични данни, запазени от доставчиците на съобщителни услуги, които в своята съвкупност позволяват да се направят точни изводи относно личния живот на лицата, чиито данни за засегнати, но това тълкуване е било мотивирано с обстоятелството, че целта, преследвана с правна уредба, която регламентира този достъп, трябва да е свързана с тежестта на намесата в съответните основни права, до която води тази дейност. В този смисъл съгласно принципа на пропорционалност в тази област тежката намеса може да бъде обоснована само от цел за борба с престъпността, която също трябва да се квалифицира като „тежка“. За сметка на това, когато намесата не е тежка, достъпът може да бъде обоснован от целта за превенция, разследване, разкриване и преследване общо на „[престъпления]“ (т. 54—57).

Що се отнася до конкретния случай, Съдът приема, че достъпът само до данните, посочени в разглеждането в главното производство искане, не може да бъде квалифициран като „тежка“ намеса в основните права на лицата, чиито данни са засегнати, тъй като тези данни не дават възможност да се направят точни изводи относно личния живот на посочените лица. Затова Съдът заключава, че намесата, до която води достъп до такива данни, може да бъде обоснована от целта за превенция, разследване, разкриване и преследване общо на „[престъпления]“, без да е необходимо тези престъпления да са квалифицирани като „тежки“ (т. 61 и 62).

Решения от 6 октомври 2020 г. (голям състав), Privacy International (C-623/17, EU:C:2020:790) и La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791)[41]

Съдебната практика относно запазването и достъпа до лични данни в областта на електронните съобщения, и по-специално решение Tele2 Sverige и Watson и др., в което Съдът приема по-конкретно, че държавите членки не могат да налагат на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данни за трафик и данни за местонахождение, поражда загриженост на някои държави, опасяващи се, че са лишени от инструмент, който според тях е необходим за опазването на националната сигурност и за борбата с престъпността.

Именно на този фон Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство) (Privacy International, C-623/17), Conseil d'État (Държавен съвет, Франция) (Le Quadrature du Net и др., съединени дела C-511/18 и C-512/18) и Cour constitutionnelle (Конституционен съд, Белгия) (Ordre des barreaux francophones et germanophone и др., C-520/18) са сезирани със спорове относно законосъобразността на правните уредби, приети от някои държави членки в тези области, предвиждащи по-специално задължение на доставчиците на електронни съобщителни услуги общо и неизбирателно да предават на публичен орган или да запазват данните на потребителите относно трафика и местонахождението.

---

40 Решение на Съда от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970).

41 Тези решения са представени в Годишния доклад за 2020 г., стр. 30—34.

С две решения, постановени от големия състав на 6 октомври 2020 г., Съдът приема, най-напред, че националните правни уредби, с които доставчиците на електронни съобщителни услуги са задължени да съхраняват данни за трафика и местонахождението или да предават тези данни на националните органи по сигурността и националните разузнавателни органи с цел опазване на националната сигурност, попадат в приложното поле на Директива 2002/58 (т. 49 и т. 1 от диспозитива на решение Privacy International и т. 104 от решение La Quadrature du Net и др.).

По-нататък Съдът припомня, че Директива 2002/58[42] не позволява изключението от принципното задължение да се гарантира поверителността на електронните комуникации и свързаните с тях данни и от забраната за съхраняване на тези данни да се превръща в правило. Това означава, че Директивата допуска държавите членки да приемат — в частност за цели на националната сигурност — законодателни мерки, с които се ограничава обхватът на предвидените в Директивата права и задължения, и конкретно на задължението да се гарантира поверителността на комуникациите и на данните за трафика[43], но само при спазване на общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и на гарантираните с Хартата основни права[44] (т. 59 и 60 от решение Privacy International и т. 111 и 113 от решение La Quadrature du Net и др.).

В този контекст Съдът приема, от една страна, по дело Privacy International, че Директива 2002/58, разглеждана във връзка с Хартата, не допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби данни за трафик и данни за местонахождение с цел опазването на националната сигурност. От друга страна, по съединени дела La Quadrature du Net и др. и по дело Ordre des barreaux francophones et germanophone и др. Съдът счита, че същата директива не допуска законодателни мерки, които предвиждат задължение за доставчиците на електронни съобщителни услуги за превантивно общо и неизбирателно запазване на данни за трафик и данни за местонахождение.

Всъщност тези задължения за предаване и за общо и неизбирателно съхраняване на подобни данни представляват особено тежка намеса по отношение на гарантираните с Хартата основни права, без поведението на лицата, за чиито данни става въпрос, да има връзка с целта на съответната правна уредба. Аналогично Съдът тълкува член 23, параграф 1 от ОРЗД, разглеждан в светлината на Хартата, в смисъл, че не допуска национална правна уредба, която задължава доставчиците на достъп до публични съобщителни услуги в интернет и доставчиците на хостингови услуги да съхраняват общо и неизбирателно в частност личните данни, свързани с тези услуги (т. 71, 82 и т. 2 от диспозитива на решение Privacy International и т. 146, 168, 174, 177 и 212 и т. 1 и 3 от диспозитива на решение La Quadrature du Net и др.).

За сметка на това Съдът приема, че в случаи, при които съответната държава членка е изправена пред тежка заплаха за националната сигурност, която се явява реална и настояща или предвидима, Директива 2002/58, разглеждана в светлината на Хартата,

[42] Член 15, параграфи 1 и 3 от Директива 2002/58.

[43] Член 5, параграф 1 от Директива 2002/58.

[44] По-конкретно членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

допуска да се разпореди на доставчиците на електронни съобщителни услуги да съхраняват общо и неизбирателно данни за трафика и за местонахождението. В този контекст Съдът пояснява, че решението, което съдържа подобно разпореждане за ограничен до строго необходимото период от време, трябва да подлежи на ефективен контрол от страна на съд или независим административен орган, чиито решения са скрепени със задължителна сила, за да се проверява дали е налице някой от посочените случаи и дали са спазени предвидените условия и гаранции. При същите условия Директивата допуска и автоматизирания анализ на данните, в частност на данните за трафика и за местонахождението, на всички потребители на електронни средства за комуникация (т. 137—139, 177—179 и т. 1 и 2 от диспозитива на решение La Quadrature du Net и др.).

Съдът добавя, че Директива 2002/58, разглеждана в светлината на Хартата, допуска законодателни мерки, които позволяват целево съхраняване за ограничен до строго необходимото период от време на данните за трафика и за местонахождението, чийто обхват да се определя въз основа на обективни и недискриминационни признаци в зависимост от категориите субекти на данни или по географски критерий. Също така Директивата допуска законодателни мерки, които предвиждат общо и неизбирателно съхраняване на IP адресите, определени за източника на дадено съобщение, стига продължителността на съхраняване да е ограничена до строго необходимото, а също допуска и законодателни мерки, които предвиждат общо и неизбирателно съхраняване на данните за самоличността на потребителите на електронни средства за комуникация, като в последния случай държавите членки не са длъжни да ограничават съхранението им във времето. Наред с това Директивата допуска и законодателна мярка, която позволява бързо съхраняване на данните, с които разполагат доставчиците на услуги, при положение че са налице случаи, в които възниква необходимостта тези данни да се съхранят над законовите срокове за съхраняването им за целите на разкриването на тежки престъпления или посегателства срещу националната сигурност, когато тези престъпления или посегателства вече са констатирани или може да се направи основателно предположение за наличието им (т. 161, 163 и 168 и т. 1 от диспозитива на решение La Quadrature du Net и др.).

Освен това Съдът постановява, че Директива 2002/58, разглеждана в светлината на Хартата, допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги да събират в реално време в частност данните за трафика и местонахождението, когато събирането им е ограничено така, че да се отнася само до лицата, за които има основателна причина да се предполага, че по един или друг начин участват в терористични дейности, и подлежи на предварителен контрол от страна на съд или независим административен орган, чиито решения са скрепени със задължителна сила, което да гарантира, че събирането на данните в реално време ще се разрешава само в границите на строго необходимото. В спешни случаи контролът трябва да се осъществява в кратки срокове (т. 192 и т. 2 от диспозитива на решение La Quadrature du Net и др.).

Накрая Съдът разглежда въпроса за запазването на последиците във времето на национална правна уредба, която е обявена за несъвместима с правото на Съюза. В това отношение той постановява, че националният съд не може да приложи разпоредба на националното право, която го оправомощава да ограничи във времето последиците от

решението си да обяви даден акт за незаконосъобразен, когато става дума за национална правна уредба, която задължава доставчиците на електронни съобщителни услуги да съхраняват общо и неизбирателно данните за трафика и за местонахождението и която е обявена за несъвместима с Директивата за правото на неприкосновеност на личния живот и електронните комуникации, разглеждана в светлината на Хартата.

При все това, за да бъде полезен на националната юрисдикция с отговора си, Съдът напомня, че при сегашното състояние на правото на Съюза единствено националното право урежда въпроса дали са допустими и как следва да се преценяват доказателствата, които са били получени чрез съхраняване на данни в противоречие с правото на Съюза, в рамките на наказателни производства спрямо лица, заподозрени в извършването на тежки престъпления. Съдът обаче уточнява, че Директива 2002/58, тълкувана в светлината на принципа на ефективност, изисква националният наказателен съд в такива наказателни производства да оставя без внимание доказателствата, които са получени чрез несъвместимо с правото на Съюза общо и неизбирателно съхраняване на данните за трафика и местонахождението, ако лицата, заподозрени в извършването на престъпни деяния, не са в състояние ефективно да изразят становище по тези доказателства (т. 222 и 228 и т. 4 от диспозитива на решение La Quadrature du Net и др.).

Решение от 2 март 2021 г. (голям състав), Prokuratuur (Условия за достъп до данните от електронни съобщения) (C-746/18, EU:C:2021:152)

Срещу Н. К. е образувано наказателно производство в Естония с обвинения за кражба, използване на банкова карта на трето лице и упражняване на насилие спрямо лица, участващи в съдебно производство. Н. К. е осъдена за тези престъпления от първоинстанционен съд на лишаване от свобода за две години. Впоследствие присъдата е потвърдена от апелативния съд. Протоколите, на които се основава констатацията на тези престъпления, са били изготвени по-конкретно въз основа на лични данни, събрани в рамките на доставката на електронни съобщителни услуги. Riigikohus (Върховен съд, Естония), до който Н. К. подава касационна жалба, изразява съмнения относно съвместимостта с правото на Съюза[45] на условията, при които разследващите служби са получили достъп до тези данни.

Тези съмнения се отнасят, на първо място, до въпроса дали продължителността на периода, за който разследващите служби са получили достъпа до данните, е критерий, позволяващ да се прецени тежестта на намесата, която този достъп представлява в основните права на засегнатите лица. Така, когато този период е много кратък или обемът на събраните данни е много ограничен, запитващата юрисдикция се пита дали целта за борба с престъпността като цяло, а не само за борба с тежката престъпност, може да обоснове подобна намеса. На второ място, запитващата юрисдикция има съмнения относно възможността естонската прокуратура, с оглед на различните задачи, които са ѝ възложени с националната правна уредба, да се счита за „независим“ административен

[45] По-конкретно с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

орган по смисъла на решение Tele2 Sverige и Watson и др.[46], който може да разреши достъпа на разследващия орган до съответните данни.

С решението си, произнесено в голям състав, Съдът приема, че Директива 2002/58, разглеждана с оглед на Хартата, не допуска национална правна уредба, позволяваща достъпа на публични органи до данни за трафик или данни за местонахождение, които могат да предоставят информация за комуникациите, извършени от ползвател на средство за електронна комуникация, или за местонахождението на използваните от него крайни устройства, и да позволят да се направят точни изводи относно неговия личен живот за целите на предотвратяването, разследването, разкриването и преследването на престъпления, без този достъп да е ограничен до производствата за борба с тежката престъпност или до предотвратяването на сериозни заплахи за обществената сигурност. Според Съда продължителността на периода, за който е поискан достъпът до тези данни, и обемът или видът на наличните данни за подобен период, нямат отражение в това отношение. Освен това, Съдът счита, че същата тази директива, разглеждана с оглед на Хартата, не допуска национална правна уредба, оправомощаваща прокуратурата да разреши достъпа на публичен орган до данните за трафик и до данните за местонахождение за целите на наказателно разследване (т. 45 и 59 и т. 1 и 2 от диспозитива).

Що се отнася до целта за предотвратяване, разследване, разкриване и преследване на престъпления, преследвана от разглежданата правна уредба, в съответствие с принципа на пропорционалност Съдът счита, че единствено борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност могат да обосноват достъпа на публичните органи до съвкупност от данни за трафик или данни за местонахождение, които могат да позволят да се направят точни изводи за личния живот на засегнатите лица, без други фактори, свързани с пропорционалността на подобно искане за достъп, като продължителността на периода, за който се иска достъп до подобни данни, да могат да имат за последица целта за предотвратяване, разследване, разкриване и преследване общо на престъпления да оправдае подобен достъп (т. 33 и 35).

Що се отнася до правомощието, дадено на прокуратурата да разрешава достъпа на публичен орган до данните за трафика и данните за местонахождението, за да ръководи наказателно разследване, Съдът припомня, че националното право трябва да определи условията, при които доставчиците на електронни съобщителни услуги са длъжни да предоставят на компетентните национални органи достъп до данните, с които разполагат. При все това, за да изпълни изискването за пропорционалност, подобна правна уредба трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да налагат минимални изисквания, така че лицата, чиито лични данни са засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на тези данни срещу рискове от злоупотреби. Тази уредба трябва да е задължителна по вътрешното право и да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на подобни данни, като по този начин гарантира ограничаването на намесата до строго необходимото (т. 48).

[46] Решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970, т. 120).

Според Съда, за да се гарантира на практика пълното спазване на тези условия, от съществено значение е достъпът на компетентните национални органи до запазените данни да се предоставя след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, и решението на тази юрисдикция или на тази структура да се постановява след мотивирана молба на тези органи, подадена по-специално в рамките на наказателни производства за предотвратяване, разкриване или наказателно преследване на престъпления. В надлежно обосновани спешни случаи контролът трябва да бъде осъществен в кратък срок (т. 51).

В това отношение Съдът уточнява, че предварителният контрол изисква, наред с останалото, юрисдикцията или административната структура, натоварена с извършването на този контрол, да разполага с всички правомощия и да представи всички необходими гаранции, за да осигури съвместяване на различните разглеждани интереси и права. Що се отнася по-специално до наказателно разследване, подобен контрол изисква тази юрисдикция или структура да е в състояние да осигури справедливо равновесие между, от една страна, интересите, свързани с нуждите на разследването в рамките на борбата с престъпността, и от друга страна, основните права на зачитане на личния живот и на защита на личните данни на лицата, чиито данни са засегнати от достъпа. Когато този контрол се извършва не от юрисдикция, а от независима административна структура, същата трябва да се ползва със статут, който ѝ позволява при упражняването на нейните функции да действа по обективен и безпристрастен начин и да бъде за тази цел защитена от всякакво външно влияние (т. 52 и 53).

Според Съда от това следва, че изискването за независимост, на което трябва да отговаря административната структура, натоварена с упражняването на предварителния контрол, налага тази структура да има качеството на трето лице по отношение на лицето, което иска достъп до данните, така че първата да е в състояние да упражнява този контрол обективно и безпристрастно, без каквото и да било външно влияние. По-специално в наказателноправната област изискването за независимост предполага структурата, на която е възложен този предварителен контрол, от една страна, да не участва в провеждането на въпросното наказателно разследване и от друга страна, да заема неутрално положение по отношение на страните в наказателното производство. Не е такъв обаче случаят на прокуратура, която ръководи производството по разследване и евентуално представлява държавното обвинение, какъвто е случаят на естонската прокуратура. От това следва, че прокуратурата не е в състояние да осъществи горепосочения предварителен контрол (т. 54, 55 и 57).

IV. Предаване на лични данни на трети страни

Решение от 6 ноември 2003 г. (голям състав), Lindqvist (C-101/01, EU:C:2003:596)[47]

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, 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 и 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 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 презумира, 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)[48]

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 разположени 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/ЕО[49] Комисията е приела, че в рамките на т.нар. схема за „сфера на

[47] Това решение е представено в Годишния доклад за 2003 г., стр. 67.

[48] Това решение е представено в Годишния доклад за 2015 г., стр. 55.

[49] 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, 2000 г., стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64).

неприкосновеност на личния живот“ (на английски „safe harbour“)[50] 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, 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, което Комисията е приела на основание член 25, параграф 6 от Директива 95/46.

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 Комисията не прави такава констатация, член 1 от това решение не отговаря на изискванията, установени в член 25, параграф 6 от Директива 95/46, 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 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 теза права, и без да се отбелязва наличието на ефективна правна защита срещу този вид намеса (т. 82, 87—89 и 96—98 и т. 2 от диспозитива).

Съдът обявява за невалиден и член 3 от Решение 2000/520, доколкото тази разпоредба лишава националните надзорни органи от правомощията, които те черпят от член 28 от Директива 95/46, 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

[50] 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.

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 съдържат достъпът и използването на тези данни (т. 93). По-конкретно, правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, засяга съществената 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 съществената 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, навиците 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 извършваното 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 извършваното от визираните в предвиденото споразумение публични органи разследване (т. 219, 220, 223 и 224).

Решение от 16 юли 2020 г. (голям състав), Facebook Ireland и Schrems (C-311/18, ECLI:EU:C:2020:559)[51]

ОРЗД гласи, че по принцип предаване на данни на трета държава е възможно само ако тази трета държава осигурява адекватно ниво на защита на тези данни. Съгласно

[51] Това решение е представено в Годишния доклад за 2020 г., стр. 27—30.

Регламента Комисията може с решение да констатира, че определена трета държава осигурява адекватно ниво на защита поради вътрешното си законодателство или поради сключените от нея международни споразумения[52]. Когато няма такова решение за наличието на адекватно ниво на защита, предаване на данните е възможно само ако установеният в Съюза износител на личните данни предвиди подходящи гаранции, каквито може например да се установят чрез определени от Комисията стандартни клаузи за защита на данните, и ако субектите на данните разполагат с приложими права и ефективни правни средства за защита[53]. Освен това ОРЗД точно урежда условията, при които е възможно такова предаване на данни в отсъствието на решение за наличието на адекватно ниво на защита и в отсъствието на подходящи гаранции[54].

Г-н Maximillian Schrems, австрийски гражданин с местоживеене в Австрия, е потребител на „Фейсбук“ от 2008 г. Дружеството Facebook Ireland предава личните данни на г-н Schrems, също както и данните на всички други потребители от Съюза, към разположени на територията на Съединените щати сървъри на Facebook Inc., където данните се обработват. Г-н Schrems подава жалба до ирландския надзорен орган, като по същество иска това прехвърляне на данни да се забрани. Той поддържа, че действащото право и практики в Съединените щати не гарантират достатъчна защита на предаваните там данни срещу достъп на публичните органи до тях. Жалбата му е отхвърлена по-специално по съображението, че в Решение 2000/520[55] Комисията е констатирала, че Съединените щати гарантират достатъчна степен на защита. С решение от 6 октомври 2015 г. (наричано по-нататък „решение Schrems I“)[56], постановено по преюдициален въпрос, отправен от High Court (Висш съд, Ирландия), Съдът обявява Решение 2000/520 за невалидно (т. 52 и 53).

След решение Schrems I и след съответно постановената от ирландския съд отмяна на решението, с което е била отхвърлена жалбата на г-н Schrems, ирландският надзорен орган приканва г-н Schrems да преформулира жалбата си предвид обявената от Съда невалидност на Решение 2000/520. В преформулираната си жалба г-н Schrems поддържа, че Съединените щати не предоставят достатъчна защита на предаваните там данни. Той иска да се спре или да се забрани за в бъдеще предаването на личните му данни от Съюза към Съединените щати, извършвано Facebook Ireland вече въз основа на стандартните клаузи за защита на данните, съдържащи се в приложението към Решение 2010/87/ЕС[57]. Тъй като счита, че решението по жалбата на г-н Schrems зависи в частност от валидността на Решение 2010/87, ирландският надзорен орган сезира High Court (Висш съд) с цел последният да отправи преюдициално запитване до Съда. След образуването на това

---

52 Член 45 от ОРЗД.

53 Член 46, параграф 1 и параграф 2, буква в) от ОРЗД.

54 Член 49 от ОРЗД.

55 Решение 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, 2000 г., стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64).

56 Решение на Съда от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650 (вж. също прессъобщение № 117/15).

57 Решение на Комисията от 5 февруари 2010 година относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО (ОВ L 39, 2010 г., стр. 5), изменено с Решение за изпълнение (ЕС) 2016/2297 на Комисията от 16 декември 2016 г. (ОВ L 344, 2016 г., стр. 100).

дело Комисията приема Решение (ЕС) 2016/1250 относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ[58] (т. 54, 55 и 57).

С преюдициалното си запитване до Съда националната юрисдикция отправя въпроси за приложимостта на ОРЗД към предаването на лични данни въз основа на стандартните клаузи за защита по Решение 2010/87, за изискваното от този регламент ниво на защита при такова предаване на данни и за задълженията на надзорните органи в този контекст. Освен това High Court (Висш съд) поставя въпроса за валидността на Решение 2010/87 и на Решение 2016/1250.

Съдът констатира, че при разглеждането на Решение 2010/87 с оглед на Хартата не се установяват обстоятелства, които могат да засегнат неговата валидност. Той обаче обявява Решение 2016/1250 за невалидно (т. 4 и 5 от диспозитива).

Съдът най-напред приема, че правото на Съюза, и по-специално ОРЗД, се прилага за предаване на лични данни за търговски цели от икономически оператор, установен в държава членка, към друг икономически оператор, установен в трета държава, въпреки че по време на предаването или след него тези данни могат да се обработват от органите на съответната трета държава за целите на обществената сигурност, отбраната и държавната сигурност. Той пояснява, че това обработване на данни от органите на трета държава не може да изключи посоченото предаване от приложното поле на ОРЗД (т. 86, 88 и 89 и т. 1 от диспозитива).

Що се отнася до изискваното ниво на защита в рамките на такова предаване, Съдът приема, че изискванията, предвидени за тази цел от разпоредбите на ОРЗД, свързани с подходящи гаранции, приложими права и ефективни правни средства за защита, трябва да се тълкуват в смисъл, че лицата, чиито лични данни са предадени на трета държава въз основа на стандартни клаузи за защита на данните, трябва да се ползват с ниво на защита, което по същество е равностойно на гарантираното в Съюза с този регламент, разглеждан в светлината на Хартата. В този контекст той пояснява, че при оценката на това ниво на защита трябва да се вземат предвид както договорните клаузи, уговорени между износителя на данни, установен в Съюза, и получателя на предаването, установен в съответната трета държава, така и, що се отнася до евентуалния достъп на публичните органи на тази трета държава до така предадените лични данни, релевантните елементи на нейната правна система (т. 105 и т. 2 от диспозитива).

Що се отнася до задълженията на надзорните органи в контекста на такова предаване, Съдът приема, че освен ако съществува надлежно прието от Комисията решение относно адекватното ниво на защита, тези органи по-специално са задължени да спрат или да забранят предаването на лични данни на трета държава, когато считат с оглед на обстоятелствата във връзка с това предаване, че стандартните клаузи за защита на данните не са или не могат да бъдат спазени в тази трета държава и че защитата на предаваните данни, изисквана от правото на Съюза, не може да бъде осигурена с други

[58] Решение за изпълнение на Комисията от 12 юли 2016 година съгласно Директива 95/46/ЕО относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (ОВ L 207, 2016 г., стр. 1).

средства, в случай че самият установен в Съюза износител не е спрял или прекратил това предаване (т. 121 и т. 3 от диспозитива).

По-нататък, Съдът проверява валидността на Решение 2010/87. Според Съда валидността на това решение не се поставя под въпрос от самия факт, че съдържащите се в него стандартни клаузи за защита на данните не обвързват, поради своя договорен характер, органите на третата държава, на която могат да се предават данни. Той обаче пояснява, че тази валидност зависи от това дали посоченото решение съдържа ефективни механизми, позволяващи на практика да се осигури спазването на изискването от правото на Съюза ниво на защита и предаването на лични данни, основаващо се на такива клаузи, да бъде спряно или забранено в случай на нарушение на тези клаузи или при невъзможност за спазването им. Съдът установява, че Решение 2010/87 въвежда такива механизми. В това отношение той по-специално подчертава, че това решение установява задължение за износителя на данни и за получателя на предаването предварително да проверят спазването на това ниво на защита в съответната трета държава, и че същото решение задължава този получател да информира износителя на данни за евентуалната си невъзможност да осигури съответствие със стандартните клаузи за защита, като тогава последният може да спре предаването на данни и/или да прекрати сключения с получателя договор (т. 132, 136, 137, 142 и 148 и т. 4 от диспозитива).

Накрая, Съдът проверява валидността на Решение 2016/1250 с оглед на изискванията, произтичащи от ОРЗД, разглеждан във връзка с разпоредбите на Хартата, гарантиращи зачитането на личния и семейния живот, защитата на личните данни и правото на ефективна съдебна защита. В това отношение Съдът отбелязва, че посоченото решение дава предимство, подобно на Решение 2000/520, на изискванията във връзка с националната сигурност, обществения интерес и спазването на американското законодателство, като така прави възможна намесата в основните права на лицата, чиито данни се предават на тази трета държава. Според Съда ограниченията на защитата на личните данни, които произтичат от вътрешноправната уредба на Съединените щати относно достъпа и използването от американските публични органи на такива данни, предадени от Съюза на тази трета държава, и които Комисията е оценила в Решение 2016/1250, не са определени така, че да отговарят на изисквания, които по същество са равностойни на предвидените в правото на Съюза съгласно принципа на пропорционалност, тъй като програмите за наблюдение, основани на тази правна уредба, не са ограничени до строго необходимото. Въз основа на съдържащите се в това решение констатации, Съдът отбелязва, че за определени програми за наблюдение посочената правна уредба изобщо не разкрива наличието на ограничения на съдържащото се в нея оправомощаване за прилагането на тези програми, нито пък съществуването на гаранции за потенциално обхванатите лица, които не са американски граждани. Съдът добавя, че макар същата правна уредба да предвижда изисквания, които американските органи трябва да спазват при прилагането на съответните програми за наблюдение, тя не предоставя на субектите на данни приложими пред съдилищата права срещу американските органи (т. 164, 165, 180—182, 184 и 185).

Що се отнася до изискването за съдебна защита, Съдът постановява, че противно на приетото от Комисията в Решение 2016/1250, посоченият в това решение механизъм на омбудсмана не предоставя на тези лица способ за защита пред орган, предоставящ гаранции, които по същество са равностойни на изискваните в правото на Съюза, който

да може да осигури както независимостта на предвидения от този механизъм омбудсман, така и наличието на норми, които оправомощават посочения омбудсман да приема обвързващи решения по отношение на американските разузнавателни структури. Поради всички тези причини Съдът обявява Решение 2016/1250 за невалидно (т. 195—197 и 201 и т. 5 от диспозитива).

V. Защита на личните данни в интернет

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

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 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 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 и 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 изтрити (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 и 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 и 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)[59]

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 искове 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.

[59] Това решение е представено в Годишния доклад за 2008 г., стр. 49.

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)[60], Директива 2001/29/ЕО относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество[61], Директива 2004/48/ЕО относно упражняването на права върху интелектуалната собственост[62] и Директива 2002/58 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).

Решение от 24 ноември 2011 г., Scarlet Extended (C-70/10, EU:C:2011:771)[63]

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, 2000/31, 2001/29, 2002/58 и 2004/48, 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

---

60 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).

61 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).

62 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).

63 Това решение е представено в Годишния доклад за 2011 г., стр. 40.

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 разноски 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 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. Всъщност 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).

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 и 2004/48 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 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. Презумира 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 във връзка с член 15, параграф 1 от Директива 2002/58 допуска държавите членки да установяват задължение за предаване на лични данни на частноправни лица, за да могат те да предявят граждански искове 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 и 2004/48 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).

Решение от 17 юни 2021 г., M.I.C.M. (C-597/19, EU:C:2021:492)

Предприятието Mircom International Content Management & Consulting (M.I.C.M.) Limited (наричано по-нататък „Mircom“) подава искане за информация срещу Telenet BVBA, доставчик на услуги за достъп до интернет, пред Ondernemingsrechtbank Antwerpen (Търговски съд Антверпен, Белгия, наричан по-нататък „запитващата юрисдикция“). Целта на искането е да се разпореди на Telenet да представи идентификационните данни на своите клиенти въз основа на IP адресите, събрани от специализирано дружество от името на Mircom. Интернет връзките на клиентите на Telenet са били използвани за споделяне на филми от каталога на Mircom в мрежа с равноправен достъп (peer-to-peer) с помощта на BitTorrent протокола. Telenet възразява срещу това искане.

В този контекст запитващата юрисдикция най-напред иска от Съда да установи дали споделянето в посочената мрежа на сегменти от медиен файл, който съдържа защитено произведение, представлява публично разгласяване съгласно правото на Съюза. По-нататък тя иска да установи дали притежателят на права върху интелектуална собственост какъвто е Mircom, който не ги използва, но търси обезщетение от предполагаеми нарушители, може да се ползва от мерките, процедурите и средствата за защита, предвидени в правото на Съюза, с цел да осигури спазването на тези права, например, като иска информация. Накрая запитващата юрисдикция иска от Съда да изясни въпроса дали са законосъобразни, от една страна, начинът, по който IP адресите на клиентите са били събрани от Mircom, и от друга страна, съобщаването на данните, което Mircom е поискало от Telenet.

Съдът постановява, че правото на Съюза[64] по принцип не е пречка нито притежателят на права върху интелектуална собственост или трето лице от негово име систематично да записва IP адресите на потребители на мрежи с равноправен достъп (peer-to-peer), чиито интернет връзки, както се твърди, са били използвани за действия по извършване на нарушение (обработване на данни нагоре по веригата), нито на посочения притежател или на трето лице да се съобщават имената и пощенските адреси на тези потребители, за да му се даде възможност да предяви пред граждански съд иск за обезщетение (обработване на данни надолу по веригата). Инициативите и исканията в това отношение обаче трябва да са основателни и пропорционални, да не представляват злоупотреба и да са предвидени в национална законодателна мярка, която ограничава обхвата на правата и задълженията от правото на Съюза. Съдът уточнява, че последното не установява задължение за дружество като Telenet да съобщава лични данни на частноправни лица, за да могат да предявят граждански искове срещу нарушенията на авторското право. Правото на Съюза обаче позволява на държавите членки да въведат такова задължение (т. 97 и 125—127 и т. 3 от диспозитива).

[64] Член 6, параграф 1,буква е) от ОРЗД и член 15, параграф 1 от Директива 2002/58.

3. Премахване на лични данни от резултатите при търсене

Решение от 24 септември 2019 г. (голям състав), GC и др. (Премахване на чувствителни данни от резултатите при търсене) (C-136/17, ECLI:EU:C:2019:773)[65]

В това решение големият състав на Съда изяснява задълженията на лицата, управляващи интернет търсачки, при отправено до тях искане за премахване на чувствителни данни от резултатите при търсене.

Google отказва да уважи исканията на четири лица да премахне различни хипервръзки от списъка с резултати, който показва интернет търсачката му след търсене на съответните им имена; става дума за хипервръзки, които водят към уебстраници, публикувани от трети лица, и по-точно към статии от пресата. След жалби от тези четири лица Commission nationale de l'informatique et des libertés (Национална комисия по информационните технологии и свободите, Франция) отказва да отправи покана до Google да изпълни въпросните искания за премахване от резултатите при търсене. Сезираният с делото Conseil d'État (Държавен съвет, Франция) отправя запитване до Съда какви са задълженията на лицето, което управлява интернет търсачка, при обработването на искане за премахване от резултатите при търсене съгласно Директива 95/46.

Първо, Съдът припомня, че обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, както и на данни, свързани със здравословното състояние и половия живот, е забранено[66], но от тази забрана има някои изключения и дерогации. Обработването на данни, отнасящи се до закононарушения, наказателни присъди или мерки за сигурност, по принцип може да се извършва само под контрола на официален орган или ако националното законодателство предвижда специфични и подходящи гаранции[67] (т. 39 и 40).

Съдът приема, че забраната и ограниченията за обработването на специалните категории от данни се прилагат по отношение на лицето, което управлява интернет търсачка, по подобие на всеки друг администратор на лични данни. Всъщност целта на тези забрани и ограничения се състои в осигуряването на по-голяма защита по отношение на подобно обработване, което поради особената чувствителност на тези данни може да представлява особено тежко вмешателство в основните права на зачитане на личния живот и на защита на личните данни (т. 42—44).

Лицето, което управлява интернет търсачка, обаче е отговорно не поради факта, че лични данни се намират на уебстраница, публикувана от трето лице, а поради факта че препраща към тази страница. При тези условия забраната и ограниченията относно обработването на чувствителни данни се прилагат спрямо лицето, управляващо интернет търсачка, само поради това препращане (реферирane) и следователно посредством

[65] Това решение е представено в Годишния доклад за 2019 г., стр. 122.
[66] Член 8, параграф 1 от Директива 95/46 и член 9, параграф 1 от Регламент 2016/679.
[67] Член 8, параграф 5 от Директива 95/46 и член 10 от Регламент 2016/679.

проверка, която трябва да се извърши под контрола на компетентните национални органи въз основа на подадено от съответното лице искане (т. 46 и 47).

Второ, Съдът приема, че когато лицето, управляващо интернет търсачка, е сезирано с искане за премахване на чувствителни данни от резултатите при търсене, то по принцип е длъжно, освен при някои изключения, да уважи това искане. Що се отнася до тези изключения, лицето, управляващо интернет търсачка, може по-специално да откаже да изпълни такова искане, когато констатира, че връзките водят към данни, които явно са направени публично достояние от съответното физическо лице[68], при условие че препращането към такива връзки отговаря на другите изисквания за законосъобразност на обработването на лични данни и ако физическото лице няма правото да възрази срещу въпросното препращане по съображения, свързани с неговото конкретно положение[69] (т. 65 и 69).

Във всички случаи, когато лицето, което управлява интернет търсачка, е сезирано с искане за премахване от резултатите при търсене, то трябва да провери дали включването в списъка с резултати на връзката към уебстраница, на която са публикувани чувствителни данни, който списък се показва след търсене, извършено въз основа на името на това лице, се оказва напълно необходимо за защитата на свободата на информация на потребителите на интернет, които са потенциално заинтересовани да имат достъп до тази страница посредством такова търсене. В това отношение Съдът подчертава, че ако правото на зачитане на личния живот и правото на защита на личните данни по принцип имат предимство пред свободата на информация на потребителите на интернет, това равновесие все пак в конкретни случаи може да зависи от естеството на въпросната информация и от чувствителността ѝ по отношение на личния живот на съответното физическо лице, както и от интереса на обществеността да разполага с тази информация, който може да бъде различен по-специално в зависимост от ролята на това лице в обществения живот (т. 66 и 68).

Трето, Съдът приема, че при подадено искане за премахване от резултатите при търсене на данни за наказателно производство срещу съответното физическо лице, които се отнасят до по-ранен етап от това производство и вече не отговарят на действителното положение, лицето, което управлява интернет търсачка, трябва да прецени дали с оглед на всички обстоятелства по случая посоченото физическо лице има право въпросната информация да не бъде повече свързвана към настоящия момент с неговото име чрез списък с резултати, който се показва след търсене, извършено въз основа на това име. Ако обаче случаят не е такъв, поради факта че включването на разглежданата връзка се оказва напълно необходимо за съвместяване на правото на зачитане на личния живот и на правото на защита на данните на съответното физическо лице със свободата на информация на потенциално заинтересованите интернет потребители, управляващото интернет търсачка лице е длъжно, най-късно при искането за премахване от резултатите при търсене, да преустрои списъка с резултатите, така че общата представа, която получава интернет потребителят, да отразява действителното съдебно положение, което

[68] Член 8, параграф 2, буква д) от Директива 95/46 и член 9, параграф 2, буква д) от Регламент 2016/679.
[69] Член 14, първа алинея, буква а) от Директива 95/46 и член 21, параграф 1 от Регламент 2016/679.

по-специално налага връзки към уебстраници, съдържащи съответната информация, да се появяват на първо място в този списък (т. 77 и 78).

Решение от 24 септември 2019 г. (голям състав), Google (Териториален обхват на премахването от резултатите при търсене) (C-507/17, ECLI:EU:C:2019:772)[70]

Националната комисия по информационните технологии и свободите (Франция) (наричана по-нататък „CNIL“) приканва Google, когато изпълнява искания за премахване от резултатите при търсене, да заличава съответните хипервръзки към уебстраници с лични данни на субекта от списъка с резултатите, който се показва след търсене въз основа на името на този субект на данни, във всички разширения на имена на домейни от своята интернет търсачка. След като Google отказва да изпълни тази покана, CNIL му налага санкция в размер на 100 000 EUR. Сезиран от Google, Conseil d'État (Държавен съвет, Франция) отправя запитване до Съда какъв е териториалният обхват на задължението на лицето, което управлява интернет търсачка, да прилага правото на премахване от резултатите при търсене съгласно Директива 95/46.

Съдът най-напред припомня, че на основание на правото на Съюза физическите лица могат да предявят правото си на премахване от резултатите при търсене пред управляващото интернет търсачка лице, което разполага с едно или повече места на установяване на територията на Съюза, независимо дали обработването на лични данни (в случая включване в резултатите при търсене на хипервръзки към уебстраници, на които се появяват лични данни на предявяващото това право лице) се извършва в Съюза или не[71].

Относно обхвата на правото на премахване от резултатите при търсене Съдът приема, че управляващото интернет търсачка лице е длъжно да извърши това премахване не във всички версии на своята търсачка, а във версиите ѝ, съответстващи на всички държави членки. В това отношение той отбелязва, че наистина предвид характеристиките на интернет и на интернет търсачките евентуалното премахване от резултатите при търсене във всички версии на една търсачка би било в състояние да осъществи напълно целта на законодателя на Съюза да гарантира високо ниво на защита на личните данни в целия Съюз, но все пак от правото на Съюза[72] изобщо не следва, че за да се гарантира постигането на такава цел, законодателят на Съюза е избрал да предостави на това право на премахване от резултатите обхват, който излиза извън територията на държавите членки. По-конкретно, макар правото на Съюза да въвежда механизми за сътрудничество между надзорните органи на държавите членки, за да могат да стигнат до единно решение, основано на претегляне между, от една страна, правото на зачитане на личния живот и на защита на личните данни и от друга, интереса на обществеността в различните държавите членки да има достъп до информация, следва да се отбележи, че понастоящем не са предвидени такива механизми, що се отнася до обхвата на премахването от резултатите при търсене извън Съюза (т. 62 и 73).

---

70 Това решение е представено в Годишния доклад за 2019 г., стр. 124.

71 Член 4, параграф 1, буква а) от Директива 95/46 и член 3, параграф 1 от Регламент 2016/679.

72 Член 12, буква б) и член 14, първа алинея, буква а) от Директива 95/46 и член 17, параграф 1 от Регламент 2016/679.

В настоящия си етап на развитие правото на Съюза задължава управляващото интернет търсачка лице да извърши исканото премахване от резултатите при търсене не само във версията на интернет търсачката, съответстваща на държавата членка по пребиваване на лицето с право на такова премахване, а във версиите ѝ, съответстващи на всички държави членки, и то по-специално за да се гарантира последователно и високо ниво на защита в целия Съюз. Освен това, ако е необходимо, управляващият интернет търсачката трябва да вземе достатъчно ефикасни мерки, за да бъдат възпрени или поне сериозно разколебани интернет потребителите в Съюза да осъществяват, евентуално от версия на интернет търсачката, съответстваща на трета държава, достъп до хипервръзките, предмет на искането за премахване, а националната юрисдикция следва да провери дали мерките, приети от управляващото търсачката лице, отговарят на тези изисквания (т. 70).

Накрая Съдът подчертава, че макар правото на Съюза да не изисква от лицето, управляващо интернет търсачка, да извършва премахване от резултатите при търсене във всички нейни версии, то обаче и не забранява това. Следователно надзорният или съдебният орган на държава членка запазва компетентността си да извърши съгласно националните стандарти за защита на основните права претегляне между, от една страна, правото на субекта на данни да се зачита личният му живот и да се защитават личните му данни, и от друга, правото на свобода на информация и след това претегляне да изиска евентуално от управляващото интернет търсачката лице да извърши премахване от резултатите при търсене във всички нейни версии (т. 65 и 72).

4. Съгласие от потребителите на уебсайтове за съхраняването на информация

Решение от 1 октомври 2019 г. (голям състав), Planet49 (C-673/17, ECLI:EU:C:2019:801)[73]

С това решение Съдът постановява, че даването на съгласие за съхраняването на информация и достъпа до информация с помощта на бисквитки, инсталирани в крайното оборудване на потребител на уебсайт, не е действително, когато разрешението произтича от предварително маркирано с отметка квадратче, независимо от това дали съответната информация представлява или не лични данни. Освен това Съдът уточнява, че доставчикът на услуги трябва да укаже на потребителя на уебсайта продължителността на функциониране на бисквитките, както и дали трети лица имат или нямат възможност за достъп до тях.

Спорът в главното производство е относно организирането на промоционална игра от Planet49 на уебсайта www.dein-macbook.de. За да участват, интернет потребителите трябва да въведат името и адреса си на уебстраница, на която се намират полета за отбелязване. Полето, с което се разрешава инсталирането на бисквитки, е предварително отметнато. Сезиран с жалба на германската Федерация на сдруженията на потребители, Bundesgerichtshof (Федерален върховен съд, Германия) изпитва съмнения относно действителността на съгласие, получено от потребителите с помощта на предварително отметнато поле, както и относно обхвата на задължението за предоставяне на информация, възложено на доставчика на услуги.

Преюдициалното запитване по същество се отнася до тълкуването на понятието за съгласие по смисъла на Директива 2002/58[74], във връзка с Директива 95/46[75] и във връзка с ОРЗД[76].

Първо, Съдът отбелязва, че член 2, буква з) от Директива 95/46/ЕО, към която препраща член 2, буква е) от Директива 2002/58, дефинира съгласието като „всяко свободно изразено, конкретно и информирано указание за волята на съответното физическо лице, с което то дава израз на своето съгласие за обработка на личните данни, които се отнасят до него“. Той отбелязва, че изискването за „манифестиране“ на воля от страна на съответното лице очевидно изисква положително, а не отрицателно действие. Съгласието, дадено посредством предварително отметнато поле, обаче не е свързано с положително действие от страна на потребителя на уебсайт. Освен това генезисът на член 5, параграф 3 от Директива 2002/58, която след изменението си с Директива 2009/136 предвижда, че потребителят трябва да „е дал своето съгласие“ за инсталирането на бисквитки, показва, че съгласието на потребителя вече не може да се презумира и трябва да произтича от негово положително действие. Накрая, активно съгласие вече се

---

73 Това решение е представено в Годишния доклад за 2019 г., стр. 125.

74 Член 2, буква е) и член 5, параграф 3 от Директива 2002/58, изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. (ОВ L 337, 2009 г., стр. 11).

75 Член 2, буква з) от Директива 95/46.

76 Член 6, параграф 1, буква а) от Регламент 2016/679.

предвижда в ОРЗД[77], член 4, точка 11 от който изисква волеизявление под формата по-специално на „ясно потвърждаващо действие“, а съображение 32 от същия изрично изключва наличието на съгласие в случай на „мълчание[...], предварително отметнати[...] полета или липса[...] на действие“ (т. 49, 52, 56 и 62).

Поради това Съдът постановява, че даването на съгласие не е действително, когато съхраняването на информация или достъпът до информация, която вече се съхранява на крайното оборудване на потребител на уебсайт, се позволява чрез предварително маркирано с отметка квадратче, от което потребителят трябва да премахне отметката, за да откаже съгласието си. Той добавя, че обстоятелството, че потребителят натиска бутона за участие в разглежданата промоционална игра, не би могло да бъде достатъчно, за да се счита, че даването на съгласие от негова страна за записването на бисквитки е било действително (т. 63).

Второ, Съдът констатира, че член 5, параграф 3 от Директива 2002/58 има за цел да защити потребителя от всяка намеса в личния му живот, независимо от въпроса дали намесата е свързана или не с лични данни. От това следва, че понятието за съгласие не трябва да се тълкува по различен начин в зависимост от това дали информацията, която се съхранява или консултира на крайното оборудване на потребител на уебсайт, представлява или не лични данни (т. 69 и 71).

Трето, Съдът отбелязва, че член 5, параграф 3 от Директива 2002/58 изисква потребителят да е дал съгласие след получаване на ясна и изчерпателна информация, по-специално относно целите на обработването. Ясната и изчерпателна информация трябва да позволи на потребителя лесно да определи последиците от евентуално даденото съгласие и да гарантира, че то се дава напълно съзнателно. В това отношение Съдът приема, че продължителността на функционирането на бисквитките, както и възможността трети лица да имат или не достъп до тези бисквитки, са част от ясната и изчерпателна информация, която трябва да се предостави на потребителя на уебсайт от доставчика на услуги (т. 73—75 и 81).

VI. 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)[78]

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 транспонирала неправилно изискването за „пълна независимост“ на

[77] Член 6, параграф 1, буква а) от Регламент 2016/679.
[78] Това решение е представено в Годишния доклад за 2010 г., стр. 36.

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.

От своя страна Федерална република Германия поддържа, че член 28, параграф 1, втора алинея от Директива 95/46 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.

Съдът постановява, че предвидената в Директива 95/46 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 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 (C-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.

Съдът установява, че Австрия не е изпълнила задълженията си, като по същество приема, че зададеният от Директива 95/46 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 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 № 45/2001, за да може да отговаря на критерия за независимост по упоменатата разпоредба от Директива 95/46. Всъщност държавите членки не са длъжни да възпроизведат в националното си законодателство аналогични на предвидените в глава V от Регламент № 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 (т. 58).

Решение от 8 април 2014 г. (голям състав), Комисия/Унгария (C-288/12, EU:C:2014:237)[79]

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.

[79] Това решение е представено в Годишния доклад за 2014 г., стр. 65.

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 и 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)[80]

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.

Сезиран с касационна жалба, Kúria (Върховен съд, Унгария) изразява съмнения относно определянето на приложимото право и правомощията на унгарския надзорен орган

[80] Това решение е представено в Годишния доклад за 2015 г., стр. 57.

предвид член 4, параграф 1 и член 28 от Директива 95/46. Затова той отправя няколко преюдициални въпроса до Съда.

Що се отнася до приложимото национално право, Съдът постановява, че член 4, параграф 1, буква а) от Директива 95/46 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 и 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, 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 и 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 IV, „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 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 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).

Решение от 5 юни 2018 г. (голям състав), Wirtschaftsakademie Schleswig-Holstein (C-210/16, ECLI:EU:C:2018:388)

В това решение (вж. също рубрика II.5, „Понятие за администратор на лични данни“), което се отнася в частност до тълкуването на членове 4 и 28 от Директива 95/46, Съдът се произнася по обхвата на правомощията за намеса на надзорните органи при обработване на лични данни, в което участват няколко субекта.

Съдът постановява, че когато установено извън Европейския съюз предприятие (като американското дружество Facebook) има няколко обекта в различни държави членки, надзорният орган на държава членка има право да упражни правомощията си по член 28, параграф 3 от тази директива по отношение на разположен на територията на тази държава членка обект на това предприятие (в случая Facebook Germany), въпреки че съгласно разпределението на дейностите в рамките на групата, от една страна, обектът отговаря единствено за продажбата на рекламни пространства и за други маркетингови дейности на територията на посочената държава членка, а от друга страна, изключителна отговорност за събирането и обработването на лични данни за цялата територия на Европейския съюз се носи от обект, разположен в друга държава членка (в случая Facebook Ireland) (т. 64 и т. 2 от диспозитива).

Освен това Съдът пояснява, че когато надзорният орган на държава членка възнамерява да упражни по отношение на организация, установена на територията на тази държава

членка, правомощията за намеса по член 28, параграф 3 от Директива 95/46 заради нарушения на правилата относно защитата на личните данни, допуснати от отговарящото за обработването на тези данни като администратор трето лице със седалище в друга държава членка (в случая Facebook Ireland), този надзорен орган е компетентен да прецени самостоятелно от надзорния орган на последната държава членка (Ирландия) законосъобразността на такова обработване на данни и може да упражни правомощията си за намеса по отношение на установената на негова територия организация, без предварително да поиска намесата на надзорния орган на другата държава членка (т. 74 и т. 3 от диспозитива).

Решение от 15 юни 2021 (голям състав), Facebook Ireland и др. (C-645/19, EU:C:2021:483)

На 11 септември 2015 г. председателят на Белгийската комисия за защита на личния живот (наричана по-нататък „CPVP“) сезира Nederlandstalige rechtbank van eerste aanleg Brussel (Първоинстанционен нидерландскоезичен съд, Брюксел, Белгия) с иск за преустановяване на нарушение срещу Facebook Ireland, Facebook Inc. и Facebook Belgium с предмет да се прекратят нарушенията на законодателството за защитата на данните, за които се твърди, че са извършени от Facebook. Тези нарушения се състоят по-специално в събирането и използването на информация за поведението при сърфиране на белгийските интернет потребители, които притежават или не профил във Facebook, посредством различни технологии като cookies (бисквитки), социалните модули[81] или пикселите.

На 16 февруари 2018 г. този съд се обявява за компетентен да се произнесе по иска, а по същество постановява, че социалната мрежа Facebook не е информирала в достатъчна степен белгийските интернет потребители за събирането и използването на съответната информация. От друга страна, даденото от интернет потребителите съгласие за събирането и обработването на посочената информация е прието за невалидно.

На 2 март 2018 г. Facebook Ireland, Facebook Inc. и Facebook Belgium обжалват това решение пред Hof van beroep te Brussel (Апелативен съд Брюксел, Белгия) — запитващата юрисдикция по настоящото дело. Пред тази юрисдикция Белгийският орган за защита на личните данни (наричан по-нататък „APD“) действа като правоприемник на председателя на CPVP. Запитващата юрисдикция приема, че е компетентна да се произнесе само по въззивната жалба на Facebook Belgium.

Запитващата юрисдикция изпитва съмнения относно последиците от прилагането на механизма за „обслужване на едно гише“, предвиден в ОРЗД[82], за компетентността на APD, и по-специално поставя въпроса дали за фактите, настъпили след влизането в сила на ОРЗД, а именно 25 май 2018 г., APD може да предяви иск срещу Facebook Belgium, след като Facebook Ireland е идентифицирано като администратор на съответните данни. Всъщност след тази дата, и по-специално в приложение на предвидения в ОРЗД принцип за „обслужване на едно гише“, единствено Ирландският комисар за защита на личните

[81] Например бутоните „Харесвам“ или „Споделям“.

[82] Според член 56, параграф 1 от ОРЗД: „Без да се засяга член 55, надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да действа като водещ надзорен орган за трансграничното обработване, извършвано от посочения администратор или обработващ лични данни“.

данни бил компетентен да предяви иск за преустановяване на нарушение под надзора на ирландските юрисдикции (т. 36 и 37).

В решението си, постановено от голям състав, Съдът уточнява правомощията на националните надзорни органи в рамките на ОРЗД. Така, той по-специално приема, че при определени условия този регламент допуска надзорен орган на държава членка да упражнява правомощието си да довежда твърдените нарушения на ОРЗД до знанието на юрисдикция на тази държава и да инициира съдебни производства във връзка с трансгранично обработване на данни[83], при положение че не е водещият орган във връзка с това обработване (т. 1 от диспозитива).

На първо място, Съдът уточнява условията, при които национален надзорен орган, който няма качеството на водещ орган, що се отнася до трансгранично третиране, трябва да упражни правомощието си да довежда твърдените нарушения на ОРЗД до знанието на юрисдикция на държава членка и по целесъобразност да инициира съдебни производства, за да осигури прилагането на този регламент. Така, от една страна, ОРЗД трябва да предостави на този надзорен орган компетентност да приеме решение, в което се установява нарушение на предвидените в този регламент правила, и от друга страна, това правомощие трябва да се упражнява при спазване на процедурите за сътрудничество и съгласуваност, предвидени в този регламент[84] (т. 75 и т. 1 от диспозитива).

Всъщност при трансграничното обработване ОРЗД предвижда механизма за „обслужване на едно гише“[85], който се основава на разпределяне на правомощията между „водещ надзорен орган“ и съответните други национални надзорни органи. Този механизъм изисква тясно, лоялно и ефективно сътрудничество между тези органи, за да се осигури последователна и еднородна защита на правилата относно защитата на личните данни и за да се запази по този начин полезното му действие. ОРЗД установява за тази цел принципната компетентност на водещия надзорен орган да приеме решение, в което се установява, че трансгранично обработване нарушава предвидените в този регламент правила[86], докато компетентността на другите национални надзорни органи да приемат подобно решение, дори временно, представлява изключение[87]. При упражняването на правомощията си обаче водещият надзорен орган не може да се освободи от задължителен диалог, както и от лоялно и ефективно сътрудничество със съответните други надзорни органи. Поради това в рамките на това сътрудничество водещият надзорен орган не може да пренебрегне становищата на другите засегнати надзорни органи, като всяко относимо и обосновано възражение, изразено от някой от последните органи, води до блокиране, поне временно, на приемането на проекторешението на водещия надзорен орган (т. 50—53, 56—59 и 63—65).

---

83 По смисъла на член 4, точка 23 от ОРЗД.

84 Предвидени в членове 56 и 60 от ОРЗД.

85 Член 56, параграф 1 от ОРЗД.

86 Член 60, параграф 7 от ОРЗД.

87 Член 56, параграф 2 и член 66 от ОРЗД установява изключенията от принципа, че водещият надзорен орган е компетентен да взема решения.

От друга страна, според Съда обстоятелството, че надзорен орган на държава членка, който не е водещият надзорен орган, що се отнася до трансгранично обработване на данни, може да упражни правомощието да довежда твърдените нарушения на ОРЗД до знанието на юрисдикция на тази държава и да инициира съдебни производства само при спазване на правилата за разпределяне на правомощията за вземане на решения между водещия надзорен орган и другите надзорни органи[88], съответства на членове 7, 8 и 47 от Хартата на основните права на Европейския съюз, които гарантират на засегнатото лице съответно правото на защита на личните му данни и правото на ефективни правни средства за защита (т. 67).

На второ място, Съдът приема, че в случай на трансгранично обработване на данни упражняването на правомощието на надзорен орган на държава членка, различен от водещия надзорен орган, да инициира съдебно производство[89], не изисква администраторът или обработващият лични данни, що се отнася до трансграничното обработване на лични данни, което е предмет на това съдебно производство, да разполага с основно място на установяване или с друго място на установяване на територията на тази държава членка. Упражняването на това правомощие обаче трябва да попада в териториалния обхват на ОРЗД[90], което предполага администраторът или обработващият лични данни за трансграничното обработване да разполага с място на установяване на територията на Съюза (т. 80, 83 и 84 и т. 2 от диспозитива).

На трето място, Съдът постановява, че в случай на трансгранично обработване на данни правомощието на надзорен орган на държава членка, различен от водещия надзорен орган, да довежда всички твърдени нарушения на ОРЗД до знанието на юрисдикция на тази държава и по целесъобразност да инициира съдебни производства, може да бъде упражнено както по отношение на основното място на установяване на администратора, което се намира в държавата членка на този орган, така и по отношение на друго място на установяване на този администратор, доколкото предметът на съдебното производство е обработване на данни в контекста на дейностите на това място на установяване и доколкото въпросният орган е компетентен да упражни това правомощие.

Съдът обаче уточнява, че упражняването на това правомощие предполага ОРЗД да е приложим. Тъй като в случая дейностите на намиращото се в Белгия място на установяване на групата Facebook са неразривно свързани с обработването на разглежданите в главното производство лични данни, чийто администратор е Facebook Ireland, що се отнася до територията на Съюза, това обработване се извършва „в контекста на дейностите на дадено място на установяване на администратора“ и следователно попада в обхвата на ОРЗД (т. 94—96 и т. 3 от диспозитива).

На четвърто място, Съдът постановява, че когато надзорен орган на държава членка, който не е „водещият надзорен орган“, е предявил иск с предмет трансгранично

88 Предвидени в членове 55 и 56 във връзка с член 60 от ОРЗД.

89 По силата на член 58, параграф 5 от ОРЗД.

90 Член 3, параграф 1 от ОРЗД предвижда, че този регламент се прилага за обработването на лични данни „в контекста на дейностите на дадено място на установяване на администратор или обработващ лични данни в Съюза, независимо дали обработването се извършва в Съюза или не“.

обработване на лични данни преди датата на влизане в сила на ОРЗД съдебно производство, по силата на правото на Съюза този иск може да бъде поддържан на основание на разпоредбите на Директива 95/46, която остава приложима по отношение на нарушенията на предвидените в нея правила, които нарушения са извършени до датата, на която тази директива е отменена. Освен това този орган може да предяви иск за нарушения, извършени след датата на влизане в сила на ОРЗД, доколкото става въпрос за едно от положенията, при които по изключение този регламент предоставя на същия орган компетентност да приеме решение, в което се установява, че съответното обработване на данни нарушава предвидените в този регламент правила и при спазване на предвидените в него процедури за сътрудничество (т. 105 и т. 4 от диспозитива).

На пето място, Съдът признава директния ефект на разпоредбата от ОРЗД, по силата на която всяка държава членка урежда със закон нейният надзорен орган да има правомощието да довежда нарушенията на този регламент до знанието на съдебните органи и по целесъобразност да инициира съдебни производства. Следователно такъв орган може да се позове на тази разпоредба, за да инициира или продължи съдебен процес срещу частноправни субекти, дори тази разпоредба да не е била специално въведена в законодателството на съответната държава членка (т. 113 и т. 5 от диспозитива).

VII. 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 V.1, „Право на възражение срещу обработването на лични данни („право на забрава“) Съдът се произнася и относно териториалния обхват на Директива 95/46.

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, 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, 60 и 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).

VIII. 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 заведения 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 равностоен 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 Регламент № 45/2001.

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 № 1049/2001[91] за получаване на достъп до документи, които съдържат лични данни, разпоредбите на Регламент № 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 № 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 изискала 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 № 1049/2001 не са предоставени никаква изрична и легитимна 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 № 45/2001 (т. 78)[92].

Решение от 16 юли 2015 г., ClientEarth и PAN Europe/ЕОБХ (C-615/13 P, EU:C: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) № 1107/2009[93], 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

[91] 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, 2001 г., стр. 43; Специално издание на български език, 2007 г., глава 1, том 3, стр. 76).

[92] Това решение е представено в Годишния доклад за 2010 г., стр. 15.

[93] 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, 2009 г., стр. 1).

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 № 1049/2001, както и в съответствие със законодателството на Съюза относно защитата на личните данни, в частност Регламент № 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 № 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 му[94] 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 № 45/2001. Тъй като понятията „лични данни“ по смисъла на член 2, буква а) от Регламент (№ 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 неотносимо (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 прибягва 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 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

[94] Решение на Общия съд от 13 септември 2013 г., ClientEarth и PAN Europe/ЕОБХ (T-214/11, EU:T:2013:483).

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, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07, 4.11.11.01.