



Тематичен фиш

Защита на личните данни

Встъпление

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

То е закрепено в първичното право, по-точно в член 8 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“) и в член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС). Това основно право е и тясно свързано с правото на зачитане на личния и семейния живот, закрепено в член 7 от Хартата.

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. Основният правен акт на Съюза в тази област тогава е Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни¹, която от 2018 г. вече не е в сила.

Впоследствие към Директива 95/46 се добавя Директива 2002/58/ЕО², която хармонизира законодателните разпоредби на държавите членки относно защитата на правото на личен живот, що се отнася в частност до обработването на лични данни в сектора на електронните съобщения³. Следва да се отбележи, че за да отчете новото технологично и търговско развитие, законодателят на Съюза започна през 2017 г. преглед на тази директива⁴, който продължава и досега⁵.

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 от 25 май 2018 г. (вж. бележка под линия 6).

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 и поправка в ОВ L 145, 2017 г., стр. 27), 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](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:2014:238)), Съдът обявява тази директива за невалидна, тъй като води до тежко посегателство върху правото на неприкосновеност на личния живот и защитата на личните данни (вж. раздел I.1 от този фиш, „Съвместимост на вторичното право на Съюза с правото на защита на личните данни“).

⁴ На 10 януари 2017 г. Комисията внесе предложение за заместването ѝ с регламент за неприкосновеността на личния живот и електронните съобщения.

⁵ На 10 февруари 2021 г. Съветът на Европейския съюз одобри мандат за преговори с цел преразглеждане на правилата в областта на защитата на неприкосновеността на личния живот и поверителността при използването на електронни съобщителни услуги, което позволи да започнат преговори с Европейския парламент. Текстът на предложението за регламент 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) може да се намери тук: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

През 2016 г. Европейският съюз реформира общата правна рамка в тази област. За целта са приети Регламент (ЕС) 2016/679⁶ относно защитата на личните данни (наричан по-нататък „ОРЗД“), който отменя Директива 95/46 и се прилага от 25 май 2018 г., както и Директива (ЕС) 2016/680⁷ за защита на данните в наказателната област, която се прилага от 6 май 2018 г.

Що се отнася до обработването на лични данни от институциите и органите на ЕС, от 11 декември 2018 г. защитата на данните се осигурява в частност с Регламент (ЕС) 2018/1725⁸. Този регламент цели да приведе във възможно най-голяма степен правилата в тази област в съответствие с правилата на ОРЗД в интерес на постигането на съгласуван подход към защитата на личните данни навсякъде в Съюза.

Накрая, за да посрещне предизвикателствата, създавани от новите технологии, от 2020 г. законодателят на Съюза започва да приема нови законодателни мерки⁹, които се съчетават с разпоредбите на правото на Съюза относно защитата на личните данни.

Предвид богатата практика на Съда в областта на защитата на личните данни настоящият тематичен фиш ще представи избрани решения с основополагащо значение в областта или с важен принос за развитието на тази съдебна практика, като особено внимание ще бъде обърнато на решенията на големия състав на Съда. По-конкретно целта на този фиш е да обхване както съдебната практика относно общата уредба на защитата на личните данни, а именно практиката по тълкуването на Директива 95/46 и ОРЗД, така и съдебната практика относно секторните регулации, и в частност тези в сектора на електронните съобщения и в областта на наказателното право. Освен това идеята е да бъдат представени

⁶ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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, и поправка в ОВ L 127, 2018 г., стр. 2).

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, и поправка в ОВ L 127, 2018 г., стр. 6).

⁸ 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 (ОВ L 295, 2018 г., стр. 39).

⁹ Тук следва да се отбележат в частност три законодателни инициативи: i) Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 година относно европейска рамка за управление на данните и за изменение на Регламент (ЕС) 2018/1724 (Акт за управление на данните) (ОВ L 152, 2022 г., стр. 1) и Регламент (ЕС) 2023/2854 на Европейския парламент и на Съвета от 13 декември 2023 година относно хармонизирани правила за справедлив достъп до данни и за тяхното използване и за изменение на Регламент (ЕС) 2017/2394 и Директива (ЕС) 2020/1828 (Акт за данните) (ОВ L, 2023/2854, стр. 1, и поправка в ОВ L, 2024/90790); ii) законодателният пакет за цифровите услуги и пазари, който се състои от Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги) (ОВ L 277, 2022 г., стр. 1) и от Регламент (ЕС) 2022/1925 на Европейския парламент и на Съвета от 14 септември 2022 година за достъпни и справедливи пазари в цифровия сектор и за изменение на директиви (ЕС) 2019/1937 и (ЕС) 2020/1828 (Акт за цифровите пазари) (ОВ L 265, 2022 г., стр. 1, и поправка в ОВ L, 2025/90024); и iii) първото по рода си законодателно предложение за създаване на регулаторна рамка за изкуствения интелект, което се конкретизира в регламент за изкуствения интелект (ОВ L, 2024/1689).

избрани решения относно нормативните актове, които се прилагат хоризонтално за цялата област, като на първо място се открие определящата роля на Хартата при развитието на съдебната практика.

Съдържание

ВСТЪПЛЕНИЕ	3
I. ПРАВОТО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ПРИЗНАТО С ХАРТАТА НА ОСНОВНИТЕ ПРАВА НА ЕВРОПЕЙСКИЯ СЪЮЗ.....	8
1. Съвместимост на вторичното право на Съюза с правото на защита на личните данни	8
2. Спазване на правото на защита на личните данни при прилагането на правото на Съюза.....	20
II. ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ ПО СМИСЪЛА НА ОБЩАТА УРЕДБА В ТАЗИ ОБЛАСТ	22
1. Обхват на общата уредба.....	22
2. Понятие за лични данни	28
3. Понятие за обработване на лични данни.....	31
4. Понятие за файл с лични данни.....	36
5. Понятие за администратор на лични данни.....	37
6. Понятие за съвместен администратор.....	39
7. Условия за законосъобразност на обработването на лични данни	40
III. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ ПО СМИСЪЛА НА СЕКТОРНАТА УРЕДБА	47
1. Обработване на лични данни в сектора на електронните съобщения	47
2. Обработване на лични данни в областта на наказателното право	68
IV. ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ СТРАНИ	72
V. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ИНТЕРНЕТ	81
1. Право на възражение срещу обработването на лични данни („право на забравя“).....	81
2. Обработване на лични данни и право на интелектуална собственост	82
3. Премахване на лични данни от резултатите при търсене.....	85
4. Съгласие от потребителите на уебсайтове за съхраняването на информация	95
5. Обработване на лични данни в социалните мрежи онлайн	97
VI. НАЦИОНАЛНИ НАДЗОРНИ ОРГАНИ	101
1. Обхват на изискването за независимост.....	101
2. Определяне на приложимото право и на компетентния надзорен орган	104
3. Правомощия на националните надзорни органи	105

4. Условия за налагане на административни наказания.....	111
5. Връзка на правомощията на националните надзорни органи с правомощията на другите национални органи.....	116

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 u Eifert (C-92/09 и C-93/09, [EU:C:2010:662](#))

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) № 1290/2005¹⁰ и № 259/2008¹¹, които уреждат финансирането на общата селскостопанска политика и предвиждат задължително публикуване на информация за физическите лица — бенефициери на ЕФГЗ и ЕЗФРСР.

В този контекст Verwaltungsgericht Wiesbaden (Административен съд Висбаден, Германия) отправя до Съда няколко въпроса за валидността на отделни разпоредби от Регламент № 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

¹⁰ 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).

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

отпуснатите им суми накърнява правото им на зачитане на техния личен живот като цяло и правото на защита на техните лични данни в частност.

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. 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.

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. 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.

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

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.

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 същественото 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.

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. 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. 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. 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.

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.

Решение от 21 юни 2022 г. (голям състав), *Ligue des droits humains (C-817/19, EU:C:2022:491)*

Резервационните данни на пътниците (Passenger Name Record, или също PNR данни) представляват информация за резервациите, съхранявани от въздушните превозвачи в техните системи за резервации и контрол на излитанията. Директивата за PNR¹² задължава тези превозвачи да предават PNR данните на всички пътници във въздушния транспорт при външни за ЕС полети на звеното за данни за пътниците (наричано по-нататък „ЗДП“) на държавата членка на пристигане или на излитане на съответния полет с оглед на борбата срещу тероризма и тежките престъпления. Всъщност така предадените PNR данни подлежат на предварителна оценка от ЗДП¹³, а впоследствие се съхраняват за евентуална последваща оценка от компетентните органи на съответната държава членка или тези на друга държава членка. Държавите членки могат да решат да прилагат Директивата и към вътрешни за ЕС полети¹⁴.

¹² Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 година относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления (ОВ L 119, 2016 г., стр. 132) (наричана по-нататък „Директивата за PNR“).

¹³ Тази предварителна оценка има за цел да се идентифицират лицата, за които се налага допълнителна проверка от компетентните органи, предвид факта, че тези лица може да са замесени в терористично престъпление или тежко престъпление. Тази оценка се извършва систематично и автоматизирано чрез съпоставяне на PNR данните с бази данни, „които са от значение“, или чрез обработване съобразно предварително определени критерии, както е предвидено в член 6, параграф 2, буква а) и параграф 3 от Директивата за PNR.

¹⁴ Като използват възможността, предвидена в член 2 от Директивата за PNR.

Cour constitutionnelle (Конституционен съд, Белгия) е сезиран от Ligue des droits humains с жалба за отмяна на белгийския закон, който транспонира в белгийското право както Директивата за PNR, така и Директивата за API¹⁵. Според жалбоподателя този закон нарушава правото на зачитане на личния живот и на защита на личните данни. Той оспорва, от една страна, твърде широкия обхват на PNR данните и от друга страна, общия характер на събирането, предаването и обработването на тези данни. Законът нарушавал и свободното движение на хора, тъй като възобновявал непряко граничния контрол, разширявайки PNR системата върху вътрешните за ЕС полети и превозите, извършвани с други средства в Съюза.

В този контекст белгийският Cour constitutionnelle (Конституционен съд) отправя преюдициално запитване до Съда в частност за валидността на Директивата за PNR.

В своето решение, постановено от голям състав, Съдът потвърждава валидността на Директивата за PNR, доколкото тя може да се тълкува в съответствие с Хартата.

В това отношение Съдът постановява, че тъй като направеното от Съда тълкуване на разпоредбите на Директивата за PNR с оглед на основните права, гарантирани в членове 7, 8 и 21, и на член 52, параграф 1 от Хартата¹⁶ осигурява съгласуваността на тази директива с тези членове, при разглеждането на поставените въпроси не се установяват обстоятелства, които могат да засегнат валидността на същата директива.

Най-напред Съдът припомня, че актовете на Съюза трябва, доколкото е възможно, да се тълкуват по начин, който не поставя под съмнение тяхната валидност, и в съответствие с цялото първично право, и в частност с разпоредбите на Хартата, поради което държавите членки трябва да не допускат да се основават на нейно тълкуване, което би влязло в конфликт с основните права, защитавани от правния ред на Съюза, или с останалите общи принципи, признати в този правен ред. Що се отнася до Директивата за PNR, Съдът уточнява, че редица съображения и разпоредби от нея изискват такова съответстващо тълкуване, като подчертава значението което законодателят на Съюза, позовавайки се на високото равнище на защита на данните, отдава на пълното зачитане на основните права, закрепени в Хартата.

¹⁵ Директива 2004/82/ЕО на Съвета от 29 април 2004 година относно задължението на превозвачите да съобщават данни на пътниците (ОВ L 261, 2004 г., стр. 24) (наричана по-нататък „Директивата за API“). Тази директива урежда предаването на предварителни данни на пътниците (като номера и вида на пътния документ и националността) от страна на въздушните превозвачи на компетентните национални органи с цел подобряване на граничния контрол и борба с незаконната имиграция.

¹⁶ Съгласно тази разпоредба всяко ограничаване на правата и свободите, признати от Хартата, трябва да бъде предвидено в закон и да зачита основното съдържание на тези права. Освен това ограничения на тези права и свободи могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

Съдът констатира, че Директивата за PNR предвижда несъмнено сериозна намеса в правата, гарантирани в членове 7 и 8 от Хартата, тъй като по-специално има за цел да въведе режим на постоянен, систематичен и нецеленасочен контрол, включващ автоматизирана оценка на лични данни на всички лица, които използват услугите на въздушния транспорт. Той припомня, че възможността за държавите членки да обосноват такава намеса трябва да се прецени, като се измери нейната тежест и като се провери дали значението на преследваната цел от общ интерес е свързано с тази тежест.

Съдът заключава, че предаването, обработването и съхранението на PNR данни, предвидени в тази директива, могат да се считат за ограничени до строго необходимото за целите на борбата срещу терористичните престъпления и тежките престъпления, при условие че предвидените с посочената директива правомощия се тълкуват стриктно. В това отношение в постановеното днес решение се уточнява по-специално, че:

- Установената с Директивата за PNR система трябва да обхваща само ясно разпознаваема и определена в точките на приложение I към тази директива информация, пряко свързана с извършения полет и съответния пътник, което за някои точки в това приложение означава, че е обхваната само изрично посочената информация¹⁷.
- Прилагането на установената с Директивата за PNR система трябва да се ограничава само до терористичните престъпления и тежките престъпления, които имат обективна връзка, най-малкото непряка, с въздушния превоз на пътниците. Що се отнася до тежките престъпления, прилагането на системата не може да обхване престъпленията, които, макар да отговарят на предвидения с тази директива критерий относно степента на тежест и да са посочени в приложение II към нея, с оглед на особеностите на националната наказателна система спадат към обикновената престъпност.
- Евентуалното разширяване на прилагането на Директивата PNR до всички или до част от полетите в рамките на ЕС, което държава членка може да реши, като използва предвидената в тази директива възможност, трябва да бъде ограничено до строго необходимото. За тази цел то трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, чието решение има обвързващо действие. В това отношение Съдът уточнява, че:

¹⁷ В този смисъл по-специално „информация[та] за плащането“ (т. 6 от приложението) трябва да бъде ограничена до начина на плащане и фактурирането на самолетния билет, без други данни, които нямат пряка връзка с полета, а „[о]бщи[те] забележки“ (т. 12) могат да се отнасят само до изрично посочените в тази точка сведения, които се отнасят до ненавършили пълнолетие пътници във въздушния транспорт.

- Прилагането на тази директива за ограничен до строго необходимото период, който може да бъде удължен, към всички вътрешни за ЕС полети от или към посочената държава членка, не надхвърля границите на строго необходимото само в случаите, когато посочената държава членка констатира наличието на конкретни обстоятелства, които позволяват да се приеме, че тя е изправена пред терористична заплаха, която е действителна и настояща или предвидима¹⁸.
- При липсата на такава терористична заплаха прилагането на посочената директива не може да обхване всички вътрешни за ЕС полети, а трябва да се ограничи до вътрешни за ЕС полети, които се отнасят по-специално до някои маршрути или схеми за пътуване или още до някои летища, за които според преценката на съответната държава членка са налице индиции, които могат да обосноват това прилагане. Строго необходимият характер на това прилагане към така избраните вътрешни за ЕС полети трябва да се преразглежда периодично в зависимост от развитието на обстоятелствата, обосновавали подбора им.
- За целите на предварителната оценка, насочена към идентифициране на лицата, за които се налага допълнителна проверка преди тяхното пристигане или заминаване, която на първо място се извършва посредством автоматизирано обработване, ЗДП може, от една страна, да съпоставя данните само с базите данни относно лицата или предметите, които се издирват или за които е подаден сигнал¹⁹. Тези бази данни трябва да са недискриминационни и да се използват от компетентните органи във връзка с борбата срещу терористичните престъпления и тежките престъпления, които имат обективна връзка, най-малкото непряка, с въздушния превоз на пътниците. От друга страна, що се отнася до предварителната оценка съобразно предварително определени критерии ЗДП не следва да използва технологии за изкуствен интелект в рамките на системи за самообучение (machine learning), които могат да променят процеса на оценка без човешка намеса или контрол, и по-конкретно критериите за оценка, на които се основава резултатът от прилагането на този процес, както и претеглянето на тези критерии. Посочените критерии трябва да са определени така, че да са насочени конкретно към лица, по отношение на които може да съществува разумно подозрение за участие в

¹⁸ Всъщност наличието на такава заплаха може само по себе си да създаде връзка между предаването и обработването на съответните данни и борбата с тероризма. Следователно прилагането за ограничен период на Директивата за PNR към всички вътрешни за ЕС полети от или към посочената държава членка не надхвърля границите на строго необходимото, като решението, с което се предвижда това прилагане, следва да подлежи на ефективен контрол от юрисдикция или от независима административна структура.

¹⁹ А именно базите данни относно лицата или предметите, които се издирват или за които е подаден сигнал по смисъла на член 6, параграф 3, буква а) от Директивата за PNR. За разлика от това анализи въз основа на различни бази данни биха могли да са под формата на извличане на данни (data mining) и да доведат до непропорционално използване на тези данни, предоставящо средствата за установяване на точния профил на съответните лица само поради това че те възнамеряват да пътуват със самолет.

терористични или тежки престъпления, и да отчитат както „уличаващите“ така и „оневиняващите“ факти, като същевременно не водят до пряка или непряка дискриминация²⁰.

- Като се има предвид степента на грешка, присъща на автоматизираното обработване на PNR данни и значителният брой „фалшиви положителни“ резултати, получени вследствие на прилагането му през 2018 г. и 2019 г., годността на установената с Директивата за PNR система за постигане на преследваните цели зависи основно от правилното провеждане с неавтоматизирани средства на извършваната от ЗДП последваща проверка на получените от това обработване резултати. В това отношение държавите членки трябва да предвидят ясни и точни правила, които да насочват и регламентират анализа, извършван от служителите на ЗДП, отговорни за този индивидуален преглед, за да се осигури пълното зачитане на основните права, закрепени в членове 7, 8 и 21 от Хартата, и по-специално да се гарантира последователна административна практика в рамките на ЗДП, съобразена с принципа на недопускане на дискриминация. По-конкретно държавите членки трябва да гарантират, че ЗДП определя обективни критерии за преглед, позволяващи на служителите му да проверяват, от една страна, дали и доколко дадено съвпадение (hit) се отнася действително до лице, което може да е замесено в терористични престъпления или тежки престъпления, и от друга страна, недискриминационния характер на автоматизираното обработване. В този контекст Съдът подчертава още, че компетентните органи трябва да се уверят, че заинтересованото лице може да разбере как функционират предварително определените критерии за оценка и програмите, използващи тези критерии, така че да може да реши, разполагайки с цялата необходима информация, дали да упражни правото си на съдебна защита. По същия начин при упражняването на това на съдебна защита право съдът, натоварен с контрола за законосъобразност на приетото от компетентните органи решение, както и — с изключение на случаите на заплаха за националната сигурност — самото заинтересовано лице, трябва да могат да се запознаят както с всички съображения, така и с доказателствата, въз основа на които е прието това решение, включително с предварително определените критерии за оценка и с функционирането на програмите, използващи тези критерии.

²⁰ Предварително определените критерии трябва да са целенасочени, пропорционални и конкретни и да подлежат на редовен преглед (член 6, параграф 4 от Директивата за PNR). Предварителната оценка съобразно предварително определени критерии трябва да се извършва по недискриминационен начин. Съгласно член 6, параграф 4, четвърто изречение от Директивата за PNR критериите при никакви обстоятелства не са основани на расата или етническия произход на лицето, на неговите политически мнения, религия или философски убеждения, членство в профсъюзи, здравословно състояние, сексуален живот или сексуална ориентация.

- Последващото разкриване и оценка на PNR данните, т.е. след пристигането или отпътуването на съответното лице, могат да се извършват само въз основа на нови обстоятелства и обективни сведения, които или могат да обосноват разумно подозрение за участие на това лице в тежки престъпления, които имат обективна връзка, най-малкото непряка, с въздушния превоз на пътниците, или да позволят да се приеме, че в случая тези данни действително биха могли да подпомогнат борбата с терористични престъпления, които имат такава връзка. Разкриването на PNR данните за целите на такава последваща оценка трябва да се осъществява поначало, освен в надлежно обосновани неотложни случаи, след предварителен контрол, извършван или от юрисдикция, или от независим административен орган, след мотивирано искане от страна на компетентните органи, независимо от това дали искането е направено преди или след изтичането на шестмесечния срок от предаването на PNR данните на ЗДП²¹.

Решение от 22 ноември 2022 г. (голям състав), Luxembourg Business Registers (C-37/20 и C-601/20, [EU:C:2022:912](#))

За целите на борбата и предотвратяването на изпирането на пари и финансирането на тероризма Директивата относно борбата с изпирането на пари²² изисква от държавите членки да водят регистър с информация за действителните собственици²³ на учредените на тяхна територия дружества и други правни образувания. Съгласно изменение на тази директива с Директива 2018/843²⁴ част от споменатата информация трябва да бъде достъпна във всички случаи за всеки член на широката общественост. Въз основа на изменената Директива относно борбата с изпирането на пари (наричана по-нататък „изменената Директива относно борбата с изпирането на пари“) люксембургското законодателство създава Регистър на действителните собственици (наричан по-нататък „РДС“), в който следва да се вписва определена информация за действителните собственици на регистрираните субекти, като тази информация става общодостъпна.

²¹ Съгласно член 12, параграфи 1 и 3 от Директивата за PNR такъв контрол се предвижда изрично само за исканията за разкриване на PNR данните, направени след изтичането на шестмесечния срок от предаването на тези данни на ЗДП.

²² Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета и за отмяна на Директива 2005/60/ЕО на Европейския парламент и на Съвета и на Директива 2006/70/ЕО на Комисията (ОВ L 141, 2015 г., стр. 73, наричана по-нататък „Директивата относно борбата с изпирането на пари“).

²³ Член 3, точка 6 от Директивата относно борбата с изпирането на пари предвижда, че „действителен собственик“ означава физическо лице или лица, което в крайна сметка притежава или контролира клиента и/или физическо лице, или лица, от чието име се осъществява дадена сделка или дейност.

²⁴ Директива (ЕС) 2018/843 на Европейския парламент и на Съвета от 30 май 2018 година за изменение на Директива (ЕС) 2015/849 за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма и за изменение на директиви 2009/138/ЕО и 2013/36/ЕС (ОВ L 156, 2018 г., стр. 43).

В този контекст WM и Sovim SA завеждат дела пред Tribunal d'arrondissement de Luxembourg (Окръжен съд Люксембург), като обжалват съответните откази на Luxembourg Business Registers, администратор на РДС, да уважи исканията им за спиране на достъпа на широката общественост до информацията, която се отнася, по първото дело, за WM в качеството му на действителен собственик на гражданско дружество за управление и придобиване на недвижими имоти, а по второто дело — за действителния собственик на Sovim SA. Поради съмненията си по двете дела относно по-конкретно валидността на разпоредбите от правото Съюза, с които се установява система за публичен достъп до информацията за действителните собственици, Tribunal d'arrondissement de Luxembourg (Окръжен съд Люксембург) отправя преюдициални запитвания до Съда.

В решението си Съдът, заседаващ в голям състав, установява невалидност на частта от Директива 2018/843, с която Директивата относно борбата с изпирането на пари се изменя в смисъл, че държавите членки трябва да гарантират, че информацията за действителните собственици на учредените на тяхна територия дружества и други правни образувания е достъпна във всички случаи за всеки член на широката общественост²⁵.

На първо място, Съдът констатира, че достъпът на широката общественост до информацията за действителните собственици, предвиден в изменената Директива относно борбата с изпирането на пари, представлява тежка намеса в основните права, закрепени съответно в членове 7 и 8 от Хартата, на зачитане на личния живот и на защита на личните данни.

В това отношение Съдът отбелязва, че тъй като съответните данни съдържат информация за идентифицирани физически лица, а именно за действителните собственици на учредените на територията на държавите членки дружества и други правни образувания, достъпът до тях на всеки член на широката общественост засяга основното право на зачитане на личния живот. Освен това предоставянето на такъв достъп на широката общественост представлява обработка на лични данни. Съдът уточнява, че такова предоставяне на достъп на широката общественост представлява намеса в споменатите две основни права, независимо от последващото използване на съобщената информация.

По отношение на тежестта на тази намеса Съдът отбелязва, че доколкото се отнася до действителните собственици, както и до характера и размера на притежаваните от тях права в дружествата или в другите правни образувания, предоставената на широката общественост информация би могла да позволи въз основа на системата от изисквани от съответното национално законодателство повече или по-малко изчерпателни идентификационни данни да се състави профил на

²⁵ Невалидност на член 1, точка 15, буква в) от Директива 2018/843, с който се изменя член 30, параграф 5, първа алинея, буква в) от Директивата относно борбата с изпирането на пари.

благосъстоянието на съответното лице в определени икономически сектори, държави и предприятия, в които то е инвестирало. Освен това посочената информация става достъпна за потенциално неограничен брой лица, така че такова обработване на лични данни може да позволи свободен достъп до тези данни и на лица, които поради причини, чужди на преследваната с тази мярка цел, се стремят да се осведомят по-конкретно за материалното и финансовото положение на действителните собственици. Това е още по-лесно, когато, както е в Люксембург, въпросните данни могат да бъдат намерени в интернет.

Потенциалните рискове за съответните лица от евентуална злоупотреба с личните им данни са още по-големи и поради това че след като бъдат предоставени на широката общественост, тези данни могат да бъдат не само свободно преглеждани, но и запамятвани и разпространявани, като при такива последователни обработвания ефективната им защита срещу злоупотреба става още по-трудна и дори немислима.

На второ място, при разглеждането на обосноваването на разглежданата намеса Съдът, първо, отбелязва, че в случая принципът на законоустановеност е спазен. Всъщност ограничаването на упражняването на споменатите основни права, до което води достъпът на широката общественост до информацията за действителните собственици, е предвидено в законодателен акт, а именно в изменената Директива относно борбата с изпирането на пари. Освен това тази директива, от една страна, изисква по-конкретно информацията да е подходяща, точна и актуална, като изрично посочва някои данни, до които трябва да се даде достъп на широката общественост. От друга страна, директивата установява условията, при които държавите членки могат да предвидят изключения от изискването за такъв достъп.

Второ, Директивата уточнява, че разглежданата намеса не засяга основното съдържание на гарантираните с членове 7 и 8 от Хартата основни права. Макар действително изменената Директива относно борбата с изпирането на пари да не съдържа изчерпателен списък на данните, до които всеки член на широката общественост трябва да има достъп, и държавите членки да имат възможност да предвидят достъп до допълнителна информация, факт е, че може да се получава и разполага само с „подходяща“ информация за действителните собственици и притежаваните права, а това изключва по-специално информация, която не е подходяща свързана с целите на изменената Директива относно борбата с изпирането на пари. Ясно е обаче, че предоставянето на така свързана с тези цели информация на широката общественост все по някакъв начин би накърнило основното съдържание на визираните основни права.

Трето, Съдът подчертава, че с предвидения достъп на широката общественост до информацията за действителните собственици законодателят на Съюза иска да предотврати изпирането на пари и финансирането на тероризма, като чрез по-голяма прозрачност създаде среда, която е по-малко вероятно да бъде използвана

за тези цели, и че това представлява цел от общ интерес, която може да оправдае дори и тежка намеса в закрепените с членове 7 и 8 от Хартата основни права.

Четвърто, по въпроса дали разглежданата намеса е подходяща, необходима и пропорционална, Съдът приема, че достъпът на широката общественост до информацията за действителните собственици би могъл да допринесе за осъществяването на посочената цел.

Според Съда обаче тази намеса не може да се счита за ограничена до строго необходимото. От една страна, строгата необходимост от тази намеса не може да се установи от факта, че критерият, който Директивата относно борбата с изпирането на пари в редакцията ѝ, преди да бъде изменена с Директива 2018/843, е предвиждала и съгласно който всяко лице, което иска да получи достъп до информацията за действителните собственици, трябва да има „законен интерес“, е трудно приложим и прилагането му може да доведе до произволни решения. Всъщност евентуалното наличие на трудности при точното определяне на случаите и условията, при които обществеността може да има достъп до информацията за действителните собственици, не дава основание на законодателя на Съюза да предвиди достъп на широката общественост до тази информация.

От друга страна, съдържащите се в Директива 2018/843 разяснения също не доказват строгата необходимост от разглежданата намеса²⁶. С оглед на обстоятелството, че както се посочва в тези разяснения, достъпът на широката общественост до информацията за действителните собственици трябва да позволи засилен контрол на информацията от страна на гражданското общество, и по-специално на печатните издания и организациите на гражданското общество, Съдът отбелязва, че както печатните издания, така и организациите на гражданското общество, свързани с предотвратяването и борбата с изпирането на пари и финансирането на тероризма, имат законен интерес от достъп до съответната информация. Същото се отнася и за лицата, които желаят да узнаят самоличността на действителните собственици на дружество или друго правно образувание поради намерение да сключат сделки с тях, или за финансовите институции и органите, участващи в борбата срещу изпирането на пари, или престъпленията, свързани с финансирането на тероризма.

Разглежданата намеса не е и пропорционална. В това отношение Съдът констатира, че материалноправните норми, които уреждат тази намеса, не отговарят на изискването за яснота и точност. Всъщност изменената Директива относно борбата с изпирането на пари предвижда, че всеки член на широката общественост има достъп „най-малко“ до посочените в тази разпоредба данни и предоставя на държавите членки възможност да предоставят достъп до

²⁶ Визират се разясненията в съображение 30 от Директива 2018/843.

допълнителна информация, включваща „най-малко“ датата на раждане или данни за съответния действителен собственик. От употребата на изреча „най-малко“ обаче следва, че тази директива разрешава предоставянето на обществеността на данни, които не са достатъчно определени, нито определяеми.

При съпоставянето на сериозността на тази намеса с важността на преследваната цел от общ интерес Съдът установява, че важността на тази цел може да оправдае дори и тежка намеса в предвидените в членове 7 и 8 от Хартата основни права.

При все това обаче, от една страна, борбата срещу изпирането на пари и финансирането на тероризма е отговорност преди всичко на държавните органи и на правни субекти, като кредитни или финансови институции, които по силата на своята дейност имат специфични задължения в тази област. Поради тази причина изменената Директива относно борбата с изпирането на пари предвижда, че информацията за действителните собственици трябва да бъде достъпна във всички случаи за компетентните органи и звената за финансово разузнаване, без никакви ограничения, както и за задължените субекти в рамките на комплексната проверка на клиента²⁷.

От друга страна, в сравнение с предишния режим, който освен достъпа на компетентните органи и на някои правни субекти е предвиждал и достъп на всички лица или организации, които могат да докажат законен интерес, въведеният с Директива 2018/843 режим значително по-тежко засяга гарантираните с членове 7 и 8 от Хартата основни права, без това утежняване да се компенсира от евентуални предимства на втория режим в сравнение с първия по отношение на борбата с изпирането на пари и финансирането на тероризма.

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](#))

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.

²⁷ Член 30, параграф 5, първа алинея, букви а) и б) от изменената Директива относно борбата с изпирането на пари.

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

Сезиран от Kammarätten 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 подобна правна уредба надхвърля границите на строго необходимото и не може да се счита за обоснована в едно демократично общество, както изисква посоченият член 15, параграф 1, тълкуван във връзка с посочените по-горе членове от Хартата.

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.

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 рисковете 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 допринасят за борбата с тежката престъпност или за предотвратяването на сериозен риск за обществената сигурност.

II. Обработването на лични данни по смисъла на общата уредба в тази област

1. Обхват на общата уредба

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/ЕО²⁸, 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/ЕО²⁹, 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.

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.

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

²⁸ 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).

²⁹ 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).

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.

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.

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

През 2010 г. испански гражданин подава жалба до Agencia Española de Protección de Datos (Испанска агенция за защита на данните, наричана по-нататък „AEPD“) срещу La Vanguardia Ediciones SL, дружеството издател на широко разпространяван в Испания всекидневник, както и срещу Google Spain и Google. Той твърди, че когато интернет потребител въведе името му в търсачката на групата Google, списъкът с резултатите съдържа линкове към две страници на всекидневника на La Vanguardia от 1998 г., съдържащи в частност обява за публична продажба на недвижимо имущество във връзка с принудително изпълнение на негови задължения. С жалбата си той иска, от една страна, да се разпорежи на La Vanguardia да премахне посочените страници или да измени съдържанието им или да използва някои от предоставяните от интернет търсачките средства за защита на тези данни. От друга страна, той иска да се разпорежи на Google Spain или на Google да заличи или да скрие тези лични данни, така че те да не се появяват повече в резултатите от търсенето и да не се съдържат във връзките към La Vanguardia.

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

В това решение Съдът се произнася и по териториалния обхват на Директива 95/46.

По този въпрос 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.

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.

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

Поради неколкостепенни 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 (Празки 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 запамятаване, 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.

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 личните 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. 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.

Решение от 16 януари 2024 г. (голям състав), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

За да провери дали е налице евентуално политическо влияние върху Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Федерална служба за защита на конституцията и борба с тероризма, Австрия)³⁰, Nationalrat (Национален съвет, Австрия) създава анкетна комисия (наричана по-нататък „анкетната комисия за BVT“). Тази анкетна комисия изслушва WK като свидетел. Въпреки искането за анонимизиране, направено от WK, протоколът от изслушването му, в който е цитирано пълното му лично и фамилно име, е публикуван на интернет страницата на Parlament Österreich (австрийския парламент). С твърдението, че такова разкриване на самоличността му противоречи на ОРЗД и на австрийското законодателство, WK подава жалба до Österreichische Datenschutzbehörde (Орган за защита на данните, Австрия) (наричан по-нататък „Datenschutzbehörde“). С решение от 18 септември 2019 г. Datenschutzbehörde приема, че няма компетентност да се произнесе по жалбата, като посочва, че принципът на разделение на властите изключва възможността като орган на изпълнителната власт той да контролира анкетната комисия за BVT, която е част от законодателната власт.

След като с решение Bundesverwaltungsgericht (Федерален административен съд, Австрия) уважава жалбата на WK и отменя решението на Datenschutzbehörde, Datenschutzbehörde подава ревизионна жалба до Върховния административен съд срещу решението на федералния административен съд.

³⁰ На 1 декември 2021 г. тя става „Direktion Staatsschutz und Nachrichtendienst“ (Дирекция „Защита на държавата и разузнавателни служби“, Австрия).

При тези обстоятелства запитващата юрисдикция иска от Съда да се произнесе дали дейностите на анкетна комисия, създадена от парламента на държава членка, попадат в приложното поле на ОРЗД и дали този регламент е приложим, когато тези дейности са свързани със защитата на националната сигурност.

На първо място, Съдът припомня, че член 2, параграф 2, буква а) от ОРЗД, съгласно който този регламент не се прилага за обработването на лични данни в хода на дейности, които са извън приложното поле на правото на Съюза, цели единствено да изключи от приложното му поле обработването на лични данни, извършвано от държавните органи в рамките на дейност, която е насочена към запазване на националната сигурност или която е от същата категория. Ето защо сам по себе си фактът, че дадена дейност е присъща на държавата или на публичен орган, не е достатъчен, за да се изключи автоматично прилагането на ОРЗД към подобна дейност.

Изложеното тълкуване, което следва от липсата на разграничение съобразно това кой извършва съответното обработване, се потвърждава от член 4, точка 7 от ОРЗД³¹.

Съдът уточнява, че парламентарното естество на анкетната комисия за BVT не означава, че дейностите ѝ са изключени от приложното поле на ОРЗД. Всъщност изключването, предвидено в член 2, параграф 2, буква а) от този регламент, се отнася само до категории дейности, които поради естеството си не попадат в приложното поле на правото на Съюза, а не до категории лица. Ето защо обстоятелството, че обработването на лични данни се извършва от анкетна комисия, създадена от парламента на държава членка при упражняване на правомощието му на контрол върху законодателната власт, само по себе си не дава основание да се направи извод, че това обработване се извършва в рамките на дейност, която е извън приложното поле на правото на Съюза.

На второ място, Съдът отбелязва, че макар държавите членки да са тези, които определят основните интереси на своята сигурност и предприемат подходящи мерки, за да я гарантират³², сам по себе си фактът, че дадена национална мярка е приета за целите на защитата на националната сигурност, не може да доведе до неприложимост на правото на Съюза и до освобождаване на държавите членки от необходимостта да спазват това право. Всъщност изключването, предвидено в член 2, параграф 2, буква а) от ОРЗД, се отнася само до категории дейности, които поради естеството си не попадат в приложното поле на правото на Съюза. В тази насока фактът, че администраторът е публичен орган, чиято основна дейност е да се гарантира националната сигурност, сам по себе си не е достатъчен, за да

³¹ Тази разпоредба дефинира понятието „администратор“ като „физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни“.

³² В съответствие с член 4, параграф 2 ДЕС.

изключи от приложното поле на ОРЗД обработването на лични данни, извършено от този орган в рамките на останалите му дейности.

В случая политическият контрол, осъществяван от анкетната комисия за BVT, сам по себе си, изглежда, не представлява дейност, която е насочена към запазване на националната сигурност или която е от същата категория. Ето защо, без да се засяга проверката, която трябва да се направи от запитващата юрисдикция, тази дейност не попада извън приложното поле на ОРЗД.

Парламентарна анкетна комисия обаче може да има достъп до лични данни, които по съображения за национална сигурност трябва да се ползват от особена защита. В тази насока чрез законодателна мярка могат да се ограничат задълженията и правата, произтичащи от ОРЗД, по-специално с цел да се гарантира националната сигурност³³. Така на тази база могат да бъдат обосновани ограничения за събирането на лични данни, предоставянето на информация на субектите на данни и достъпа им до тези данни или пък разкриването на посочените данни, без съгласието на субектите на данни, на различни от администратора лица, стига подобни ограничения да са съобразени със същността на основните права и свободи и да представляват необходима и пропорционална мярка в едно демократично общество.

Според Съда обаче от предоставената му информация не е видно анкетната комисия за BVT да е твърдяла, че разкриването на личните данни на субекта на данни е необходимо за опазването на националната сигурност и се основава на предвидена за тази цел национална законодателна мярка, като това, според случая, трябва да бъде проверено от запитващата юрисдикция.

2. Понятие за лични данни

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

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

³³ Съгласно член 23 от ОРЗД.

статичните IP адреси, динамичните IP адреси по принцип не позволяват да се направи връзка посредством общодостъпни файлове между даден компютър и физическото включване към мрежата, използвано от доставчика на интернет услуги. Сами по себе си записаните данни не позволяват на доставчика на онлайн медийни услуги да идентифицира ползвателя. За сметка на това доставчикът на интернет услуги разполага с допълнителна информация, която, ако бъде комбинирана с този IP адрес, би позволила да бъде идентифициран ползвателят.

В този контекст Bundesgerichtshof (Федерален върховен съд, Германия), сезиран с ревизионна жалба по делото, отправя запитване до Съда дали IP адресът, 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. Фактът, че допълнителната информация, необходима за идентифицирането на ползвател на интернет сайт, се притежава не от доставчика на онлайн медийни услуги, а от доставчика на интернет услуги на този ползвател, не изглежда да е от естество да изключи възможността динамичните IP адреси, запазени от доставчик на онлайн медийни услуги, да представляват за него лични данни по смисъла на член 2, буква а) от Директива 95/46.

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.

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“.

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

На четвърто място, Съдът постановява, че е възможно писмените отговори, дадени от кандидат по време на изпит за професионални умения, и евентуалните коментари на проверителя по тях да бъдат подложени на проверка — по-специално, що се отнася до тяхната точност и до необходимостта от съхраняването им по смисъла на член 6, параграф 1, букви г) и д) от Директива 95/46 — и да бъдат поправени или изтрети на основание член 12, буква б) от същата директива. Предоставянето на кандидат на право на достъп до тези отговори и коментари по силата на член 12, буква а) от същата директива служи на целта на последната, а именно да гарантира защитата на правото на кандидата на личен живот при обработването на засягащите го данни, при това независимо дали въпросният кандидат разполага с такова право на достъп и по силата на националната правна уредба, приложима към изпитната процедура. Съдът обаче подчертава, че правата на достъп и на поправяне по член 12, букви а) и б) от Директива 95/46 не обхващат изпитните въпроси, които сами по себе си не представляват лични данни на кандидата.

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

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. 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.

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

Това решение (вж. също раздел II.1., „Обхват на общата уредба“) 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 индексирание, 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. 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.

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

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 на изцяло лични или домашни занимания по смисъла на член 3, параграф 2, второ тире от същата директива.

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 пътищата³⁴ 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“³⁵, за което ОРЗД предвижда засилена защита поради особената чувствителност на съответните данни.

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

³⁴ Член 14¹, параграф 2 от Ceļu satiksmes likums (Закон за движението по пътищата) от 1 октомври 1997 г. (Latvijas Vēstnesis, 1997 г., бр. 274/276).

³⁵ Член 10 от ОРЗД.

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.

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 Съюза³⁶. 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.

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 сфера³⁷. Всъщност Съдът приема, че в рамките на посоченото съобщаване CSDD не може да се счита за такъв „компетентен орган“³⁸.

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“³⁹, 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 припомним трите релевантни критерия за преценка на наказателноправния характер на дадено нарушение, а именно правната квалификация на нарушението във вътрешното право, естеството на нарушението

³⁶ Член 2, параграф 2, буква а) от ОРЗД.

³⁷ Член 2, параграф 2, буква г) от ОРЗД.

³⁸ 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).

³⁹ Член 10 от ОРЗД.

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 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.

Решение от 5 декември 2023 г. (голям състав), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

През 2020 г. литовските органи решават да организират придобиване на мобилно информационно приложение за подобряване на управлението на пандемията от COVID-19. С това приложение те искат да се подпомогне епидемиологичното наблюдение чрез записване и наблюдение на данни на лица, изложени на вируса COVID-19.

За тази цел Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Национален център по общественото здраве към Министерство на здравеопазването, Литва, наричан по-нататък „НЦОЗ“), на който е възложено да придобие такова мобилно приложение, се обръща за разработването му към дружеството UAB „IT sprendimai sėkmei“ (наричано по-нататък „дружеството ITSS“). Впоследствие служители на НЦОЗ изпращат до това дружество електронни писма във връзка с формулирането на въпросите в мобилното приложение.

В периода от април до май 2020 г. е предоставен публичен достъп до разработеното от дружеството ITSS мобилно приложение. То е използвано от 3 802 души, които са въвели в него свои данни. Поради липса на финансиране обаче НЦОЗ не възлага на дружеството ITSS обществена поръчка, за да придобие официално мобилното приложение, и прекратява отнасящата се до него процедура.

Същевременно националният надзорен орган започва проверка относно обработването на личните данни, събрани при използването на приложението. Въз основа на проверката този орган приема решение за налагане на

административно наказание „имуществена санкция“ на НЦОЗ и на дружеството ITSS, което счита за съвместен администратор.

НЦОЗ оспорва решението пред Vilniaus apygardos administracinis teismas (Окръжен административен съд Вилнюс, Литва). Този съд не е сигурен как следва да тълкува някои от разпоредбите на ОРЗД, и отправя преюдициално запитване до Съда.

В решението си Съдът, заседаващ в голям състав, разяснява в частност понятието „обработване“. В това отношение той посочва, че използването на лични данни за изпитване на мобилно информационно приложение представлява обработване по смисъла на ОРЗД. Това обаче не е така, ако данните са анонимизирани по такъв начин, че субектът на данните не може или вече не може да бъде идентифициран, или ако данните са фиктивни и не се отнасят за съществуващо физическо лице.

Всъщност, от една страна, въпросът дали личните данни се използват за изпитване на информационно приложение, или за друга цел, е без значение за квалифицирането на разглежданата операция като „обработване“. От друга страна, само обработването на лични данни може да се квалифицира като „обработване“ по смисъла на ОРЗД. Фиктивните или анонимните данни не представляват лични данни.

4. Понятие за файл с лични данни

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

В това решение (вж. също раздел 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 обхваната от това понятие, не е необходимо тя да включва картотеки, специфични списъци или други подобни класификационни системи.

5. Понятие за администратор на лични данни

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

По това дело (вж. също раздел II.3, „Понятие за обработване на лични данни“, и раздел 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.

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

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).

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 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).

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.

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 операцияите 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.

Решение от 5 декември 2023 г. (голям състав), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

По това дело (вж. също раздел II.3, „Понятие за обработване на лични данни“) Съдът отбелязва, че субект, който е възложил на предприятие да разработи мобилно информационно приложение и в този контекст е участвал в определянето на целите и средствата за извършването посредством това приложение обработване на лични данни, може да се счита за администратор⁴⁰. Това е така независимо от факта, че самият субект не е извършвал операции по обработване на лични данни, не е давал изрично съгласие за извършването на конкретни такива операции или за предоставянето на публичен достъп до мобилното приложение и не е придобивал приложението, освен ако преди предоставянето на публичния достъп до приложението изрично не се е противопоставил както на това предоставяне, така и на последвалото го обработване на лични данни.

6. Понятие за съвместен администратор

Решение от 5 декември 2023 г. (голям състав), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

По това дело (вж. също раздел II.3, „Понятие за обработване на лични данни“, и раздел I Österreichische Datenschutzbehörde I.5, „Понятие за администратор на лични данни“) Съдът отбелязва, че за квалифицирането на два субекта като съвместни администратори не се изисква те да имат нито споразумение, което да определя целите и средствата на обработването на лични данни, нито споразумение, което да урежда условията за съвместната им отговорност за това обработване. Вярно е наистина, че съгласно ОРЗД⁴¹ съвместните администратори трябва чрез споразумение помежду си да определят по прозрачен начин съответните си задължения, за да гарантират спазването на изискванията на този регламент. Наличието на такова споразумение обаче не е предварително условие

⁴⁰ По смисъла на член 4, точка 7 от ОРЗД.

⁴¹ Член 26, параграф 1 във връзка със съображение 79 от ОРЗД.

за квалифицирането на два или повече субекта като съвместни администратори, а е задължение, което ОРЗД налага на съвместните администратори, след като бъдат квалифицирани като такива, за да се гарантира спазването на наложените им с този регламент изисквания. Квалифицирането се основава следователно само на факта, че при определянето на целите и средствата на обработването на данните са участвали няколко субекта.

По отношение на съвместното определяне от съответните субекти на целите и средствата за обработването Съдът уточнява, че участието в това определяне може да бъде в различни форми, като например може да е резултат от съвместно решение или от съвпадащи решения на два или повече субекта. В последния случай решенията би трябвало все пак да са взаимно допълващи се и да са необходими за извършването на обработването по такъв начин, че всяко от тях да има осезаемо въздействие върху определянето на целите и средствата за обработването.

7. Условия за законосъобразност на обработването на лични данни

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

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 заплахата 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.

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.

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.

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.

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

В това решение (вж. също раздел 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.

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.

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

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.

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.

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 Съюза⁴² 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, информирано и недвусмислено⁴³. В това отношение съгласието не е валидно дадено в случаите на мълчание, предварително отметнати полета или липса на действие.

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.

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

⁴² Член 7 от Директива 95/46 и член 6 от ОРЗД.

⁴³ Член 2, буква з) от Директива 95/46 и член 4, параграф 11 от ОРЗД.

естество да докаже изразено с потвърждаващо действие съгласие. Националната юрисдикция следва да направи необходимите в това отношение проверки.

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.

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 отменено 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.

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.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 обществеността на достъп до официални документи, нито правото на свобода на информацията обосновават подобна правна уредба.

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“⁴⁴. 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.

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.

Освен това по същите причини Съдът приема, 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.

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.

⁴⁴ 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 [...]“.

III. Обработване на лични данни по смисъла на секторната уредба

1. Обработване на лични данни в сектора на електронните съобщения

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

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]“.

В този контекст Съдът пояснява, че наистина в решение *Tele2 Sverige и Watson и др.*⁴⁵ 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]“.

Що се отнася до конкретния случай, Съдът приема, че достъпът само до данните, посочени в разглежданото 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“.

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](#))

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 загрижеността 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) (*La 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

⁴⁵ 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](#)).

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.

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.

По-нататък Съдът припомня, че Директива 2002/58⁴⁶ 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 трафика⁴⁷, но само при спазване на общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и на гарантираните с Хартата основни права⁴⁸.

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

⁴⁶ Член 15, параграфи 1 и 3 от Директива 2002/58.

⁴⁷ Член 5, параграф 1 от Директива 2002/58.

⁴⁸ По-конкретно членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

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.

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, допуска да се разпорежи 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.

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.

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.

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.

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 Съюза⁴⁹ 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 орган по смисъла на решение Tele2 Sverige и Watson и др.⁵⁰, 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 във връзка с 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.

Що се отнася до целта за предотвратяване, разследване, разкриване и преследване на престъпления, преследвана от разглежданата в главното производство 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

⁴⁹ 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.

⁵⁰ 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).

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.

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.

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.

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.

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.

Решение от 5 април 2022 г. (голям състав), *Commissioner of An Garda Síochána* и др. (C-140/20, [EU:C:2022:258](#))

Преюдициалното запитване по настоящото дело е отправено от Supreme Court (Върховен съд, Ирландия) в рамките на гражданско производство, образувано по инициатива на лице, осъдено на доживотен затвор за убийство, извършено в Ирландия. Въпросното лице оспорва съвместимостта с правото на Съюза на някои разпоредби от националния закон относно запазването на данните, създадени във връзка с електронни съобщения. В съответствие с този закон свързани с телефония данни за трафик и данни за местонахождение на въпросното лице са били запазени от доставчиците на електронни съобщителни услуги, като е бил предоставен достъп до тях на полицейските служби. Изразените от запитващата юрисдикция съмнения се отнасят по-специално до съвместимостта с Директива 2002/58, разглеждана във връзка с Хартата, на режим на общо и неизбирателно запазване на тези данни във връзка с борбата с тежката престъпност.

В решението си, постановено от голям състав, Съдът потвърждава, уточнявайки обхвата ѝ, съдебната практика, установена с решение *La Quadrature du Net* и др.⁵¹, като припомня, че общото и неизбирателно запазване на свързаните с електронните съобщения данни за трафик и данни за местонахождение не е разрешено за целите на борбата с тежката престъпност и предотвратяването на

⁵¹ Решение от 6 октомври 2020 г., *La Quadrature du Net* и др. (C-511/18, C-512/18, C-520/18, [EU:C:2020:791](#)).

сериозни заплахи за обществената сигурност. Той потвърждава и по отношение на полицейски служител съдебната практика, установена с решение *Prokuratuur* (Условия за достъп до данните за електронните съобщения)⁵², по-специално що се отнася до задължението достъпът на компетентните национални органи до посочените запазени данни да се постави в зависимост от предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура.

Съдът приема, на първо място, че Директива 2002/58 във връзка с Хартата не допуска законодателни мерки, предвиждащи общо и неизбирателно запазване на данни за трафик и данни за местонахождение като превантивна мярка за целите на борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност. Всъщност, като се имат предвид, от една страна, възпиращото въздействие върху упражняването на основните права⁵³, което може да има това запазване, и от друга страна, сериозността на намеренията, до която то води, такова запазване трябва да бъде изключение, а не правило в установената с тази директива система, така че тези данни да не могат да бъдат предмет на системно и продължително запазване. Престъпността, дори особено тежка, не може да се приравни на заплаха за националната сигурност, доколкото подобно приравняване би могло да въведе междинна категория между националната сигурност и обществената сигурност, така че към обществената сигурност да се приложат изискванията, които са свързани с националната сигурност.

За сметка на това Директива 2002/58 във връзка с Хартата допуска законодателни мерки, предвиждащи за целите на борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност целево запазване на данни за трафик и на данни за местонахождение, което е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите засегнати лица или посредством географски критерий, за ограничен до строго необходимото период от време, който може да бъде удължен. Съдът добавя, че такава мярка за запазване, насочена към места или инфраструктури, редовно посещавани от много голям брой хора, или към стратегически места като летища, гари, морски пристанища или зони за събиране на пътни такси, би могла да позволи на компетентните органи да получат информацията относно присъствието на тези места или в тези географски зони на лицата, използващи там електронно съобщително средство, и да направят изводи — за целите на борбата с тежката престъпност — относно присъствието им и дейността им на тези места или в тези географски зони. Във всеки случай евентуалното наличие на трудности точно да се определят случаите и условията, при които следва да се извършва целево запазване, не оправдава държавите членки да предвиждат общо и неизбирателно запазване на данните за трафик и на данните за местонахождение.

⁵² Решение от 2 март 2021 г., *Prokuratuur* (Условия за достъп до данните за електронните съобщения) (C-746/18, [EU:C:2021:152](#)).

⁵³ Закрепени в членове 7—11 от Хартата.

Посочената директива, разглеждана във връзка с Хартата, допуска и законодателни мерки, които за същите цели предвиждат общо и неизбирателно запазване на IP адреси, дадени на източника на свързване с интернет, за ограничен до строго необходимото период от време, както и на данни относно самоличността на ползвателите на електронни съобщителни средства. Що се отнася до последния аспект, Съдът по-специално уточнява, че нито Директива 2002/58, нито друг акт от правото на Съюза са пречка за приемането на национална правна уредба, която се отнася до борбата с тежката престъпност и по силата на която придобиването на електронно съобщително средство (като предплатена SIM карта) зависи от проверката на официални документи, удостоверяващи самоличността на купувача, и от регистрацията от продавача на получената по този начин информация, като продавачът е длъжен при необходимост да даде достъп до тази информация на компетентните национални органи.

Не е различно положението и по отношение на законодателните мерки, които също за целите на борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност предвиждат да се разпорежи на доставчиците на електронни съобщителни услуги посредством решение на компетентния орган, подлежащо на ефективен съдебен контрол, да извършват за определен период бързо запазване („quick freeze“) на данните за трафик и на данните за местонахождение, с които разполагат тези доставчици на услуги. Всъщност такова запазване може да бъде обосновано единствено с борбата с тежката престъпност и *a fortiori* с опазването на националната сигурност, стига при тази мярка и при достъпа до така запазените данни да се спазват границите на строго необходимото. Съдът припомня, че подобна мярка за бързо запазване може да бъде приложена и за данните за трафик и данните за местонахождение, свързани с лица, различни от тези, за които има подозрения, че са подготвили или извършили тежко престъпление или посегателство срещу националната сигурност, ако тези данни въз основа на обективни и недискриминационни критерии могат да допринесат за разкриването на такова престъпление или посегателство срещу националната сигурност, като например данните на пострадалото от него лице, както и данните на неговото социално или професионално обкръжение.

След това обаче Съдът посочва, че всички горепосочени законодателни мерки трябва да гарантират с ясни и точни правила, че запазването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби. Различните мерки за запазване на данни за трафик и на данни за местонахождение могат да се приложат съвместно според избора на националния законодател и при спазване на границите на строго необходимото.

Освен това Съдът уточнява, че предоставянето на достъп за целите на борбата с тежката престъпност до такива данни, които са били запазени общо и неизбирателно за целите на справянето със сериозна заплаха за националната сигурност, би засегнало йерархията на целите от общ интерес, които могат да обосноват мярка, приета въз основа на Директива 2002/58. Всъщност това би позволило достъпът да може да се обоснове от цел с по-малко значение от целта, обосновала запазването, а именно опазването на националната сигурност, като така би могла да се лиши от всякакво полезно действие забраната за общо и неизбирателно запазване за целите на борбата с тежката престъпност.

На второ място, Съдът постановява, че Директива 2002/58, разглеждана във връзка с Хартата, не допуска национална правна уредба, по силата на която централизираното обработване на исканията за достъп до запазени от доставчиците на електронни съобщителни услуги данни, отправени от полицията при разследването и преследването на тежки престъпления, се извършва от полицейски служител, дори последният да е подпомаган от звено в рамките на полицията, което се ползва с определена самостоятелност при упражняването на функциите си и чиито решения подлежат на последващ съдебен контрол. Всъщност, от една страна, такъв служител не отговаря на изискванията за независимост и безпристрастност, които съществуват за административен орган, осъществяващ предварителен контрол спрямо отправените от компетентните национални органи искания за достъп до данни, доколкото той няма качеството на трето лице по отношение на тези органи. От друга страна, макар решението на такъв служител да подлежи на последващ съдебен контрол, този контрол не може да замести независим контрол, който, освен в надлежно обосновани спешни случаи, е предварителен.

На трето и последно място, Съдът потвърждава практиката си, съгласно която правото на Съюза не допуска национална юрисдикция да ограничи действието във времето на възложено ѝ по силата на националното право обявяване на невалидност на национална правна уредба, която налага на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данни за трафик и на данни за местонахождение, поради несъвместимостта на тази правна уредба с Директива 2002/58. При това положение Съдът припомня, че в съответствие с принципа на процесуална автономия на държавите членки допустимостта на доказателствата, получени чрез такова запазване, зависи от националното право, стига да са спазени по-специално принципите на равностойност и ефективност.

Решение от 20 септември 2022 г. (голям състав), VD и SR (C-339/20 и C-397/20, [EU:C:2022:703](#))

След разследване на Autorité des marchés financiers (Надзорен орган за финансовите пазари, Франция, наричан по-нататък „AMF“) са образувани

наказателни производства срещу VD и SR, две физически лица, обвинени в злоупотреба с вътрешна информация, укривателство във връзка със злоупотреба с вътрешна информация, съучастие в престъпление, корупция и изпиране на пари. В рамките на това разследване AMF е използвал лични данни от телефонни обаждания на VD и SR, които данни са генерирани въз основа на френския Code des postes et des communications électroniques (Кодекс за пощите и електронните съобщения) при предоставянето на електронни съобщителни услуги.

Доколкото привличането като обвиняем на всеки от тях се основава на данните за трафик, предоставени от AMF, VD и SR поотделно сезират Cour d'appel de Paris (Апелативен съд Париж, Франция) с жалба, като изтъкват по-специално основание, изведено от нарушение на член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11, както и на член 52, параграф 1 от Хартата. По-специално, като се позовават на съдебната практика, установена с решение Tele2 Sverige и Watson и др.⁵⁴, VD и SR оспорват факта, че за да пристъпи към събиране на посочените данни, AMF се е основал на разглежданите национални разпоредби, при положение че, според тях, тези разпоредби, от една страна, не са в съответствие с правото на Съюза, доколкото предвиждат общо и неизбирателно запазване на данните за свързване, и от друга страна, не определят никакви ограничения на правомощията на разследващите служители на AMF да изискват запазените данни.

С две решения от 20 декември 2018 г. и 7 март 2019 г. Cour d'appel de Paris (Апелативен съд, Париж) отхвърля жалбите на VD и SR. За да отхвърли посоченото по-горе основание съдът, разглеждащ делото по същество, се позовава по-специално на факта, че Регламентът относно пазарната злоупотреба⁵⁵ допуска компетентните органи да изискват, до степента, позволена от националното законодателство, съществуващите записи на данни за трафик, съхранявани от операторите на електронни съобщителни услуги, когато има основания да се подозира нарушение на забраната за злоупотреба с вътрешна информация и когато тези записи могат да се окажат от значение за разследването на това нарушение.

Тогава VD и SR подават жалба пред Cour de cassation (Касационен съд, Франция) — запитващата юрисдикция по настоящите дела.

В този контекст запитващата юрисдикция иска да се установи дали член 15, параграф 1 от Директива 2002/58, разглеждан с светлината на Хартата, може да бъде съгласуван с изискванията, произтичащи от член 12, параграф 2, букви а) и г)

⁵⁴ Решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, [EU:C:2016:970](#)).

⁵⁵ Регламент (ЕС) № 596/2014 на Европейския парламент и на Съвета от 16 април 2014 година относно пазарната злоупотреба (Регламент относно пазарната злоупотреба) и за отмяна на Директива 2003/6 и директиви 2003/124/ЕО, 2003/125/ЕО и 2004/72/ЕО на Комисията (ОВ L 173, 2014 г., стр. 1).

от Директивата за пазарната злоупотреба⁵⁶ и от член 23, параграф 2, букви ж) и з) от Регламента относно пазарната злоупотреба. Този въпрос е породен от разглежданите в главното производство законодателни мерки, които предвиждат превантивно общо и неизбирателно запазване на данните за трафик от операторите на електронни съобщителни услуги в продължение на една година, считано от деня на записването, за целите на борбата с престъпленията, свързани с пазарната злоупотреба, сред които е злоупотребата с вътрешна информация. В случай че Съдът приеме, че законодателството относно разглежданото в главните производства запазване на данни за свързване не е в съответствие с правото на Съюза, се поставя въпросът за временното запазване на действието на това законодателство, за да се избегне правна несигурност и да се позволи събраните и запазени преди това данни да бъдат използвани за целите на разкриването и преследването на злоупотребата с вътрешна информация.

В решението си Съдът, заседаващ в голям състав, приема, че общото и неизбирателно запазване на данни за трафик в продължение на една година, считано от деня на записването, от операторите на електронни съобщителни услуги, не е разрешено превантивно за целите на борбата с престъпленията, свързани с пазарната злоупотреба. Освен това Съдът потвърждава своята практика, съгласно която правото на Съюза не допуска национална юрисдикция да ограничава във времето действието на възложено ѝ по силата на националното право обявяване на невалидност на национални разпоредби, несъвместими с правото на Съюза.

Съдът припомня най-напред, че за да се тълкува разпоредба от правото на Съюза, трябва не само да се вземе предвид нейният текст, но и контекстът ѝ, както и целите, преследвани от правната уредба, от която тя е част.

Що се отнася до текста на разпоредбите, посочени в преюдициалните въпроси, Съдът приема за установено, че докато член 12, параграф 2, буква г) от Директивата „относно пазарната злоупотреба“ се позовава на правомощието на AMF „да изисква съществуващи записи на телефонните разговори и на разменените сведения“, член 23, параграф 2, букви ж) и з) от Регламент относно пазарната злоупотреба препраща към правомощието на този орган да изисква, от една страна, „записи[те] [...] за пренос на данни, съхранявани от инвестиционни посредници, кредитни институции или финансови институции“, и от друга страна, „доколкото е позволено от националното право, съществуващи записи на пренос на данни, съхранявани от далекосъобщителен оператор“. Според Съда от текста на тези разпоредби недвусмислено следва, че те само осигуряват рамка за правомощието на AMF да „изисква“ данните, с които разполагат тези оператори,

⁵⁶ Директива 2003/6/ЕО на Европейския парламент и на Съвета от 28 януари 2003 година относно търговията с вътрешна информация и манипулирането на пазара (пазарна злоупотреба) (ОВ L 96, 2003 г., стр. 16; Специално издание на български език, 2007 г., глава 6, том 5, стр. 210)

което съответства на достъп до тези данни. Освен това позоваването на „съществуващите“ записи, „съхранявани“ от посочените оператори, навежда на мисълта, че законодателят на Съюза не е имал намерение да уреди възможността за националния законодател да въвежда задължение за запазване на такива записи. Според Съда това тълкуване освен това се потвърждава както от контекста, в който се вписват посочените разпоредби, така и от целите, преследвани от правната уредба, от която са част същите тези разпоредби.

Що се отнася до контекста, в който се вписват посочените в преюдициалните въпроси разпоредби, Съдът отбелязва, че макар съгласно релевантните разпоредби от Директивата за пазарната злоупотреба⁵⁷ и Регламента относно пазарната злоупотреба, законодателят на Съюза да е възнамерявал да наложи на държавите членки приемането на необходимите мерки, така че компетентните финансови органи да разполагат с набор от подходящи инструменти, правомощия и ресурси, както и с надзорни и разследващи правомощия, необходими за осигуряване на ефикасността на изпълнението на техните задачи, тези разпоредби не казват нищо нито относно евентуалната възможност държавите членки да въвеждат за тази цел в тежест на операторите на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данните за трафик, нито относно условията, при които посочените данни трябва да бъдат запазвани от тези оператори с цел евентуалното им предаване на компетентните органи.

Що се отнася до целите, преследвани от разглежданата правна уредба, Съдът отбелязва, че както от Директивата за пазарната злоупотреба⁵⁸, така и от Регламента относно пазарната злоупотреба следва, че целта на тези инструменти е да се гарантира целостта на финансовите пазари на Съюза и да се укрепи доверието на инвеститорите в тези пазари — доверие, което почива по-специално на факта, че те ще бъдат равнопоставени и защитени срещу незаконно използване на вътрешна информация. Така забраната на търговията с вътрешна информация, установена в посочените актове⁵⁹, има за цел да гарантира равенството на съдоговорителите по дадена борсова сделка, като се избегне възможността един от тях, който разполага с вътрешна информация и поради това е в по-благоприятно положение спрямо другите инвеститори, да извлече облага в ущърб на тези, които не са запознати с нея. Макар съгласно Регламента относно пазарната злоупотреба⁶⁰ записите на данни за свързване да представляват важно, и понякога единствено, доказателство за разкриване и доказване на злоупотреба с вътрешна информация или манипулиране на пазара, този регламент все пак се

⁵⁷ Съответно член 12, параграф 1 от Директивата за пазарната злоупотреба и член 23, параграф 3 във връзка със съображение 62 от Регламента за пазарната злоупотреба.

⁵⁸ Съответно съображения 2 и 12 от Директивата за пазарната злоупотреба и член 1 във връзка със съображения 2 и 24 от Регламента за пазарната злоупотреба.

⁵⁹ Член 2, параграф 1 от Директивата за пазарната злоупотреба и член 8, параграф 1 от Регламента за пазарната злоупотреба.

⁶⁰ Съображение 62 от Регламента за пазарната злоупотреба.

отнася само до записи, „съхранявани“ от операторите на електронни съобщителни услуги, както и до правомощията на компетентния финансов орган да „изисква“ от тези оператори „съществуващите“ данни. Ето защо от посочения текст по никакъв начин не следва, че така законодателят на Съюза е искал да признае на държавите членки правомощието да налагат на операторите на електронни съобщителни услуги общо задължение за запазване на данни. Оттук следва, че нито Директивата „относно пазарната злоупотреба“, нито Регламентът относно пазарната злоупотреба могат да представляват правното основание за общо задължение за запазване на записи на данни за трафик, съхранявани от операторите на електронни съобщителни услуги, за целите на упражняването на правомощията, предоставени на компетентния финансов орган съгласно тази актове.

На следващо място Съдът припомня, че Директива 2002/58 представлява референтният акт в областта на запазването и по-общо на обработването на лични данни в сектора на електронните комуникации, така че тълкуването ѝ, както е направено с оглед на тази директива, урежда и записите на данни за трафик, съхранявани от операторите на електронни съобщителни услуги, които компетентните финансови органи по смисъла на Директивата за пазарната злоупотреба и Регламента относно пазарната злоупотреба⁶¹ могат да изискат от тези оператори. Ето защо преценката на законосъобразността на обработването на записите, съхранявани от операторите на електронни съобщителни услуги⁶², трябва да се извършва с оглед на условията, предвидени в Директива 2002/58, както и на тълкуването на тази директива в практиката на Съда.

Така Съдът постановява, че Директивата за пазарната злоупотреба и Регламентът относно пазарната злоупотреба, разглеждани във връзка с Директива 2002/58 и в светлината на Хартата, не допускат законодателни мерки, които предвиждат — превантивно за целите на борбата с престъпленията, свързани с пазарната злоупотреба, част от които е злоупотребата с вътрешна информация — временно, т.е. в продължение на една година, считано от деня на записването, но общо и неизбирателно запазване на данните за трафик от операторите на електронни съобщителни услуги.

На последно място, Съдът потвърждава практиката си, съгласно която правото на Съюза трябва да се тълкува в смисъл, че не допуска национална юрисдикция да ограничава във времето действието на възложено ѝ по силата на националното право обявяване на невалидност на национални разпоредби — които, от една страна, налагат на операторите на електронни съобщителни услуги общо и неизбирателно запазване на данните за трафик, и от друга страна, позволяват

⁶¹ Съответно член 11 от Директивата за пазарната злоупотреба и член 22 от Регламента за пазарната злоупотреба.

⁶² По смисъла на член 12, параграф 2, буква г) от Директивата за пазарната злоупотреба и член 23, параграф 2, букви ж) и з) от Регламента за пазарната злоупотреба.

предоставянето на такива данни на компетентния финансов орган без предварителното разрешение на съд или независим административен орган — поради това, че тези разпоредби са несъвместими с Директива 2002/58, разглеждана в светлината на Хартата. При това положение Съдът припомня, че в съответствие с принципа на процесуална автономия на държавите членки допустимостта на доказателствата, получени чрез такова запазване, зависи от националното право, стига да са спазени по-специално принципите на равностойност и ефективност. Последният принцип изисква от националния наказателен съд да не взема предвид данни и доказателства, получени чрез несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик, ако засегнатите лица не са в състояние да обсъдят ефективно тези данни и доказателства от област, в която са необходими специални познания, каквито съдът няма, и които данни и доказателства могат да повлияят съществено на преценката на фактите и обстоятелствата.

Решение от 30 април 2024 г. (пленум), La Quadrature du Net и др. (Лични данни и борба с нарушенията на права върху интелектуална собственост) (C-470/21, [EU:C:2024:370](#))

Сезиран с преюдициално запитване от Conseil d'État (Държавен съвет, Франция), пленумът на Съда доразвива съдебната практика по Директива 2002/58, като дава разяснения, от една страна, за условията, при които всеобщото съхраняване на IP адреси от доставчиците на електронни съобщителни услуги може да не се смята за тежка намеса по отношение на правото на неприкосновеност на личния живот, правото на защита на личните данни и свободата на изразяване на мнение, всичките гарантирани от Хартата⁶³, а от друга страна, за възможността публичните органи да получават достъп до определени лични данни, съхранени при спазване на посочените условия, в рамките на борбата срещу извършваните в интернет нарушения на правата на интелектуална собственост.

В разглеждания случай четири сдружения отправят искане до Premier ministre (министър-председател, Франция) да отмени декрета за автоматизираната обработка на лични данни⁶⁴. Искането им е оставено без внимание и тези сдружения подават жалба до Conseil d'État (Държавен съвет), като искат отмяна на

⁶³ Членове 7, 8 и 11 от Хартата.

⁶⁴ Décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet » (Декрет № 2010—236 от 5 март 2010 г. относно автоматизираната обработка на лични данни, разрешена съгласно член L. 331—29 от Кодекса на интелектуалната собственост, наречена „Система за управление на мерките за закрила на произведения в интернет“) (JORF, бр. 56 от 7 март 2010 г., текст № 19), изменен с Décret n° 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Декрет № 2017-924 от 6 май 2017 г. за управлението на авторските и сродните им права от организации за управление на права и за изменение на Кодекса на интелектуалната собственост) (JORF, бр. 109 от 10 май 2017 г., текст № 176).

мълчаливия отказ. Според тях декретът и разпоредбите, които са правното му основание⁶⁵, са в противоречие с правото на Съюза.

Съгласно френското законодателство, за да може да установява кои са отговорните лица за извършваните в интернет нарушения на авторското и сродните му права, Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Висш орган за разпространение на произведенията и защита на правата в интернет, наричан по-нататък „Hadopi“), има право да получава достъп до определени данни, които доставчиците на електронни съобщителни услуги са длъжни да съхраняват. Тези данни се отнасят до самоличността на съответните хора, съответстваща на техните IP адреси, събрани преди това от организациите на носителите на права. Щом бъде идентифициран притежателят на IP адреса, който е бил използван за извършването на дейности, съставляващи подобно нарушение, Hadopi предприема процедура, известна като „поетапни мерки“. По-конкретно, този орган е оправомощен да изпрати на съответното лице две препоръки, които приличат на предупреждения, а ако дейностите продължат — и писмо, с което му се съобщава, че подлежи на наказателно преследване за тези дейности. Накрая, органът може да сезира прокуратурата с цел образуване на наказателно производство срещу лицето⁶⁶.

В този контекст Conseil d'État (Държавен съвет) отправя запитване до Съда за тълкуването на Директива 2002/58 във връзка с Хартата⁶⁷.

На първо място, що се отнася до съхраняването на данните за самоличността и съответните IP адреси, Съдът подчертава, че не всяко общо и неизбирателно съхраняване на IP адреси е непременно тежка намеса по отношение на правото на неприкосновеност на личния живот, правото на защита на личните данни и свободата на изразяване на мнение, гарантирани с Хартата.

Задължението да се съхраняват тези данни, може да бъде обосновано с целта за борба срещу престъпленията въобще, когато е наистина изключено да може съхраняването им да доведе до тежки вмешателства в личния живот на съответното лице поради възможността да се направят точни изводи относно него, например чрез свързване на тези IP адреси със съвкупност от данни за трафика или местонахождението.

Затова държавата членка, която възнамерява да възложи такова задължение на доставчиците на електронни съобщителни услуги, трябва да се увери, че условията

⁶⁵ По-конкретно член L. 331-21, трета, четвърта и пета алинея от Code de la propriété intellectuelle (Кодекс на интелектуалната собственост).

⁶⁶ Считано от 1 януари 2022 г., Hadopi се слива с Conseil supérieur de l'audiovisuel (Висш съвет за аудио-визуални медии, CSA), друг независим публичен орган, за да създадат Autorité de régulation de la communication audiovisuelle et numérique (Орган за регулиране на аудио-визуалните и цифровите съобщения, ARCOM). Процедурата на поетапните мерки обаче остава по същество непроменена.

⁶⁷ Член 15, параграф 1 от Директива 2002/58.

и редът за съхраняване на данните изключват възможността да се направят точни изводи за личния живот на съответните лица.

Съдът пояснява, че за тази цел условията и редът за съхраняването на данните трябва да се отнасят до самата структура на съхраняването им, която по същество трябва да е организирана така, че да гарантира наистина непропускливо разделяне на различните категории съхранявани данни. В този смисъл националните правила за тези условия и ред трябва да гарантират, че всяка категория данни, включително за самоличността и IP адресите, ще се съхранява напълно отделно от останалите категории съхранявани данни и че разделянето им ще е наистина непропускливо, чрез сигурна и надеждна компютърна система. Нещо повече, доколкото предвиждат възможност за свързване на съхранените IP адреси със самоличността на съответното лице за целите на борбата с престъпността, тези правила трябва да позволяват тези данни да бъдат свързани единствено чрез използването на функционален технически способ, който не застрашава ефикасността на непропускливото разделяне на тези категории данни. Надеждността на отделянето им трябва да подлежи на редовен контрол от страна на друг публичен орган. При условие че приложимото национално законодателство предвижда такива стриктни изисквания, произтичащата от съхраняването на IP адресите намеса не може да се квалифицира като „тежка“.

Затова Съдът заключава, че когато е налице законодателен механизъм, който гарантира, че няма да е възможно чрез комбиниране на данни да се направят точни изводи за личния живот на лицата, чиито данни се съхраняват, Директива 2002/58 във връзка с Хартата допуска държавата членка да наложи задължение за общо и неизбирателно съхраняване на IP адресите за срок, който не надхвърля границите на строго необходимото, за целите на борбата с престъпленията въобще.

На второ място, що се отнася до достъпа до данните за самоличност, съответстващи на IP адреси, Съдът постановява, че Директива 2002/58 във връзка с Хартата по принцип допуска национална правна уредба, която разрешава достъпа на публичен орган до данните, които доставчиците на електронни съобщителни услуги съхраняват разделно и наистина непропускливо, с единствената цел този орган да може да идентифицира онези от притежателите на тези адреси, за които подозира, че са отговорни за нарушения на авторското и сродните му права в интернет, и да вземе мерки спрямо тях. В такъв случай националната правна уредба трябва да забранява на разполагащите с такъв достъп служители, първо, да разкриват под каквато и да е форма информация за съдържанието на файловете, отваряни от притежателите на тези адреси, освен за целите и само за целите на сезирането на прокуратурата, второ, да проследяват пътя им в сайтовете и страниците в интернет („clickstream“), и трето, да използват тези IP адреси за други цели освен за приемането на посочените мерки.

В този контекст Съдът в частност припомня, че наистина свободата на изразяване на мнение и поверителността на личните данни са от първостепенно значение, но тези основни права все пак не са абсолютни. Всъщност при претеглянето на съответните права и интереси те трябва понякога да отстъпят пред други основни права и съображения от общ интерес, като защитата на обществения ред и предотвратяването на престъпленията или защитата на правата и свободите на други лица. Така е например, когато отдаването на преимущество на посочените въпроси от първостепенно значение би могло да накърни ефективността на наказателното производство, например като осуети или прекомерно затрудни ефективното разкриване и наказване на извършителя на престъплението.

В същия контекст Съдът се позовава и на своята практика, че когато става дума за борбата с престъпленията, които засягат авторското или сродните му права в интернет, обстоятелството, че достъпът до IP адресите може да е единственият метод за разследване, позволяващ да се установи самоличността на съответното лице, сочи, че съхраняването на тези адреси и достъпът до тях са строго необходими за осъществяването на следваната цел и съответно отговарят на изискването за пропорционалност. Впрочем, ако не се разреши такъв достъп, това би създавало реален риск от системна безнаказаност за престъпленията, които се извършват в интернет или чието извършване или подготвяне е улеснено от характерните особености на интернет. Наличието на такъв риск обаче е релевантно обстоятелство за преценката — при претеглянето на съответните права и интереси — дали евентуалната намеса по отношение на правото на неприкосновеност на личния живот, правото на защита на личните данни и свободата на изразяване на мнение е пропорционална мярка спрямо целта за борба с престъпленията.

На трето място, Съдът се произнася по въпроса дали достъпът на публичния орган до данните за самоличност, съответстващи на даден IP адрес, трябва да е възможен само след предварителен контрол от съд или независим административен орган, и приема, че такова изискване за контрол е необходимо, когато в контекста на съответната национална правна уредба този достъп съдържа риск от тежка намеса по отношение на основните права на съответното лице, в смисъл че би могъл да позволи на този публичен орган да направи точни изводи за личния живот на това лице и евентуално да му изготви подробен профил. Обратно, не следва да се прилага такова изискване за предварителен контрол, когато намесата по отношение на основните права не може да се квалифицира като тежка.

В това отношение Съдът пояснява, че ако е въведен механизъм за съхранение, който гарантира наистина непропускливо разделяне на различните категории съхранявани данни, достъпът на публичния орган до данните за самоличност, съответстващи на IP адресите, по принцип не е обвързан с изискване за предварителен контрол. Всъщност наличието на такъв достъп само за целите на

идентифицирането на притежателя на даден IP адрес по общо правило не представлява тежка намеса по отношение на упоменатите права.

Съдът обаче не изключва да има и нетипични ситуации, в които при процедури като тази на поетапните мерки, за която става дума в главното производство, да има риск публичният орган да може да направи точни изводи за личния живот на съответното лице, в частност когато то извършва нарушаващи авторското или сродни права дейности в мрежи с равноправен достъп (peer-to-peer) повторно или даже в голям мащаб във връзка с конкретни видове защитени произведения, които разкриват евентуално чувствителна информация за личния му живот.

В разглеждания случай притежателят на даден IP адрес може да е особено изложен на такъв риск, когато публичният орган трябва да реши дали да сезира прокуратурата с оглед на образуването на наказателно производство. Всъщност интензивността на посегателството над правото на неприкосновеност на личния живот би могла постепенно да нараства с напредването през различните стадии на процедурата на поетапните мерки, която се осъществява на принципа на последователните действия. Достъпът на компетентния орган до съвкупността от данни, които се отнасят до съответното лице и са натрупани през различните стадии на тази процедура, може да му позволи да направи точни изводи за личния живот на това лице. Следователно националната правна уредба трябва да предвижда предварителен контрол, който да се осъществява, преди публичният орган да може да свърже данните за самоличността с тази съвкупност от данни и преди евентуално да бъде изпратено уведомителното писмо, че действията на лицето биха могли да подлежат на наказателно преследване. Освен това този контрол трябва да запазва ефективността на процедурата на поетапните мерки, като в частност позволява да се идентифицират случаите на повторност на съответните деяния. За тази цел процедурата трябва да е организирана и структурирана така, че натоварените с проверката служители на компетентния публичен орган да не могат да свързват данните за самоличността на лицето, съответстващи на IP адреси, предварително събрани в интернет, с данни, с които този орган вече разполага и които биха могли да позволяват да се направят точни изводи за личния живот на това лице.

Също така, що се отнася до предмета на предварителния контрол, Съдът отбелязва, че ако съответното лице е заподозряно в извършването на престъпление, което спада към престъпленията въобще, отговорният за контрола съд или независим административен орган трябва да откаже достъп, когато той би позволил на публичния орган да направи точни изводи за личния живот на това лице. Обратно, достъпът трябва да бъде разрешен дори ако позволява да се направят такива точни изводи, когато съответното лице е заподозряно в извършването на деяния, които в съответната държава членка се смятат за посегателства срещу основен обществен интерес и в този смисъл спадат към тежките форми на престъпност.

Съдът също така уточнява, че предварителният контрол не бива в никакъв случай да е изцяло автоматизиран, тъй като при наказателните производства този контрол изисква претегляне на легитимните интереси за борба с престъпността спрямо зачитането на неприкосновеността на личния живот и защитата на личните данни. Това претегляне е необходимо да се извършва с участието на физическо лице, като тази необходимост е още по-голяма, когато автоматизмът и големият мащаб на обработването на съответните данни пораждат рискове за личния живот.

Затова Съдът заключава, че възможността натоварените с проверката служители на публичния орган да свържат данните за самоличността на лицето, съответстващи на даден IP адрес, с файловете, които съдържат данни, позволяващи да се узнае заглавието на защитените произведения, чието предоставяне на разположение в интернет е причината за събирането на IP адресите от организациите на носителите на права, трябва да е обвързана с контрол от страна на съд или независим административен орган в случаите на повторно извършване на дейността, водеща до нарушение на авторското или сродните му права от същото лице. Този контрол не може да е изцяло автоматизиран и трябва да се осъществява преди свързването на съответните данни, което би могло в тези случаи да позволи да се направят точни изводи за личния живот на съответното лице, чийто IP адрес е използван за дейности, които може да нарушават авторското или сродните му права.

На четвърто и последно място, Съдът отбелязва, че използваната от публичния орган система за обработване на данни трябва на редовни интервали да се подлага на контрол от независима организация, която има качеството на трето лице спрямо този публичен орган. Този контрол служи за проверка на целостта на системата, включително ефективните гаранции срещу рисковете от злоупотреба с достъпа или с данните или от неправомерен достъп или неправомерно използване на тези данни, както и на ефикасността и надеждността ѝ за откриването на евентуални нарушения.

Във връзка с това Съдът отбелязва, че в разглеждания случай автоматизираното обработване на личните данни от публичния орган въз основа на информацията за нарушенията на права на интелектуална собственост, констатирани от организациите на носителите на тези права, би могло да дава определен брой грешни положителни резултати и най-вече би могло да създава риска потенциално много голям брой данни да бъдат превратно използвани от трети лица за злоупотреби или неправомерни цели, което обяснява необходимостта от такъв контрол. Наред с това той добавя, че въпросното обработване трябва да е съобразено със специалните правила за защита на личните данни по Директива 2016/680. Всъщност, макар че в случая не разполага със собствени правомощия за вземане на решения в процедурата на поетапните мерки, публичният орган трябва да се квалифицира като „публичен орган“, участващ в предотвратяването и

разкриването на престъпления, и затова попада в приложното поле на тази директива. В този смисъл лицата, до които се отнася тази процедура, трябва да се ползват с всички материалноправни и процесуалноправни гаранции, предвидени от Директива 2016/680, за които запитващата юрисдикция има задачата да се увери, че са предвидени в националното законодателство.

2. Обработване на лични данни в областта на наказателното право

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 Шенген⁶⁸, 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

⁶⁸ 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. 19; Специално издание на български език, 2007 г., глава 19, том 1, стр. 183) (наричана по-нататък „КПСШ“).

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 право⁶⁹.

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 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.

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 2016/680⁷⁰. 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 бюлетина⁷¹. Впрочем това обработване от органите на държавите членки може да се окаже задължително именно за да се провери дали този принцип е приложим.

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

⁶⁹ 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, и поправка в ОВ L 127, 2018 г., стр. 6).

⁷⁰ Вж. член 2, параграф 1 и член 3, точка 2 от Директива 2016/680.

⁷¹ Вж. член 4, параграф 1, буква б) и член 8, параграф 1 от Директива 2016/680.

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 наказания⁷².

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*.

Решение от 21 юни 2022 г. (голям състав), *Ligue des droits humains (C-817/19, EU:C:2022:491)*

По това дело (вж. също раздел I.1, „Съвместимост на вторичното право на Съюза с правото на защита на личните данни“), след като установява валидността на Директивата за PNR, Съдът разяснява тълкуването на някои от нейните разпоредби⁷³.

Първо, Съдът отбелязва, че в Директивата изчерпателно се изброяват целите, преследвани с обработването на PNR данните. Следователно тази директива не допуска национално законодателство, което разрешава обработването на PNR данни за цели различни от борбата срещу терористичните престъпления и тежките престъпления. Поради това национално законодателство, което освен това допуска като цел на обработването на PNR данни да се извършва контрол на съответните дейности от разузнавателните служби и службите за сигурност, може да е в противоречие с изчерпателния характер това изброяване. По същия начин установената с Директивата за PNR система не може да бъде предвидена за целите на подобряването на граничния контрол и борбата срещу незаконната имиграция. От това следва също, че PNR данните не могат да бъдат съхранявани в единна база данни, с която може да се прави справка за постигането както на целите на Директивата за PNR, така и на други цели.

⁷² Вж. член 1, параграф 1 и член 8, параграф 1 от Директива 2016/680.

⁷³ По-конкретно член 2 („Прилагане на [Директивата] по отношение на вътрешни за ЕС полети“), член 6 („Обработване на резервационни данни на пътниците“) и член 12 („Срок за съхраняване на данните и деперсонализация“) от Директивата за PNR.

Второ, Съдът изяснява понятието за независим национален орган, компетентен да провери дали са изпълнени условията за разкриване на PNR данните за целите на тяхната последваща оценка и да одобри такова разкриване. По-конкретно органът, създаден като ЗДП, не може да бъде квалифициран като такъв, тъй като няма качеството на трето лице по отношение на органа, който иска достъп до данните. Всъщност, тъй като неговите служители могат да бъдат командировани от органите, които са оправомощени да искат такъв достъп, ЗДП изглежда по необходимост свързано с тези органи. Следователно Директивата за PNR не допуска национално законодателство, съгласно което органът, създаден като ЗДП, има същевременно качеството на компетентен национален орган, оправомощен да одобрява разкриването на PNR данни в рамките на шест месеца след предаването на тези данни на ЗДП.

Трето, що се отнася до срока на съхранение на PNR данните, Съдът постановява, че член 12 от Директивата за PNR във връзка с членове 7 и 8, и член 52, параграф 1 от Хартата не допуска национално законодателство, което предвижда общ срок от пет години за съхраняване на тези данни, приложим без разграничение към всички пътуващи със самолет пътници.

Всъщност според Съда след изтичане на първоначалния срок за съхраняване от шест месеца съхраняването на PNR данни не изглежда ограничено до стриктно необходимото, що се отнася до пътуващите със самолет пътници, за които нито предварителната оценка, нито евентуалните проверки, извършени в рамките на първоначалния срок на съхраняване от шест месеца, нито някое друго обстоятелство е разкрило наличието на обективни сведения — като например факта, че PNR данните за съответни пътници са показали положително съвпадение, проверено в рамките на предварителната оценка — от които да може да се установи опасност в областта на терористичните престъпления и тежките престъпления, които имат обективна връзка, най-малкото непряка, с въздушния превоз на тези пътници. За разлика на това Съдът счита, че съхранението през първоначалния срок от шест месеца на PNR данните на всички пътници във въздушния транспорт, обхванати от установената с тази директива система, по принцип не надхвърля границите на строго необходимото.

Четвърто, Съдът предоставя указания относно евентуалното прилагане на Директивата за PNR за целите на борбата срещу терористичните престъпления и тежките престъпления към други транспортни средства, превозващи пътници в Съюза. Директивата обаче, тълкувана с оглед на член 3, параграф 2 ДЕС, член 67, параграф 2 ДФЕС и член 45 от Хартата, не допуска система за предаване и обработване на PNR данни за превозите, извършвани с други средства в Съюза, при липсата на действителна и настояща или предвидима терористична заплаха, пред която е изправена съответната държава членка. При това положение, както за вътрешните за ЕС полети, прилагането на установената с Директивата за PNR система трябва да бъде ограничено до PNR данните за превозите, които се отнасят

по-специално до някои маршрути или схеми за пътуване или още до някои гари или морски пристанища, за които са налице индикации, които могат да обосноват това прилагане. Съответната държава членка трябва да подбере превозите, за които са налице такива индикации, и да преразглежда периодично това прилагане в зависимост от развитието на обстоятелствата, обосновавали подбора им.

IV. Предаване на лични данни на трети страни

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

По това дело (вж. също раздел 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.

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.

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

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/ЕО⁷⁴ Комисията е приела, че в рамките на т.нар. схема за „сфера на неприкосновеност на личния живот“ (на английски „safe harbour“)⁷⁵ 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 тези права, и без да се отбелязва наличието на ефективна правна защита срещу този вид намеса.

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

⁷⁴ 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 (ОБ L 215, 2000 г., стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64).

⁷⁵ 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.

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. Съдът заключава, че невалидността на членове 1 и 3 от Решение 2000/520 засяга валидността на цялото решение.

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

Освен това и преди всичко, защитата на основното право на зачитане на личния живот на равнище на Съюза изисква дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото. Следователно 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 разграничаване, ограничаване 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. По-конкретно, правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, засяга същественото съдържание на основното право на зачитане на личния живот. Също така правна уредба, в която не се предвижда никаква възможност правният субект да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни, не зачита същественото съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата.

Становище 1/15 (Споразумение PNR EC—Канада) от 26 юли 2017 г. (голям състав)
([EU:C:2017:592](#))

На 26 юли 2017 г. Съдът се произнеса за първи път по съвместимостта на проект за международно споразумение с Хартата, 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.

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.).

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.

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.

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

В това отношение Съдът подчертава, че в предвиденото споразумение е важно пътниците във въздушния транспорт да бъдат информирани за предаването на техните PNR данни в съответната трета страна и за използването на същите

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

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

Решение от 16 юли 2020 г. (голям състав), *Facebook Ireland u Schrems (C-311/18, EU:C:2020:559)*

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 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 споразумения⁷⁶. 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 защита⁷⁷. 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 гаранции⁷⁸.

Г-н Maximillian Schrems, пребиваващ в Австрия гражданин на тази държава, е потребител на Facebook 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

⁷⁶ Член 45 от ОРЗД.

⁷⁷ Член 46, параграф 1 и параграф 2, буква в) от ОРЗД.

⁷⁸ Член 49 от ОРЗД.

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 2000/520⁷⁹ Комисията е констатирала, че Съединените щати гарантират достатъчна степен на защита. С решение от 6 октомври 2015 г. Съдът, сезиран с преюдициално запитване от High Court (Висш съд, Ирландия), обявява това решение за невалидно (наричано по-нататък „решението Schrems I“⁸⁰).

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/ЕС⁸¹. 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 дело Комисията приема Решение (ЕС) 2016/1250 относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ⁸².

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 изискването 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.

⁷⁹ 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).

⁸⁰ Решение на Съда от 6 октомври 2015 г., Schrems, C-362/14, [EU:C:2015:650](#).

⁸¹ 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).

⁸² 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).

Съдът констатира, че при разглеждането на Решение 2010/87 с оглед на Хартата не се установяват обстоятелства, които могат да засегнат неговата валидност. За сметка на това Съдът обявява за невалидно Решение 2016/1250.

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.

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 Съдът уточнява, че при оценката на това ниво на защита трябва да се вземат предвид както договорните клаузи, уговорени между администратора или обработващия лични данни, установени в Европейския съюз, 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.

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 средства, в случай че самият установен в Съюза износител не е спрял или прекратил това предаване.

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 изискваното 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 Съдът подчертава по-специално че това решение установява задължение за администратора и получателя на лични данни предварително да проверят спазването в съответната трета държава на това ниво на защита и задължава получателя на тези данни да информира администратора за евентуалната си невъзможност да осигури съответствие с тези клаузи, като тогава последният може да спре предаването на данни и/или да прекрати сключения договор.

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, обществен 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.

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.

V. Защита на личните данни в интернет

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

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

В това решение (вж. също раздел II.1, „Обхват на общата уредба“, и раздел 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.

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. Ето защо, ако вследствие на искане от съответното лице се установи, че включването на тези връзки в списъка с резултатите към настоящия момент е несъвместимо с Директивата, информацията

и съответните връзки в посочения списък трябва да бъдат изтрети. 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.

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.

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](#))

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

При тези обстоятелства Juzgado de lo Mercantil no 5 de Madrid (Съд по търговски дела № 5, Мадрид, Испания) отправя запитване до Съда дали европейското законодателство задължава държавите членки да предвидят задължение за

съобщаване на лични данни в рамките на гражданско производство, за да осигурят ефективна защита на авторското право.

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

В това отношение Съдът заключава, че Директива 2000/31/ЕО за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директивата за електронната търговия)⁸³, Директива 2001/29/ЕО относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество⁸⁴, Директива 2004/48/ЕО относно упражняването на права върху интелектуалната собственост⁸⁵ 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.

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.

⁸³ 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, 2000 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 29, стр. 257).

⁸⁴ 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, 2001 г., стр. 10; Специално издание на български език, 2007 г., глава 17, том 1, стр. 230).

⁸⁵ 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, 2004 г., стр. 45; Специално издание на български език, 2007 г., глава 17, том 2, стр. 56).

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 разпорежба 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 иски за защита от нарушенията на авторското право, но същевременно не задължава държавите членки да предвидят такова задължение. Органите и юрисдикциите на държавите членки обаче са длъжни не само да тълкуват националното си право в съответствие с тези директиви, но и да не се основават на тълкуване на последните, което би влязло в конфликт с посочените основни права или с другите общи принципи на правото на Съюза, като принципа на пропорционалност.

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.

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.

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, [EU:C:2019:773](#))

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 забранено⁸⁶, 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 гаранции⁸⁷.

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

⁸⁶ Член 8, параграф 1 от Директива 95/46 и член 9, параграф 1 от Регламент 2016/679.

⁸⁷ Член 8, параграф 5 от Директива 95/46 и член 10 от Регламент 2016/679.

чувствителност на тези данни може да представлява особено тежко вмешателство в основните права на зачитане на личния живот и на защита на личните данни.

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

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 лице⁸⁸, 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 положение⁸⁹.

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.

⁸⁸ Член 8, параграф 2, буква д) от Директива 95/46 и член 9, параграф 2, буква д) от Регламент 2016/679.

⁸⁹ Член 14, първа алинея, буква а) от Директива 95/46 и член 21, параграф 1 от Регламент 2016/679.

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 по-специално налага връзки към уебстраници, съдържащи съответната информация, да се появяват на първо място в този списък.

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

Commission nationale de l'informatique et des libertés (Национална 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 не⁹⁰.

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 Съюза⁹¹ 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.

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.

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

⁹⁰ Член 4, параграф 1, буква а) от Директива 95/46 и член 3, параграф 1 от Регламент 2016/679.

⁹¹ Член 12, буква б) и член 14, първа алинея, буква а) от Директива 95/46 и член 17, параграф 1 от Регламент 2016/679.

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.

Решение от 8 декември 2022 г. (голям състав), Google (Премахване от резултатите при търсене, на съдържание, за което се твърди, че е неистинно) (C-460/20, [EU:C:2022:962](#))

През 2015 г. G LLC, лице, което е управлява интернет сайт, публикува на този сайт три статии за ищците в главното производство — TU, който заема отговорни длъжности и притежава дялове в различни дружества, и RE, която е неговата партньорка в личния живот и до май 2015 г. е прокурист на едно от тези дружества. В тези статии, едната от които е илюстрирана с четири снимки на ищците, се прави внушение, че посочените лица водят луксозен живот, и се разглежда по критичен начин инвестиционният модел, прилаган от някои от техните дружества. Достъпът до тези статии е възможен, след като в интернет търсачката, управлявана от Google LLC (наричано по-нататък „Google“), се изпишат фамилните и собствените имена на жалбоподателите — както поотделно, така и в съчетание с наименованията на някои от дружествата. Чрез връзка в списъка с резултати от търсенето се препраща към тези статии, както и към снимките, представени под формата на миниатюрни изображения (thumbnails).

Ищците в главното производство искат от Google, в качеството му на администратор на лични данни, обработвани чрез неговата интернет търсачка, от една страна, да премахне от списъка с резултатите при търсене връзките, препращащи към разглежданите статии, с мотива че те съдържали неистинни твърдения и клеветнически мнения, а от друга страна, да отстрани миниатюрните изображения от списъка с резултати от търсенето. Google отказва да уважи това искане.

Тъй като исканията им са отхвърлени както в първоинстанционното, така и във въззивното производство, ищците в главното производство сезират Bundesgerichtshof (Федерален върховен съд, Германия) с ревизионна жалба, в рамките на която Bundesgerichtshof сезира Съда с преюдициално запитване относно тълкуването на ОРЗД и на Директива 95/46⁹².

⁹² Съответно член 17, параграф 3, буква а) от ОРЗД и член 12, буква б) и член 14, първа алинея, буква а) от Директива 95/46.

С решението си, постановено от голям състав, Съдът развива практиката си относно приложимите изисквания към исканията за премахване от резултатите при търсене, подавани до лицето, което управлява интернет търсачка, въз основа на разпоредбите относно защитата на личните данни. По-специално той разглежда, от една страна, обхвата на задълженията и отговорностите на лицето, което управлява интернет търсачка, когато то обработва искане за премахване от резултатите при търсене, при положение че в това искане се сочат като основание твърдения за неистинност на информацията, включената в съдържание, към което се препраща, и от друга страна, тежестта на доказване, възложена на субекта на данните във връзка с тази неистинност. От друга страна, той се произнася по необходимостта при разглеждане на отправено искане за заличаване на снимки, показвани в списъка с резултатите при търсене на изображения, да се вземе предвид първоначалният контекст на публикацията на тези снимки в интернет.

На първо място, Съдът постановява, че в контекста на претеглянето между, от една страна, правата на зачитане на личния живот и на защита на личните данни и от друга страна, свободата на изразяване и правото на информация⁹³, когато се разглежда искане за заличаване от списъка с резултати при търсене на връзка, която насочва към съдържание, включващо информация, за която се твърди, че е неистинна, това премахване от резултатите при търсене не се обвързва с условието на въпроса относно истинността на съдържанието, към което се препраща, да е даден поне индикативен отговор в рамките на производство по иск, предявен от подалото искането лице, срещу доставчика на съдържанието.

Преди всичко останало, за да разгледа при какви условия лицето, което управлява интернет търсачка, е длъжно да уважи искане за премахване от резултатите при търсене и следователно да изтрие от списъка с резултатите, който се показва след търсене по името на субекта на данните, връзката към интернет страница, на която са публикувани твърдения, които това лице намира за неистинни, Съдът по-специално припомня следното:

- доколкото дейността на интернет търсачка може да засегне значително и в допълнителна степен по отношение на дейността на издателите на интернет сайтове основните права на зачитане на личния живот и на защита на личните данни, лицето, което управлява търсачката в качеството си на лице, което определя целите и средствата на тази дейност, трябва да гарантира в рамките на своята отговорност, компетентност и възможности, че предвидените в Директива 95/46 и ОРЗД гаранции могат да разгърнат цялостното си действие и може действително да се осъществи ефикасна и пълна защита на съответните лица,

⁹³ Основни права, гарантирани съответно от членове 7, 8 и 11 от Хартата.

- когато е сезирано с искане за премахване от резултатите при търсене, лицето, което управлява интернет търсачка, трябва да провери дали включването на връзката към въпросната интернет страница в списъка, който се показва след търсене по името на субекта на данните, е необходимо за упражняването на правото на свобода на информация на интернет потребителите, които са потенциално заинтересовани да получат достъп до тази интернет страница посредством такова търсене, защитено от свободата на изразяване и правото на информация,
- ОРЗД изрично закрепва изискването за претегляне между, от една страна, основните права на зачитане на личния живот и на защита на личните данни и от друга страна, основното право на свобода на информация.

На първо място, Съдът изтъква, че макар правото на зачитане на личния живот и правото на защита на личните данни да имат по принцип предимство пред законния интерес на интернет потребителите, които потенциално биха могли да имат достъп до въпросната информация, това равновесие все пак може да зависи от релевантните обстоятелства във всеки отделен случай, по-специално от естеството на тази информация и от чувствителността ѝ по отношение на личния живот на субекта на данни, както и от интереса на обществеността да разполага с посочената информация, който може да бъде различен по-специално в зависимост от ролята на този субект в обществения живот.

Въпросът дали съдържанието, към което се препраща, е истинно или не, също представлява релевантен елемент за тази преценка. Така при определени обстоятелства правото на информация на интернет потребителите и свободата на изразяване на доставчика на съдържание могат да надделеят над правата на зачитане на личния живот и на защита на личните данни по-специално когато субектът на данните играе определена роля в обществения живот. Въпреки това тази тенденция се преобръща във всички случаи, когато се окаже неистинна дори част от информацията, посочена в искането за премахване от резултатите при търсене, щом тя не е с второстепенен характер спрямо цялото съдържание. В подобна хипотеза би могло дори да се твърди, че в действителност правата на предоставяне и на получаване на информация изобщо не влизат в действие, тъй като тези права не могат да включват право на разпространяване и достъп до такава информация.

По-нататък, що се отнася, от една страна, до задълженията да се установи дали информацията, включена в съдържанието, към което се препраща, е с истинен или неистинен характер, Съдът уточнява, че лицето, което иска премахване от резултатите при търсене поради неистинност на тази информация, трябва да докаже, че тази информация е очевидно неистинна или че такава е поне част от тази информация, която не е маловажна от гледна точка на цялото съдържание. Все пак, за да се избегне възлагането на това лице на прекомерна тежест, която може да навреди на полезното действие на правото на премахване от резултатите

при търсене, то трябва да представи единствено доказателствата, които, с оглед на обстоятелствата в конкретния случай, може разумно да се изисква от него да издири. По принцип посоченото лице не може да бъде задължено още от досъдебната фаза на правния спор да представи в подкрепа на искането си за премахване от резултатите при търсене съдебно решение, постановено срещу издателя на интернет сайта, дори под формата на решение, взето в рамките на производство по постановяване на привременни или обезпечителни мерки.

От друга страна, що се отнася до задълженията и отговорностите на лицето, което управлява интернет търсачката, Съдът подчертава, че за да провери дали дадено съдържание може да продължи да бъде включвано в списъка с резултатите от търсенето, извършено чрез неговата търсачка, след като е подадено на искане за премахване от резултатите при търсене, това лице трябва да се основе на всички налични права и интереси, както и на всички обстоятелства по конкретния случай. Все пак лицето, което управлява интернет търсачка, не може да бъде задължавано да разследва фактите и за тази цел да организира обмен на кореспонденция, при условията на състезателност с доставчика на съдържанието, за да се получат липсващите доказателства относно истинността на съдържанието, към което се препраща. Ако посоченото лице, което управлява интернет търсачката, бъде обвързано със задължение да вземе участие при доказването на обстоятелството дали съдържанието, към което се препраща, е истинно или не, на същото лице би била възложена тежест, надхвърляща това, което разумно може да се очаква от него с оглед на неговата отговорност, компетентност и възможности. Това разрешение би създавало сериозен риск от резултатите при търсене да бъдат премахнати съдържания, с които се задоволява законосъобразна и приоритетна за обществеността нужда от информация, и по този начин да се окаже трудно тези съдържания да бъдат намерени в интернет. Вследствие на това би съществувал реален риск от възпиращ ефект върху упражняването на свободата на изразяване и на информация, ако лицето, което управлява интернет търсачката, извършва премахване от резултатите при търсене почти систематично, за да се избегне понасянето на тежестта за разследване на релевантните факти, в опит да се установи дали посоченото съдържание е истинно или не.

Следователно, когато лицето, поискало премахване от резултатите при търсене, представи доказателства, установяващи очевидната неистинност на включена в съдържанието, към което се препраща, информация или поне на част от тази информация, която не е маловажна от гледна точка на цялото съдържание, лицето, което управлява интернет търсачката, е длъжно да уважи това искане. Същото важи и за случая, когато направило такова искане лице представи съдебно решение, постановено срещу издателя на интернет сайта, което се основава на констатацията, че информацията, съдържаща се в съдържанието, към което се препраща, която не е маловажна от гледна точка на цялото съдържание, поне на пръв поглед е неистинна. За сметка на това, когато не е представено такова съдебно решение, в случай че неистинният характер на информацията не

следва очевидно от гледна точка на представените от подалото искането лице доказателства, лицето, което управлява интернет търсачката, не е длъжно да уважи искането за премахване от резултатите при търсене. Когато разглежданата информация може да допринесе за дебат от общ интерес, с оглед на всички обстоятелства по настоящия случай следва да се придаде особено значение на правото на свобода на изразяване и на информация.

Накрая, Съдът добавя, че когато лицето, което управлява интернет търсачка, не изпълни искане за премахване от резултатите при търсене, субектът на данните трябва да може да сезира надзорния или съдебния орган, за да може той да извърши необходимите проверки и да разпорежи на посочения администратор да предприеме необходимите мерки. В това отношение именно съдебните органи трябва да осигурят претеглянето на конкуриращите се интереси, тъй като те са в най-добра позиция да извършат сложно и задълбочено претегляне, като вземат предвид всички критерии и обстоятелства, установени в релевантната съдебна практика.

На второ място, Съдът постановява, че при претеглянето между горепосочените основни права при искане за заличаване от списъка с резултатите при търсене на изображения по името на физическо лице, вследствие на което се визуализират снимки на това лице под формата на миниатюрни изображения, следва да се държи сметка за информативната стойност на тези снимки, независимо от контекста на тяхната публикация на интернет страницата, откъдето те са изтегляни. Въпреки това следва да се вземе предвид всеки текстови елемент, който съпътства пряко визуализирането на тези снимки в резултатите при търсенето и който може да предостави разяснения относно информативната им стойност.

За да стигне до този извод, Съдът подчертава, че търсенето по името на дадено лице на изображения чрез търсачка в интернет се подчинява на същите принципи, каквито са приложими и към търсенето на интернет страници и на съдържащата се в тях информация. Той посочва, че когато след търсене по име се показват снимки на субекта на данни под формата на миниатюрни изображения, тази визуализация може да представлява особено силно вмешателство в правото на зачитане на личния живот и в правото на защита на личните данни на това лице.

Следователно, когато лицето, което управлява интернет търсачка, е сезирано с искане за премахване, с което се иска от резултатите при търсене на изображения въз основа на името на дадено лице да бъдат заличени снимките, показвани под формата на миниатюрни изображения на това лице, управляващият интернет търсачката трябва да провери дали визуализирането на въпросните снимки е необходимо за упражняването на правото на свобода на информация на интернет потребителите, които са потенциално заинтересовани да имат достъп до тези снимки посредством такова търсене

Доколкото обаче интернет търсачката показва снимки на субекта на данните извън контекста, в който те са публикувани на интернет страница, към която се препраща, най-често за да илюстрират съдържащите се в тази страница текстови откъси, следва да се определи дали този контекст все пак трябва да се вземе предвид при претеглянето на конкуриращите се права и интереси, което следва да бъде извършено. Във връзка с това въпросът дали посочената преценка трябва да включва и съдържанието на интернет страницата, в която е включена снимката, чието премахване от показваните резултати под формата на миниатюрно изображение е поискано, зависи от предмета и естеството на въпросното обработване.

Що се отнася, на първо място, до предмета на разглежданото обработване, Съдът отбелязва, че публикуването на снимки като средство за невербална комуникация може да има по-силно въздействие върху интернет потребителите, отколкото текстовите публикации. Това е така, защото сами по себе си снимките са важно средство за привличане на вниманието на интернет потребителите и могат да предизвикат интерес от достъп до статиите, които илюстрират. Именно обаче поради това, че снимките често позволяват различни тълкувания, показването им в списъка с резултатите при търсене под формата на миниатюрни изображения може да представлява особено силно вмешателство в правото на субекта на данни на защита на своето изображение, което трябва да се вземе предвид при претеглянето на конкуриращите се права и интереси. Извършването на отделно претегляне се налага в зависимост от обстоятелството дали става въпрос, от една страна, за статии, съдържащи снимки, публикувани от издателя на интернет страницата, които в първоначалния им контекст илюстрират съдържашата се в тези статии информация и изразените в тях становища, и от друга страна, снимки, показвани под формата на миниатюрни изображения в списъка с резултати от лицето, което управлява интернет търсачка, извън контекста, в който те са публикувани на първата интернет страница.

В това отношение Съдът припомня, че основанието за публикуването на лични данни на даден интернет сайт не е непременно идентично с основанието, което се прилага за дейността на интернет търсачките, като дори когато случаят е такъв, резултатът от претеглянето на разглежданите интереси, което трябва да се извърши, може да бъде различен в зависимост това дали обработването на данни е извършвано от лицето, което управлява интернет търсачката, или от издателя на тази интернет страница. От една страна, легитимните интереси, обосноваващи това обработване, могат да бъдат различни и от друга страна, последиците от посоченото обработване за субекта на данните, и по-специално за личния му живот, не са непременно едни и същи.

Що се отнася, на второ място, до естеството на обработването от страна на лицето, което управлява интернет търсачката, Съдът констатира, че като открива публикуваните в интернет снимки на физически лица и като ги възпроизвежда

отделно в резултатите от търсенето на изображения — под формата на миниатюрни изображения — лицето, което управлява интернет търсачка, предлага услуга, свързана с обработване на лични данни, която се различава от обработването на данни от страна на издателя на интернет страницата, от която са изтегляни снимките, както и от обработването, администрирано от лицето, което управлява интернет търсачката, с оглед на препращането към тази страница.

Следователно дейността, осъществявана от лицето, което управлява интернет търсачка, състояща се в показването на резултати при търсене на изображения под формата на миниатюрни изображения, следва да бъде подлагана на самостоятелна преценка, тъй като допълнителното засягане на основните права, произтичащо от такава дейност, може да бъде особено интензивно, защото при търсене по име се обединява цялата налична в интернет информация за съответното лице. В рамките на тази самостоятелна преценка следва да се вземе предвид обстоятелството, че тази визуализация сама по себе си представлява търсеният от интернет потребителя резултат, независимо от последващото му решение дали да получи достъп до първоначалната интернет страница.

Съдът отбелязва все пак, че подобно специфично претегляне, при което се взема предвид самостоятелното естество на обработването, извършено от лицето, което управлява интернет търсачката, не засяга евентуалната релевантност на текстуалните елементи, които могат пряко да съпътстват визуализирането на снимка в списъка с резултатите при търсене, тъй като тези елементи могат да предоставят разяснения относно информационната стойност на тази снимка за обществеността и следователно да повлияят при претеглянето на съответните права и интереси.

4. Съгласие от потребителите на уебсайтове за съхраняването на информация

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

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 2002/58⁹⁴, във връзка с Директива 95/46⁹⁵ и във връзка с ОРЗД⁹⁶.

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 предвижда в ОРЗД⁹⁷, 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“.

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,

⁹⁴ 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).

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

⁹⁶ Член 6, параграф 1, буква а) от Регламент 2016/679.

⁹⁷ Пак там.

не би могло да бъде достатъчно, за да се счита, че даването на съгласие от негова страна за записването на бисквитки е било действително.

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.

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.

5. Обработване на лични данни в социалните мрежи онлайн

Решение от 4 юли 2023 г. (голям състав), Meta Platforms и др. (Общи условия за използване на социална мрежа) (C-252/21, [EU:C:2023:537](#))

Дружество Meta Platforms е собственик на социалната онлайн мрежа „Facebook“, която е безплатна за частните ползватели. Икономическият модел на тази социална мрежа се базира на финансиране чрез онлайн реклама, съобразена с отделните ползватели на тази мрежа. Такава реклама е технически възможна благодарение на автоматизираното създаване на подробни профили на ползвателите на мрежата и на онлайн услугите, предлагани на равнището на група Meta. Така, за да могат да използват посочената социална мрежа, при регистрирането си ползвателите трябва да приемат определените от Meta Platforms общи условия, които препращат към определените от това дружество политики за използване на данни и бисквитки. Съгласно посочените политики освен данните, които тези ползватели предоставят пряко при регистрирането си, Meta Platforms събира и свързани с ползвателите данни относно действията на ползвателите във и извън социалната мрежа и свързва тези данни с акаунтите на съответните ползватели във Facebook. Колкото до последните данни, наричани и „данни off Facebook“, става дума, от една страна, за данните за посещения на уебсайтове и приложения на трети лица, и от друга, за данните за използването на други онлайн услуги, собственост на група Meta (сред които Instagram и WhatsApp).

Общият преглед на така събраните данни позволява да се направят подробни изводи за предпочитанията и интересите на същите ползватели.

С решение от 6 февруари 2019 г. Bundeskartellamt (Федерален орган за защита на конкуренцията, Германия) забранява на Meta Platforms, от една страна, да обвързва в действащите към тогавашния момент общи условия използването на социалната мрежа Facebook от частни ползватели, които живеят в Германия, с обработването на техните данни off Facebook, и от друга, да обработва тези данни без тяхно съгласие. Освен това федералният орган за защита на конкуренцията задължава Meta Platforms да измени тези общи условия така, че от тях ясно да следва, че посочените данни няма да бъдат събирани, свързвани с потребителските акаунти във Facebook или използвани без съгласието на съответните ползватели. Накрая, този орган подчертава, че такова съгласие не е валидно, когато то представлява условие за използването на социалната мрежа. Той мотивира решението си с това, че разглежданото обработване на данни, което не било в съответствие с ОРЗД, представлявало злоупотреба с господстващото положение на Meta Platforms на пазара на социални онлайн мрежи.

Meta Platforms обжалва това решение пред Oberlandesgericht Düsseldorf (Висш областен съд Дюселдорф, Германия). Този съд не е сигурен, наред с друго, как следва да тълкува и прилага някои от разпоредбите на ОРЗД, и отправя преюдициално запитване до Съда.

С решението си големият състав на Съда внася уточнения за възможността операторът на социална мрежа да обработва „чувствителни“ лични данни на ползвателите ѝ, за условията за законосъобразност на извършваното от такъв оператор обработване и за валидността на съгласието, което тези ползватели са дали за целите на такова обработване на предприятие с господстващо положение на националния пазар на социални онлайн мрежи.

Що се отнася до обработването на специални категории лични данни⁹⁸, Съдът приема, че когато ползвател на социална онлайн мрежа посещава уебсайтове или приложения във връзка с една или повече от тези категории и евентуално въвежда данни в тях, когато се регистрира или прави онлайн поръчки, обработването на лични данни от оператора на тази социална онлайн мрежа⁹⁹ следва да се счита за „обработване на специални категории лични данни“ по смисъла на член 9, параграф 1 от ОРЗД, когато прави възможно разкриването на

⁹⁸ Упоменати в член 9, параграф 1 от ОРЗД. Съгласно тази разпоредба „[се] забранява [...] обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице“.

⁹⁹ Това обработване се състои в събирането — чрез интегрирани интерфейси, бисквитки или подобни технологии за записване — на данни, резултат от посещаването на тези сайтове и приложения, както и на въведените от ползвателя данни, в свързването на всички тези данни с акаунта в социалната мрежа на този ползвател и в използването на посочените данни от този оператор.

информация, която попада в някоя от въпросните специални категории, независимо дали тази информация се отнася до ползвател на тази мрежа или до друго физическо лице. Такова обработване на данни по принцип е забранено, освен с някои изключения¹⁰⁰.

Във връзка с последното Съдът уточнява, че когато ползвател на социална онлайн мрежа посещава уебсайтове или приложения, свързани с една или повече от упоменатите специални категории данни, той не прави явно обществено достояние¹⁰¹ данните за това посещаване, събрани от оператора на тази социална онлайн мрежа чрез бисквитки или подобни технологии за записване. Освен това, когато въвежда данни в такива уебсайтове или приложения или натиска вградени в тези сайтове или приложения бутони, като бутоните „Харесвам“ или „Споделяне“, или бутоните, които позволяват на ползвателя да се идентифицира на тези сайтове или приложения, като използва идентификаторите за връзка, свързани с потребителския му акаунт в социалната мрежа, телефонния му номер или имейла му, такъв ползвател явно прави обществено достояние така въведените данни или данните, резултат от натискането на тези бутони, само в случай че изрично е изразил предварително решението си, евентуално след напълно информирано извършване на индивидуални настройки, да направи свързаните с него данни публично достъпни за неограничен брой лица.

На трето място, що се отнася по-общо до условията за законосъобразност на обработването на лични данни, Съдът припомня, че съгласно ОРЗД обработването на данни е законосъобразно, ако и доколкото субектът на данните е дал съгласие за това за една или повече конкретни цели¹⁰². Когато липсва такова съгласие или когато съгласието не е свободно изразено, конкретно, информирано и недвусмислено, подобно обработване все пак е обосновано, ако отговаря на някое от изискванията за необходимост¹⁰³, които трябва да се тълкуват стриктно. Обработването от оператор на онлайн социална мрежа на лични данни на нейните ползватели обаче може да се счита за необходимо за изпълнението на договора, по който тези ползватели са страни, само ако това обработване е обективно необходимо за постигането на цел, която е неразделна част от

¹⁰⁰ Предвидени в член 9, параграф 2 от ОРЗД. Тази разпоредба гласи: „Параграф 1 не се прилага, ако е налице едно от следните условия:

- а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на Съюза или правото на държава членка се предвижда, че посочената в параграф 1 забрана не може да бъде отменена от субекта на данни; [...]
- д) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;
- е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

[...]”.

¹⁰¹ По смисъла на член 9, параграф 2, буква д) от ОРЗД.

¹⁰² Видно от формулировката на член 6, параграф 1, първа алинея, буква а) от ОРЗД.

¹⁰³ Споменати в член 6, параграф 1, букви б)–е) от ОРЗД. Съгласно тези разпоредби обработването е законосъобразно, само ако и доколкото, наред с останалото, е необходимо за изпълнението на договор, по който субектът на данните е страна [член 6, параграф 1, първа алинея, буква б) от ОРЗД], за спазването на законово задължение, което се прилага спрямо администратора [член 6, параграф 1, първа алинея, буква в) от ОРЗД], или за целите на легитимните интереси на администратора или на трета страна [член 6, параграф 1, първа алинея, буква е) от ОРЗД].

предназначената за същите ползватели договорна престация, така че основната цел на договора не би могла да бъде постигната без това обработване.

В допълнение, според Съда разглежданото обработване на данни може да се счита за необходимо за целите на легитимните интереси на администратора или на трета страна, само ако посоченият оператор е уведомил ползвателите, от които са били събрани данните, за преследван с обработването им легитимен интерес, това обработване се извършва в границите на строго необходимото за постигането на този легитимен интерес и от претеглянето на противоположните интереси, през призмата на всички релевантни обстоятелства, е видно, че интересите и основните права или свободи на тези ползватели нямат преимущество пред легитимния интерес на администратора или на трета страна. Съдът приема по-специално, че когато посочените ползватели не са дали съгласие, техните интереси и основни права имат преимущество пред интереса на оператора на социална онлайн мрежа от персонализиране на рекламата, с която той финансира дейността си.

Накрая, Съдът уточнява, че разглежданото обработване на данни е обосновано, когато действително е необходимо за спазването на законово задължение, което се прилага спрямо администратора по силата на разпоредба от правото на Съюза или на съответната държава членка, това правно основание е съобразено с общественения интерес и е пропорционално на преследваната легитимна цел и това обработване се извършва в границите на строго необходимото.

Що се отнася до валидността на съгласието на съответните ползватели за обработване на техните данни съгласно ОРЗД, според Съда обстоятелството, че операторът на социална онлайн мрежа има господстващо положение на пазара на социалните онлайн мрежи, само по себе си не изключва възможността ползвателите на тази социална мрежа да дадат валидно съгласие за извършването от този оператор обработване на личните им данни. Като се има предвид обаче, че това положение може да накърни свободата на избор на тези ползватели и да доведе до очевидна неравнопоставеност между тях и посочения оператор, то е важен фактор за преценката дали съгласието действително е било дадено валидно, и по-специално свободно, което посоченият оператор носи тежестта да докаже¹⁰⁴.

По-специално, ползвателите на въпросната социална мрежа трябва да имат свободата да откажат индивидуално, в хода на процеса по сключване на договора, да дадат съгласието си за специални операции по обработване на данни, които не са необходими за изпълнението на договора, без обаче да са принудени да се откажат изцяло от ползването на тази социална онлайн мрежа, което предполага на посочените ползватели, евентуално срещу подходящо възнаграждение, да се

¹⁰⁴ Съгласно член 7, параграф 1 от ОРЗД.

предложи равностойна алтернатива, която не се съпътства от такива операции по обработване на данни. Освен това трябва да е възможно да се даде отделно съгласие за обработването на данни off Facebook.

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](#))

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 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.

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 задачите 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.

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.

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.

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 разпореда 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.

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

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.

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.

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.

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.

2. Определяне на приложимото право и на компетентния надзорен орган

Решение от 1 октомври 2015 г., Weltimmo (C-230/14, [EU:C:2015:639](#))

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 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.

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. 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.

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 раздел 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.

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.

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.

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

В това решение (вж. също раздел 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).

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.

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 Commission belge de la protection de la vie privée (Белгийска 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 модули¹⁰⁵ 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 Autorité belge de protection des données (Белгийски 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 ОРЗД¹⁰⁶, 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

¹⁰⁵ Например бутоните „Харесвам“ или „Споделям“.

¹⁰⁶ Съгласно 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 в съответствие с процедурата по член 60“.

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 данни бил компетентен да предяви иск за преустановяване на нарушение под надзора на ирландските юрисдикции.

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 данни¹⁰⁷, при положение че не е водещият орган във връзка с това обработване.

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 регламент¹⁰⁸.

Всъщност при трансграничното обработване ОРЗД предвижда механизма за „обслужване на едно гише“¹⁰⁹, 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 правила¹¹⁰, докато компетентността на другите национални надзорни органи да приемат подобно решение, дори временно, представлява изключение¹¹¹. При упражняването на правомощията си обаче водещият надзорен

¹⁰⁷ По смисъла на член 4, точка 23 от ОРЗД.

¹⁰⁸ Предвидени в членове 56 и 60 от ОРЗД.

¹⁰⁹ Член 56, параграф 1 от ОРЗД.

¹¹⁰ Член 60, параграф 7 от ОРЗД.

¹¹¹ Член 56, параграф 2 и член 66 от ОРЗД установяват изключенията от принципа, че водещият надзорен орган е компетентен да взема решения.

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.

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 органи¹¹², 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.

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 производство¹¹³, 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 ОРЗД¹¹⁴, което предполага администраторът или обработващият лични данни за трансграничното обработване да разполага с място на установяване на територията на Съюза.

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

¹¹² Предвидени в членове 55 и 56 във връзка с член 60 от ОРЗД.

¹¹³ По силата на член 58, параграф 5 от ОРЗД.

¹¹⁴ 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“.

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.

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

На пето и последно 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.

Решение от 16 януари 2024 г. (голям състав), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

По това дело (вж. също раздел II.1, „Обхват на общата уредба“) Съдът отбелязва, че разпоредбите на ОРЗД относно компетентността на националните надзорни органи и относно правото на обжалване¹¹⁵ не налагат да се приемат национални мерки за прилагане и са достатъчно ясни, конкретни и безусловни, за да имат

¹¹⁵ Съответно член 55, параграф 1 и член 77, параграф 1 от ОРЗД.

директен ефект. Следователно ОРЗД предоставя на държавите членки свобода на преценка досежно броя на надзорните органи, които да бъдат създадени¹¹⁶, но за сметка на това определя обхвата на техните правомощия, за да наблюдават прилагането на този регламент. Поради това, когато държава членка реши да създаде само един национален надзорен орган, същият задължително разполага с всички правомощия, предвидени от този регламент. Всяко различно тълкуване би поставило под въпрос полезния ефект на тези разпоредби и има опасност да отслаби полезния ефект на всички останали разпоредби от ОРЗД, до които може да се отнася дадена жалба.

По отношение на факта, че националните конституционни разпоредби изключват възможността надзорен орган, който е част от изпълнителната власт, да наблюдава прилагането на ОРЗД от орган на законодателната власт, Съдът подчертава, че в съзвучие именно с конституционната структура на държавите членки ОРЗД просто изисква те да създадат поне по един надзорен орган, като им дава възможност да създадат и няколко. Следователно този регламент предоставя на всяка държава членка свобода на преценка, което ѝ позволява да създаде толкова надзорни органа, колкото по-специално налага нейната конституционна структура.

В допълнение позоваването от държава членка на разпоредби от националното ѝ право не може да накърни единството и ефикасността на правото на Съюза. Всъщност действието на принципа на предимство на правото на Съюза обвързва всички органи на дадена държава членка, без националните разпоредби в частност, в това число и конституционни, да могат да са пречка за това.

Следователно, щом е решила да създаде само един надзорен орган, държавата членка не може да се позовава на разпоредби от националното право, били те и с конституционен ранг, за да изключи обработването на лични данни, което попада в приложното поле на ОРЗД, от упражнявания от този орган надзор.

4. Условия за налагане на административни наказания

Решение от 5 декември 2023 г. (голям състав), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

По това дело (вж. също раздел II.3, „Понятие за обработване на лични данни“, раздел II.5, „Понятие за администратор на лични данни“, и раздел II.6, „Понятие за съвместен администратор“), Съдът констатира, че член 83 от ОРЗД допуска да се

¹¹⁶ Упоменати в член 51, параграф 1 от ОРЗД.

наложи административно наказание „глоба“ или „имуществена санкция“ на администратор само ако се установи, че последният е нарушил нормите на този регламент умишлено или по небрежност¹¹⁷.

В това отношение Съдът уточнява, че законодателят на Съюза не предоставя свобода на преценка на държавите членки да определят материалноправните условия, при които надзорен орган може да реши да наложи административно наказание „глоба“ или „имуществена санкция“ на основание на посочената разпоредба. Фактът, че ОРЗД им предоставя възможност да предвиждат както изключения за установените в тях публични органи и структури¹¹⁸, така и процедурни изисквания за надзорните органи при налагането на административно наказание „глоба“ или „имуществена санкция“¹¹⁹, по никакъв начин не означава, че държавите членки могат да предвиждат такива материалноправни условия.

По отношение на тези условия Съдът отбелязва, че един от изброените в ОРЗД елементи, които надзорният орган следва да вземе предвид, когато налага административно наказание „глоба“ или „имуществена санкция“ на администратор, е „дали нарушението е извършено умишлено или по небрежност“¹²⁰. За сметка на това нито един от тези елементи не се отнася до възможност да се ангажира отговорността на администратора при липса на вина от негова страна. В този смисъл на администратора може да се наложи административно наказание „глоба“ или „имуществена санкция“ съгласно член 83 от Регламента само за нарушенията на разпоредбите на ОРЗД, които той е извършил умишлено или по небрежност.

Съдът добавя, че това тълкуване намира потвърждение в общия разум и целта на ОРЗД. В този контекст той пояснява, че наличието на система от санкции по ОРЗД, която позволява да се наложи административно наказание, когато специфичните обстоятелства по конкретния случай дават основание за това, създава стимул за администраторите на данни и обработващите лични данни да спазват Регламента, а чрез възпиращия си ефект административните наказания спомагат за засилване на защитата на субектите на данните. При все това законодателят на Съюза не е счел за необходимо да предвиди налагане на административно наказание при липса на вина. Като се има предвид, че с ОРЗД се търси равнище на защита, което да е едновременно еквивалентно и еднородно, и че за тази цел той трябва да се прилага последователно навсякъде в Съюза, би се стигнало до противоречие с

¹¹⁷ Нарушение по член 83, параграфи 4—6.

¹¹⁸ По силата на член 83, параграф 7 от ОРЗД, който предвижда, че „[...] всяка държава членка може да определя правила за това дали и до каква степен могат да бъдат налагани административни наказания „глоба“ или „имуществена санкция“ на публични органи и структури, установени в тази държава членка“.

¹¹⁹ По силата на член 83, параграф 8 във връзка със съображение 129 от ОРЗД.

¹²⁰ Член 83, параграф 2, буква б) от ОРЗД.

тази цел, ако се позволи на държавите членки да предвидят такъв режим за налагането на административни наказания.

Освен това Съдът стига до извода, че такова наказание може да се наложи на администратор за извършени от негово име от обработващ лични данни операции по обработване, освен ако при тези операции обработващият лични данни е действал за изпълнение на свои собствени цели или по начин, който е несъвместим с определените от администратора рамка, ред и условия или с който не би могло разумно да се приеме, че администраторът би се съгласил. В такъв случай за отговорен за обработването трябва да се счита обработващият лични данни.

Решение от 5 декември 2023 г. (голям състав), *Deutsche Wohnen* (C-807/21, [EU:C:2023:950](#))

Deutsche Wohnen SE (наричано по-нататък „DW“) е дружество за недвижими имоти, което чрез своите дялове в различни дружества непряко притежава много жилищни и търговски обекти. Като част от търговската си дейност то обработва лични данни на наемателите на тези обекти.

След две проверки през 2017 г. и 2019 г. Berliner Beauftragte für den Datenschutz (Берлински орган за защита на личните данни, Германия) констатира редица нарушения на ОРЗД, извършени от DW. Затова с наказателно постановление от 30 октомври 2019 г. този надзорен орган налага на дружеството имуществени санкции.

DW обжалва наказателното постановление пред Landgericht Berlin (Областен съд Берлин, Германия), който прекратява административно-наказателното производство. Посоченият съд отбелязва, че съгласно германския закон¹²¹ извършители на административно нарушение могат да са само физическите, а не и юридическите лица. Същевременно юридическото лице може да отговаря само за действията на членовете на своите органи или на представителите си. Staatsanwaltschaft Berlin (Берлинска прокуратура, Германия) подава протест срещу това съдебно решение до Kammergericht Berlin (Висш областен съд Берлин, Германия). Тази юрисдикция се обръща към Съда с преюдициално запитване за тълкуването на ОРЗД.

В решението си големият състав на Съда се произнася относно условията за налагане на административни наказания по ОРЗД. На първо място, той разглежда въпроса дали държавите членки могат да обвързват налагането на

¹²¹ Gesetz über Ordnungswidrigkeiten (Закон за административните нарушения) от 24 май 1968 г. (BGBl. 1968 I, стр. 481), в редакцията, обнародвана на 19 февруари 1987 г. (BGBl. 1987 I, стр. 602), и с измененията съгласно Закона от 19 юни 2020 г. (BGBl. 2020 I, стр. 1350).

административно наказание на юридически лица с условието преди това да е прието, че нарушението на този регламент е извършено от идентифицирано физическо лице. На второ място, той се спира на въпроса, обсъждан и в решение Nacionalinis visuomenės sveikatos centras (вж. по-горе) дали трябва санкционираното нарушение на разпоредбите на ОРЗД да е извършено умишлено или по небрежност.

По въпроса за налагането на административни наказания по ОРЗД на юридически лица Съдът най-напред отбелязва, че предвидените в ОРЗД принципи, забрани и задължения са адресирани в частност до „администраторите“, а администраторите отговарят за всяко обработване на лични данни, извършено от тях или от тяхно име. В случай на нарушение по разпоредбите на ОРЗД именно тази отговорност е основанието за налагането на административно наказание на администратора съгласно член 83 от този регламент. Законодателят на Съюза обаче не е въвел разграничение между физическите и юридическите лица за целите на определянето на тази отговорност, а тя зависи единствено от условието тези лица, сами или съвместно с други, да определят целите и средствата за обработването на личните данни¹²². Следователно по принцип всяко лице, което отговаря на това условие, носи отговорност в частност за всяко извършено от него или от негово име нарушение на ОРЗД. Това означава, от една страна, че юридическите лица носят отговорност не само за нарушенията, извършени от техни представители, управители или ръководители, но и за нарушенията, извършени от всяко друго лице, което действа в рамките на търговската дейност на тези юридически лица и от тяхно име. От друга страна, административните наказания, предвидени в ОРЗД в случай на такива нарушения, трябва да може да се определят пряко на юридическите лица, ако същите могат да се окачествят като администратори на данни.

По-нататък Съдът отбелязва, че нито една от разпоредбите на ОРЗД не позволява да се приеме, че определянето на административно наказание на юридическо лице в качеството му на администратор зависи от условието преди това да е констатирано, че това нарушение е извършено от идентифицирано физическо лице. Освен това законодателят на Съюза не е оставил свобода на преценка на държавите членки в това отношение. Фактът, че ОРЗД предоставя на държавите членки възможността да предвидят изисквания относно процедурата, която трябва да следват надзорните органи при налагането на административни наказания¹²³, изобщо не означава, че те са овластени да предвиждат и допълнителни материалноправни условия свръх определените в ОРЗД.

¹²² Съгласно член 4, точка 7 от ОРЗД.

¹²³ Както следва от член 58, параграф 4 и член 83, параграф 8 от ОРЗД, разглеждани в светлината на съображение 129 от него.

В този контекст Съдът пояснява, че би било в противоречие с целта на ОРЗД да се допусне държавите членки едностранно да изискват като необходимо условие за налагането на административно наказание съгласно член 83 от ОРЗД на администратор — юридическо лице, преди това да е прието или да може да се приеме, че съответното нарушение е извършено от идентифицирано физическо лице. Освен това подобно допълнително изискване в крайна сметка би създадо риск от отслабване на ефективността и възпиращия ефект на административните наказания, налагани на юридически лица в качеството им на администратори.

Накрая, Съдът подчертава, че понятието „предприятие“ по смисъла на членове 101 и 102 ДФЕС¹²⁴ няма отражение върху това дали и при какви условия може да се наложи административно наказание съгласно ОРЗД на администратор — юридическо лице, а е релевантно единствено за целите на определянето на размера на административното наказание.

Затова Съдът стига до извода, че ОРЗД¹²⁵ не допуска национална правна уредба, съгласно която на юридическо лице в качеството му на администратор на данни може да се определи административно наказание за нарушение по този регламент¹²⁶ само ако преди това е прието, че нарушението е извършено от идентифицирано физическо лице.

Колкото до въпроса дали държавите членки могат да предвиждат налагане на административно наказание дори когато санкционираното нарушение не е извършено умишлено или по небрежност, Съдът най-напред припомня, че материалноправните условия, които трябва да съблюдава надзорният орган, когато налага административно наказание на администратора, се уреждат единствено от правото на Съюза, а държавите членки не разполагат с никаква свобода на действие в това отношение. По същите съображения като възприетите в посоченото по-горе решение *Nacionalinis visuomenės sveikatos centras* Съдът констатира, че съгласно член 83 от ОРЗД може да се наложи административно наказание само ако е установено, че администраторът, който е едновременно юридическо лице и предприятие, умишлено или по небрежност е извършил нарушение на съдържащите се в този регламент правила.

¹²⁴ Към който препраща съображение 150 от ОРЗД.

¹²⁵ Член 58, параграф 2, буква и) и член 83, параграфи 1—6 от ОРЗД.

¹²⁶ От посочените в член 83, параграфи 4—6 от ОРЗД.

5. Връзка на правомощията на националните надзорни органи с правомощията на другите национални органи

Решение от 4 юли 2023 г. (голям състав), Meta Platforms и др. (Общи условия за използване на социална мрежа) (C-252/21, [EU:C:2023:537](#))

По това дело (вж. също раздел V.5, „Обработване на лични данни в социални мрежи онлайн“), като се произнася относно правомощието на органа за защита на конкуренцията да констатира, че дадено обработване на лични данни не е в съответствие с ОРЗД, Съдът приема, че когато проверява дали дадено предприятие е извършило злоупотреба с господстващо положение¹²⁷, органът за защита на конкуренцията може — при спазване на задължението си за лоялно сътрудничество¹²⁸ с органите, които осъществяват надзор за защита на данните — да констатира, че общите условия за използване на това предприятие относно обработването на лични данни и прилагането на тези условия не са в съответствие с този регламент, щом тази констатация е необходима, за да се установи наличието на такава злоупотреба. Когато обаче в рамките на установяването на злоупотреба с господстващо положение разкрие нарушение на ОРЗД, органът за защита на конкуренцията не замества надзорните органи.

Така предвид принципа на лоялно сътрудничество, когато при упражняване на правомощията си трябва да проверят дали дадено поведение на предприятие е в съответствие с разпоредбите на ОРЗД, органите за защита на конкуренцията трябва да се съгласуват и да си сътрудничат лоялно със съответните национални надзорни органи или с водещия надзорен орган. При това положение всички тези органи са длъжни да се съобразят със съответните си правомощия и компетентности, за да се спазят задълженията, произтичащи от ОРЗД, и целите на този регламент, както и за да се запази полезният им ефект. Ето защо, когато при проверката дали предприятие е извършило злоупотреба с господстващо положение органът за защита на конкуренцията счита, че е необходимо да провери дали поведението на това предприятие е в съответствие с разпоредбите на ОРЗД, той трябва да провери дали това поведение или сходно поведение вече е било предмет на решение на компетентния национален надзорен орган или на водещия надзорен орган или пък на Съда. Ако е така, органът за защита на конкуренцията не може да дерогира това решение, но същевременно има свободата да направи собствените си изводи от гледна точка на прилагането на правото на конкуренция.

¹²⁷ Прогласено в член 4, параграф 3 ДЕС.

¹²⁸ По смисъла на член 102 ДФЕС.

Когато има съмнения за обхвата на преценката, извършена от компетентния национален надзорен орган или от водещия надзорен орган, когато съответното поведение или сходно поведение същевременно е предмет на разглеждане от тези органи или пък когато при липсата на разследване на посочените органи счита, че поведението на дадено предприятие не е в съответствие с разпоредбите на ОРЗД, органът за защита на конкуренцията трябва да се консултира с тези органи и да потърси сътрудничество с тях, за да разсее съмненията си или да изясни дали следва да изчака приемането на решение от съответния надзорен орган, преди сам да пристъпи към преценка. Ако те не възразят или не дадат отговор в разумен срок, органът за защита на конкуренцията може да продължи своето разследване.



СЪД
НА ЕВРОПЕЙСКИЯ СЪЮЗ

Дирекция „Изследвания и документация“

юли 2024 г.