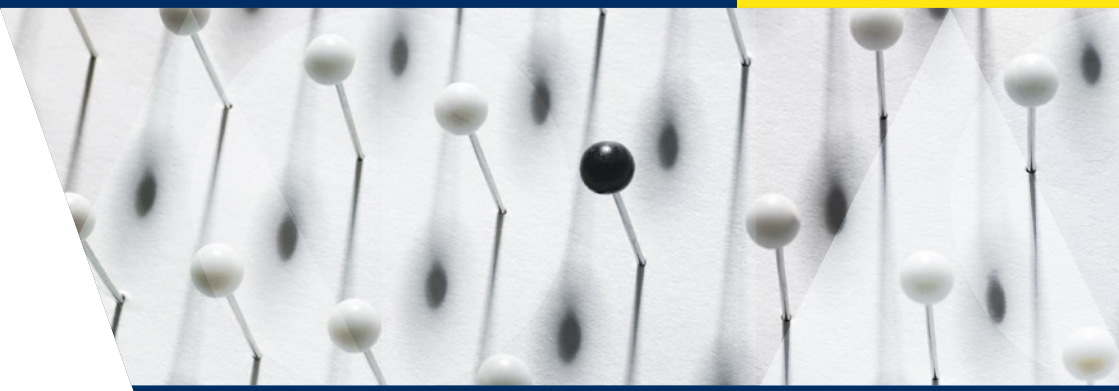
НАРЪЧНИК



Наръчник по европейско право в областта на защитата на данните

Издание 2018 г.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Ръкописът на този наръчник е завършен през април 2018 г.

Актуална информация ще бъде публикувана на сайта: fra.europa.eu; на страницата на Съвета на Европа: coe.int/dataprotection; сайта на Европейския съд по правата на човека в меню Case-Law (практическо право): echr.coe.int, и на Европейския надзорен орган за защита на данните: edps.europa.eu.

Снимки (корица и основно тяло): © iStockphoto

Люксембург: Служба за публикации на Европейския съюз, 2019 г.

CE:	ISBN 978-92-871-9836-5		
FRA – print:	ISBN 978-92-9474-299-5	doi:10.2811/7318	TK-05-17-225-BG-C
FRA – pdf:	ISBN 978-92-9474-293-3	doi:10.2811/850556	TK-05-17-225-BG-N

Оригиналът на този наръчник е на английски език. Съветът на Европа (СЕ) и Европейският съд по правата на човека (ЕСПЧ) не носят отговорност за качеството на превода от английски на други езици. Становищата, изразени в този наръчник, не са обвързващи за СЕ и ЕСПЧ. В наръчника има препратки към подбрани коментари и ръководства. СЕ и ЕСПЧ не носят отговорност за тяхното съдържание, нито включването на тези публикации в документа представлява някаква форма на реклама. Допълнителни публикации по темата можете да намерите на интернет страниците на библиотеката на ЕСПЧ на echr.coe.int/Library.

Съдържанието на настоящия наръчник не представлява официална позиция на Европейския надзорен орган по защита на данните (ЕНОЗД) и не го обвързва при упражняването на неговите компетенции. ЕНОЗД не поема отговорност за качеството на преводите на езици, различни от английски.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Наръчник по европейско право в областта на защитата на данните

Издание 2018 г.

Предговор

Съвременното общество е в непрекъснат процес на цифровизация. Темповете на технологично развитие и начините на обработка на лични данни оказват влияние върху живота на всеки от нас ежедневно и по различни начини в контекста на тези промени. Наскоро бяха преразгледани правните рамки на Европейския съюз (ЕС) и Съвета на Европа, гарантиращи правото на неприкосновеност на личния живот и личните данни.

Европа има водеща позиция в света по отношение на защитата на данните. Стандартите на ЕС в тази област се основават на Конвенция № 108 на Съвета на Европа, на правните актове на ЕС — включително Общия регламент относно защитата на данните и Директивата за защита на данните, обработвани от органите на полицията и наказателното правосъдие — и на съответната съдебна практика на Европейския съд по правата на човека и Съда на Европейския съюз.

Осъществените от ЕС и Съвета на Европа реформи в областта на защитата на данните са всеобхватни и в определени отношения — сложни, а ползите се простират в широк мащаб и засягат както отделните лица, така и предприятията. Целта на настоящия наръчник е да повиши осведомеността и знанията за правилата за защита на данните, особено сред неспециализираните в областта юристи, които се занимават в работата си с въпроси във връзка със защитата на данните.

Наръчникът е съставен от Агенцията на ЕС за основните права (FRA) съвместно със Съвета на Европа (заедно със Секретариата на Европейския съд по правата на човека) и Европейския надзорен орган по защита на данните. Той актуализира изданието от 2014 г. и представлява част от правните наръчници, изготвяни съвместно от FRA и Съвета на Европа.

Изразяваме благодарност към органите за защита на данните в Белгия, Естония, Франция, Грузия, Унгария, Ирландия, Италия, Монако, Швейцария и Обединеното кралство за полезните им коментари върху работната версия на наръчника. Също така изказваме признателност на отдела за защита

на данните и отдела за международни потоци от данни и правна защита към Европейската комисия. Благодарим за съдействието на Съда на Европейския съюз, който ни предостави документи по време на подготвителната работа върху наръчника.

Christos Giakoumopoulos

Генерален директор по правата на човека и върховенството на закона на Съвета на Европа

Giovanni Buttarelli

Европейски надзорен орган по защита на данните

Michael O'Flaherty

Директор на Агенцията на Европейския съюз за основните права

Съдържание

Съкращения и акроними

BCR	Задължителни фирмени правила
CCTV	Вътрешна система за видеонаблюдение
CETS	Поредица договори на Съвета на Европа
CRM	Управление на връзките с клиенти
ENISA	Агенция на Европейския съюз за мрежова и информационна сигурност
EPPO	Европейска прокуратура
ESMA	Европейски орган за ценни книжа и пазари
eTEN	Трансевропейски телекомуникационни мрежи
EuroPriSe	Европейски печат за неприкосновеност на личния живот
eu-LISA	Агенция на ЕС за широкомащабни информационни системи
FRA	Агенция на Европейския съюз за основните права
GPS	Глобална система за определяне на местоположението
ISP	Доставчик на интернет услуги
PIN	Персонален идентификационен номер
PNR	Резервационни данни на пътниците
SWIFT	Дружество за световни междубанкови финансови телекомуникации
ВДПЧ	Всеобща декларация за правата на човека
ВИС	Визова информационна система
ДЕС	Договор за Европейския съюз
ДЛЗД	Длъжностно лице за защита на данните
ДФЕС	Договор за функционирането на Европейския съюз
ЕАСТ	Европейска асоциация за свободна търговия
ЕЗА	Европейска заповед за арест
ЕЗПЕ	Единна зона за плащания в евро
ЕИП	Европейско икономическо пространство
ЕКЗД	Европейски комитет по защита на данните
ЕКПЧ	Европейска конвенция за защита на правата на човека
ЕНОЗД	Европейски надзорен орган по защита на данните

ЕО	Европейска общност
ЕОБХ	Европейски орган за безопасност на храните
ЕС	Европейски съюз
ЕСПЧ	Европейски съд по правата на човека
ИКТ	Информационни и комуникационни технологии
КГН	Координационна група за надзор
Конвенция № 108	Конвенция (на Съвета на Европа) за защита на лицата при автоматизираната обработка на лични данни Протоколът за изменение (CETS No. 223) на Конвенция № 108 („модернизирана Конвенция № 108“) беше приет от Комитета на министрите на Съвета на Европа по повод на неговото 128-о заседание, проведено в гр. Елсинор, Дания (17-18 май 2018 г.). Препратките в текста „модернизирана Конвенция № 108“ се отнасят за конвенцията, както е изменена с Протокол CETS No. 223.
МИС	Митническа информационна система
МПГПП	Международен пакт за граждански и политически права
НЗЕ	Национално звено на Европол
НПО	Неправителствена организация
Н-ШИС	Национална Шенгенска информационна система
ОВ	Официален вестник
ОЗД	Орган за защита на данните
ОИСР	Организация за икономическо сътрудничество и развитие
ООН	Организация на обединените нации
ОРЗД	Общ регламент относно защитата на данните
СЕ	Съвет на Европа
СНО	Съвместен надзорен орган
Съд на ЕС	Съд на Европейския съюз (преди декември 2009 г. наричан Съд на Европейските общности — СЕО)
Хартата	Харта на основните права на Европейския съюз
Ц-ШИС	Централна Шенгенска информационна система
ШИС	Шенгенска информационна система

Как да се използва този наръчник

В наръчника се съдържа преглед на правните норми, свързани със защитата на данните, определени от Европейския съюз (ЕС) и Съвета на Европа (СЕ). Той е предназначен да помага на практикуващите юристи, които не са специализирани в областта на защитата на данните, включително адвокати, съдии и други практикуващи юристи, както и на работещите за други органи, например неправителствени организации (НПО), които може да се сблъскат с правни въпроси, свързани със защитата на данните.

Наръчникът служи като първа отправна точка за справки по отношение на свързаното право на ЕС и Европейската конвенция за правата на човека (ЕСПЧ), както и Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108) и други инструменти на Съвета на Европа.

Всяка глава започва с таблица, в която са посочени приложимите правни разпоредби по отношение на темите, разглеждани във всяка конкретна глава. Таблиците обхващат както правото на Съвета на Европа, така и правото на ЕС и включват избрана съдебна практика на Европейския съд по правата на човека (ЕСПЧ) и Съда на Европейския съюз (Съда на ЕС). След това съответните закони на тези две различни европейски уредби са представени един след друг, в зависимост от приложимостта им спрямо конкретната разглеждана тема. Това дава възможност на читателя да види къде двете правни системи съвпадат и в кои аспекти се различават. Това би следвало също така да помогне на читателите да намерят основната информация, отнасяща се до тяхното положение, особено ако спрямо тях се прилага само правото на Съвета на Европа. В някои глави подреждането на темите в таблиците може леко да се различава от тяхното подреждане в рамките на самата глава, ако това спомага за сбитото представяне на съдържанието. В наръчника е представен и кратък преглед на рамката на ООН.

Практикуващите юристи в държави извън ЕС, които са държави — членки на Съвета на Европа, и страни по ЕКПЧ и Конвенция № 108, могат да имат достъп до информацията, приложима за тяхната собствена държава, като отидат направо на разделите относно Съвета на Европа. Практикуващите юристи в държави извън ЕС трябва също така да имат предвид, че след приемането на европейския Общ регламент относно защитата на данните правилата на ЕС за защита на данните се прилагат за организации и други субекти, които не са установени в ЕС, ако същите обработват лични данни и предлагат стоки

и услуги на субекти на данни в Съюза или наблюдават поведението на такива субекти на данни.

Практикуващите юристи в държавите членки на ЕС ще трябва да използват и двата раздела, тъй като тези държави са обвързани и с двете правни уредби. Следва да се отбележи, че реформите и модернизацията на правилата за защита на данните в Европа, предприети в рамките както на Съвета на Европа (модернизирана Конвенция № 108, както беше изменена с Протокол CETS No. 223), така и на ЕС (приемането на Общия регламент относно защитата на данните и на Директива 2016/680/ЕС), бяха проведени успоредно. Регулаторните органи в двете правни системи положиха всички усилия, за да гарантират последователност и съвместимост между двете правни рамки. По този начин реформите доведоха до по-голяма хармонизация между правото за защита на данните на Съвета на Европа и на ЕС. Читателите, които се нуждаят от повече информация по конкретен въпрос, могат да намерят списък с по-специализирани материали в раздела „Допълнителна литература“. За информация относно разпоредбите на Конвенция № 108 и нейния допълнителен Протокол от 2001 г., които продължават да се прилагат до влизането в сила на Протокола за изменение, читателите трябва да се запознят с версията на Наръчника от 2014 г.

Правото на Съвета на Европа е представено чрез кратки препратки към определени дела на ЕСПЧ. Те са избрани сред големия брой съдебни решения на ЕСПЧ по въпроси, свързани със защитата на данните.

Свързаното право на ЕС се състои от приети законодателни мерки, от съответните разпоредби на Договорите и от Хартата на основните права на Европейския съюз съгласно тълкуването, наложено в съдебната практика на Съда на ЕС. Освен това наръчникът представя становищата и насоките, приети от Работната група по член 29 — консултативния орган, натоварен от Директивата за защита на личните данни със задачата да предоставя експертни съвети на държавите членки на ЕС, който след 25 май 2018 г. ще бъде заменен от Европейския комитет по защита на данните (ЕКЗД). Становищата на Европейския надзорен орган по защита на данните също предоставят важна информация относно тълкуването на правото на ЕС и поради тази причина са включени в настоящия наръчник.

Делата, описани или цитирани в настоящия наръчник, представят примери за важна част от съдебната практика както на ЕСПЧ, така и на Съда на ЕС.

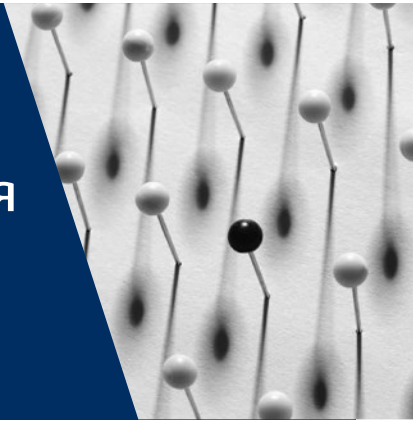
Насоките в края на наръчника са предназначени да помогнат на читателя в търсенето на съдебна практика онлайн. Представената съдебна практика на Съда на ЕС е свързана с предходната Директива за защита на личните данни. Тълкуванията на Съда на ЕС обаче продължават да са валидни за съответните права и задължения, установени от Общия регламент относно защитата на данните.

В допълнение в текстови карета, оцветени в синьо, са представени практически примери с хипотетични сценарии. Те допълнително илюстрират прилагането на практика на европейските правила за защита на данните, по-специално когато по темата не съществува конкретна съдебна практика на ЕСПЧ или на Съда на ЕС. В другите текстови карета, оцветени в сиво, са представени примери от източници, различни от съдебната практика на ЕСПЧ и Съда на ЕС, например законодателни актове и становища, издадени от Работната група по член 29.

Наръчникът започва с кратко описание на ролята на двете правни системи, както са определени от ЕКПЧ и правото на ЕС (глава 1). Глави 2—10 обхващат следните въпроси:

- терминологията в областта на защитата на данните;
- основните принципи на европейското право в областта на защитата на данните;
- правилата на европейското право в областта на защитата на данните;
- независимия надзор;
- правата на субектите на данни и тяхното прилагане;
- трансграничното прехвърляне и предоставяне на лични данни;
- защитата на данните в контекста на полицията и наказателното правосъдие;
- други европейски правила за защита на данните в конкретни области;
- съвременните предизвикателства в областта на защитата на личните данни.

1 Контекст и предистория на европейското право в областта на защитата на данните



ЕС	Обхванати въпроси	СЕ
Правото на защита на данните		
Договор за функционирането на Европейския съюз, член 16 Харта на основните права на Европейския съюз (Хартата), член 8 (правото на защита на личните данни) Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (Директива за защита на личните данни), ОВ L 281, 23.11.1995 г. (в сила до май 2018 г.) Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, ОВ L 350, 30.12.2008 г. (в сила до май 2018 г.) Регламент (ЕС) 2016/679 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 (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016 г.		ЕКПЧ, член 8 (право на зачитане на личния и семейния живот, на жилището и на тайната на кореспонденцията) Модернизирана Конвенция за защита на лицата при автоматизираната обработка на лични данни (модернизирана Конвенция № 108)

ЕС	Обхванати въпроси	СЕ
Директива (ЕС) 2016/680 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 (Директива за защита на данните, обработвани от полицейските и наказателноправните органи), ОВ L 119, 4.5.2016 г. Директива 2002/58/ЕО 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 електронни комуникации), ОВ L 201, 31.7.2002 г. Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (Регламент относно защитата на данните при обработването им от институции на ЕС), ОВ L 8, 12.1.2001 г.		
Ограничения на правото на защита на личните данни		
Хартата, член 52, параграф 1 Общ регламент относно защитата на данните, член 23 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 2010 г.		ЕКПЧ, член 8, параграф 2 Модернизирана Конвенция № 108, член 11 ЕСПЧ, *S. u Marper/ Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 2008 г.
Балансиране на правата		
Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 2010 г.	**Общо по въпросите**	

ЕС	Обхванати въпроси	СЕ
Съд на ЕС, C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy u Satamedia Oy* [голям състав], 2008 г. Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 2014 г.	Свобода на изразяване на мнение	ЕСПЧ, *Axel Springer AG/Германия* [голям състав], № 39954/08, 2012 г. ЕСПЧ, *Mosley/ Обединеното кралство*, № 48009/08, 2011 г. ЕСПЧ, *Bohlen/Германия*, № 53495/09, 2015 г.
Съд на ЕС, C-28/08 P *Европейска комисия/ The Bavarian Lager Co. Ltd.* [голям състав], 2010 г. Съд на ЕС, C-615/13P, *ClientEarth, PAN Europe/ЕОБХ*, 2015 г.	Достъп до документи	ЕСПЧ, *Magyar Helsinki Bizottság/Унгария* [голям състав], № 18030/11, 2016 г.
Общ регламент относно защитата на данните, член 90	Професионална тайна	ЕСПЧ, *Pruteanu/Румъния*, № 30181/05, 2015 г.
Общ регламент относно защитата на данните, член 91	Свобода на религията или убеждения	
	Свобода на изкуствата и науките	ЕСПЧ, *Vereinigung bildender Künstler/ Австрия*, № 68354/01, 2007 г.
Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 2008 г.	Защита на собствеността	
Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 2014 г. Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ Salvatore Manni*, 2017 г.	Икономически права	

1.1 Правото на защита на личните данни

Ключови въпроси

- Съгласно член 8 от ЕКПЧ правото на лицата на защита във връзка с обработването на лични данни е част от правото на зачитане на личния и семейния живот, на жилището и тайната на кореспонденцията.

- Конвенция № 108 на Съвета на Европа е първият и за момента единственият международен правно обвързващ инструмент, в който се разглежда защитата на данните. Конвенцията премина през процес на модернизация, приключил с приемането на Протокол за изменение CETS No. 223.
- Съгласно правото на ЕС защитата на данните е призната като отделно основно право. Това право е потвърдено в член 16 от Договора за функционирането на ЕС, както и в член 8 от Хартата на основните права на Европейския съюз.
- В рамките на правото на ЕС защитата на данните е уредена за първи път в Директивата за защита на личните данни през 1995 г.
- С оглед на бързото развитие на технологиите, през 2016 г. ЕС прие ново законодателство, за да адаптира правилата за защита на данните към цифровата ера. Общият регламент относно защитата на данните е приложим от май 2018 г., като отменя Директивата за защита на личните данни.
- Заедно с Общия регламент относно защитата на данните ЕС прие законодателство относно обработването на лични данни от държавните органи за целите на правоприлагането. Директива (ЕС) 2016/680 установява правилата и принципите за защита на данните, които регламентират обработването на лични данни за целите на предотвратяването, разследването, разкриването и наказателното преследване на престъпления или прилагането на наказания за извършени престъпления.

1.1.1 Правото на зачитане на личния живот и правото на защита на личните данни: кратко встъпление

Макар и тясно свързани, правото на зачитане на личния живот и правото на защита на личните данни са отделни права. Правото на неприкосновеност на личния живот, наричано в европейското право право на зачитане на личния живот, се появява в международното право, регламентиращо правата на човека, а именно във Всеобщата декларация за правата на човека (ВДПЧ), приета през 1948 г., като едно от основните защитени права на човека. Скоро след приемането на ВДПЧ Европа също потвърди това право в Европейската конвенция за правата на човека (ЕКПЧ) — договор, който е със задължителен характер за договарящите се страни по него и който беше изготвен през 1950 г. ЕКПЧ предвижда, че всеки човек има право на зачитане на личния и семейния живот, на жилището и тайната на кореспонденцията. Намесата в това право от страна на публичните органи е забранена, освен когато е в съответствие със закона, преследва важни и законни обществени интереси и е необходима в едно демократично общество.

ВДПЧ и ЕКПЧ бяха приети много преди развитието на компютрите и интернет и възхода на информационното общество. Тези събития донесоха значителни предимства на хората и на обществото, като подобриха качеството на живот, ефективността и производителността. В същото време те създават нови рискове за правото на зачитане на личния живот. В отговор на нуждата от специални правила, регламентиращи събирането и използването на лична информация, възникна ново понятие за неприкосновеност, известно в някои юрисдикции като „неприкосновеност на личната информация", а в други като „право на информационно самоопределение"[1]. Това понятие доведе до създаването на специални правни уредби, осигуряващи защита на личните данни.

Защитата на личните данни в Европа започна през 70-те години на XX век с приемането (от някои държави) на законодателство с цел упражняване на контрол върху обработването на лична информация от публични органи и големи дружества[2]. Впоследствие бяха приети инструменти за защита на данните на европейско равнище[3] и през годините защитата на личните данни се превърна в самостоятелна ценност, отделна от правото на зачитане на личния живот. В правния ред на ЕС защитата на личните данни е призната за основно право, отделно от основното право на зачитане на личния живот. Това разделение поражда въпроса за връзката и различията между тези две права.

Правото на зачитане на личния живот и правото на защита на личните данни са тясно свързани. И двете са насочени към защитата на сходни ценности, т.е. независимостта и човешкото достойнство на хората, като им предоставят

1 Германският федерален конституционен съд потвърди правото на информационно самоопределение в решение от 1983 г. по дело *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Съдът приема, че информационното самоопределение произтича от основното право на зачитане на неприкосновеността на личността, защитено в германската конституция. В решение от 2017 г. ЕСПЧ признава, че член 8 от ЕКПЧ „предвижда правото на някаква форма на информационно самоопределение". Вж. ЕСПЧ, *Satakunnan Markkinapörssi Oy и Satamedia Oy/Финландия* [голям състав], № 931/13, 27 юни 2017 г., параграф 137.

2 Германската провинция Хесен прие първия закон за защита на данните през 1970 г.; той се прилага само в тази провинция. През 1973 г. Швеция прие първия в света национален закон за защита на данните. До края на 80-те години на XX век няколко европейски държави (Франция, Германия, Нидерландия и Обединеното кралство) също приеха законодателство относно защитата на данните.

3 През 1981 г. беше приета Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108). През 1995 г. ЕС прие своя първи всеобхватен инструмент за защита на данните — Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

лично пространство, в което те могат свободно да развиват личността си, да мислят и да си създават собствено мнение. Ето защо те са изключително важна предпоставка за упражняването на други основни свободи, като свободата на изразяване на мнение, свободата на мирни събрания и на сдружаване и свободата на религията.

Двете права се различават по своята формулировка и обхват. Правото на зачитане на личния живот се състои от обща забрана за намеса, като се вземат предвид определени критерии за обществен интерес, които могат да оправдаят намеса в конкретни случаи. Защитата на личните данни се счита за съвременно и активно право[4], с което се въвеждат принципите на взаимозависимост и взаимоограничаване на законодателната, изпълнителната и съдебната власт, така че физическите лица да бъдат защитени винаги когато се обработват техни лични данни. Обработването трябва да е съобразено с основните компоненти в областта на защитата на личните данни, а именно независимия надзор и зачитането на правата на субекта на данни[5].

Член 8 от Хартата на основните права на ЕС (Хартата) не само утвърждава правото на защита на личните данни, но също така определя основните ценности, свързани с това право. Той предвижда, че обработването на личните данни трябва да бъде добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго определено от закона легитимно основание. Лицата трябва да имат право на достъп до личните си данни, както и правото да изискат коригирането им, като спазването на това право подлежи на контрол от независим орган.

Правото на защита на личните данни влиза в действие винаги когато се обработват лични данни; следователно то е по-обширно от правото на зачитане на личния живот. Всяка операция по обработване на лични данни е предмет на подходяща защита. Защитата на личните данни се отнася за всички видове лични данни и тяхното обработване, без значение от връзката и отражението върху неприкосновеността на личния живот. Обработването на лични данни също така може да наруши правото на неприкосновеност на личния живот,

4 Генерален адвокат Sharpston описва делото като включващо две отделни права: „класическото" право на защита на личния живот и „по-съвременно" — правото на защита на данните. Вж. Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen*, *Заключение на генерален адвокат Sharpston*, 17 юни 2010 г., параграф 71.

5 Hustinx, P., Изказвания и статии на ЕНОЗД, *EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, юли 2013 г.

както е показано в примерите по-долу. Не е необходимо обаче да е налице нарушение на неприкосновеността на личния живот, за да се задействат правилата за защита на личните данни.

Правото на неприкосновеност на личния живот се отнася за ситуации, при които личният интерес или „личният живот" на лицата е изложен на риск. Както е показано в настоящия наръчник, понятието за „личен живот" се тълкува широко в съдебната практика като покриващо интимни ситуации, чувствителна или поверителна информация, информация, която може да доведе до предубедено възприемане на дадено лице от обществото и дори аспекти от професионалния живот и общественото поведение на дадено лице. Преценката дали има или е имало намеса в „личния живот" обаче зависи от контекста и фактите по всеки случай.

От друга страна, всяка операция, включваща обработване на лични данни, може да попадне в обхвата на правилата за защита на личните данни и да задейства правото на защита на личните данни. Например когато работодател документира информация, отнасяща се до имената и възнагражденията, плащани на служителите, самото документиране на тази информация не може да се счита за намеса в личния живот. За такава намеса обаче може да се говори, ако например работодателят предостави „личната информация" за служителите на трети страни. Работодателите трябва във всеки случай да спазват правилата за защита на личните данни, защото документирането на информация относно служителите представлява обработване на лични данни.

Пример: По делото *Digital Rights Ireland*[6] Съдът на ЕС беше призован да се произнесе относно валидността на Директива 2006/24/ЕО в светлината на основните права на защита на личните данни и зачитане на личния живот, утвърдени в Хартата на основните права на ЕС. Директивата изисква доставчиците на обществено достъпни електронни съобщителни услуги или обществени съобщителни мрежи да запазват телекомуникационни данни на гражданите за период до две години, за да се осигури съществуването на данните за целите на предотвратяването, разследването и съдебното преследване на

6 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

сериозни престъпления. Мярката се отнася само за метаданни, данни за местоположението и данни, необходими за идентифицирането на абонат или ползвател. Тя не е приложима за съдържанието на електронните съобщения.

Съдът на ЕС приема, че директивата представлява намеса в основното право на защита на личните данни, „тъй като тя предвижда обработка на лични данни“[7]. Освен това той констатира, че директивата представлява намеса в правото на личен живот[8]. Когато бъдат разгледани в съвкупност, от тези лични данни, запазени в съответствие с директивата, до които компетентните органи имат достъп, е възможно „да се изведат много точни заключения за личния живот на лицата, чиито данни са били запазени, например относно навиците им в ежедневния живот, мястото на постоянно или временно пребиваване, ежедневните им или други пътувания, упражняваните дейности, социалните връзки на тези лица и социалните кръгове, в които се движат“[9]. Намесата в тези две права е особено обширна и тежка.

Съдът на ЕС обявява Директива 2006/24/ЕО за невалидна, като констатира, че макар и тя да преследва легитимна цел, намесата в правото на защита на личните данни и правото на неприкосновеност на личния живот е тежка и не се ограничава до строго необходимото.

1.1.2 Международна правна рамка: Организация на обединените нации

В рамката на Организацията на обединените нации защитата на личните данни не се признава за основно право, макар че правото на неприкосновеност на личния живот е трайно утвърдено основно право в международния правен ред. В член 12 от ВДПЧ относно неприкосновеността на личния и семейния живот[10] за първи път се залага правото на защита на личното пространство на физическите лица срещу намеса от страна на другите,

7 *Пак там*, параграф 36.

8 *Пак там*, параграфи 32–35.

9 *Пак там*, параграф 27.

10 Организация на обединените нации (ООН), Всеобща декларация за правата на човека (ВДПЧ), 10 декември 1948 г.

особено от страна на държавата. Макар и да е необвързваща декларация, ВДПЧ има важен статут като основополагащ инструмент в международното право в областта на правата на човека и оказа влияние върху развитието на другите инструменти в областта на правата на човека в Европа. Международният пакт за граждански и политически права (МПГПП) влиза в сила през 1976 г. Той постановява, че никой не може да бъде обект на своеволно и незаконно вмешателство в личния му живот, дома или кореспонденцията му, нито на незаконно накърняване на неговата чест и добро име. МПГПП е международен договор, който ангажира подписалите го 169 страни да зачитат и гарантират упражняването на гражданските права на физическите лица, включително правото на неприкосновеност на личния живот.

След 2013 г. Организацията на обединените нации прие две резолюции по въпросите на неприкосновеността на личния живот, озаглавени „правото на неприкосновеност на личния живот в цифровата ера“[11], в отговор на развитието на новите технологии и на разкритията относно масовото наблюдение, предприето в някои държави (разкритията на Сноудън). В тях се осъжда категорично масовото наблюдение и се подчертава въздействието, което такова наблюдение може да окаже върху основните права на неприкосновеност на личния живот и свобода на изразяване на мнение, както и върху функционирането на жизнеспособно и демократично общество. Макар и да не са правно обвързващи, те предизвикаха важен международен политически дебат на високо равнище относно неприкосновеността на личния живот, новите технологии и наблюдението. Те доведоха и до определянето на специален докладчик за правото на неприкосновеност на личния живот, с мандат да насърчава и защитава това право. Конкретните задачи на докладчика включват събирането на информация относно националните практики и опит във връзка с неприкосновеността на личния живот и предизвикателствата, породени от новите технологии, обмена и насърчаването на най-добрата практика, и установяването на възможните пречки.

Докато предишните резолюции бяха съсредоточени върху отрицателните последици от масовото наблюдение и върху отговорността на държавите да ограничават правомощията на разследващите органи, последните резолюции отразяват ключово развитие на дебата в Организацията на обединените

11 Вж. ООН, Генерална асамблея, Резолюция относно правото на неприкосновеност на личния живот в цифровата ера, A/RES/68/167, Ню Йорк, 18 декември 2013 г.; и ООН, Генерална асамблея, Преразгледана проектрорезолюция относно правото на неприкосновеност на личния живот в цифровата ера, A/C.3/69/L.26/Rev.1, Ню Йорк, 19 ноември 2014 г.

нации относно неприкосновеността на личния живот[12]. В приетите през 2016 и 2017 г. резолюции се потвърждава необходимостта от ограничаване на прамощията на разузнавателните агенции и се осъжда масовото наблюдение. В същото време обаче в тях изрично се посочва, че „увеличаващите се възможности на стопанските предприятия да събират, обработват и използват лични данни могат да представляват риск за упражняването на правото на неприкосновеност на личния живот в цифровата ера". Ето защо в допълнение към отговорността на държавните органи в резолюциите се посочва и отговорността на частния сектор да зачита правата на човека, а дружествата се призовават да уведомяват потребителите относно събирането, използването, споделянето и задържането на лични данни и да установяват прозрачни политики за обработване на данните.

1.1.3 Европейската конвенция за защита на правата на човека

Съветът на Европа беше създаден след края на Втората световна война, за да обедини европейските държави с цел насърчаване на върховенството на закона, демокрацията, правата на човека и социалното развитие. За тази цел през 1950 г. той прие ЕКПЧ, която влезе в сила през 1953 г.

Договарящите се страни са поели международно задължение да спазват ЕКПЧ. Всички държави членки на Съвета на Европа вече са включили или са привели в действие ЕКПЧ в своето национално законодателство, което изисква от тях да действат в съответствие с разпоредбите на Конвенцията. Договарящите се страни трябва да зачитат предвидените в конвенцията права, когато упражняват някаква дейност или правомощие. Това включва дейностите, предприети за целите на националната сигурност. Няколко принципни решения на Европейския съд по правата на човека (ЕСПЧ) са свързани с дейности на държавните органи в чувствителни области на правото и практиката относно националната сигурност[13]. Съдът няма никакви колебания, че

12 ООН, Генерална асамблея, Преразгледана проекторезолюция относно правото на неприкосновеност на личния живот в цифровата ера, A/C.3/71/L.39/Rev.1, Ню Йорк, 16 ноември 2016 г.; ООН, Съвет на по правата на човека, Правото на неприкосновеност на личния живот в цифровата ера, A/HRC/34/L.7/Rev.1, 22 март 2017 г.

13 Вж. например: ЕСПЧ, *Klass и други/Германия*, № 5029/71, 6 септември 1978 г.; ЕСПЧ, *Rotaru/Румъния* [голям състав], № 28341/95, 4 май 2000 г.; и ЕСПЧ, *Szabó и Vissy/Унгария*, № 37138/14, 12 януари 2016 г.

дейностите по наблюдение представляват намеса в правото на зачитане на личния живот[14].

За да се гарантира, че договарящите се страни спазват задълженията си съгласно ЕКПЧ, през 1959 г. беше създаден ЕСПЧ в Страсбург, Франция. ЕСПЧ гарантира, че държавите спазват своите задължения съгласно Конвенцията, като разглежда жалби от лица, групи лица, НПО или юридически лица относно предполагаеми нарушения на Конвенцията. ЕСПЧ може също така да разглежда междудържавни дела, заведени от една или повече държави членки на Съвета на Европа срещу друга държава членка.

Към 2018 г. Съветът на Европа включва 47 договарящи се страни, 28 от които са също и държави членки на ЕС. Не е необходимо жалбоподателят пред ЕСПЧ да бъде гражданин на някоя от договарящите се страни, въпреки че предполагаемите нарушения трябва да са извършени в рамките на юрисдикцията на някоя от тях.

Правото на защита на личните данни е част от правата, защитени съгласно член 8 от ЕКПЧ, който гарантира правото на зачитане на личния и семейния живот, на жилището и кореспонденцията и определя условията, при които се допускат ограничения на това право[15].

ЕСПЧ е разгледал много ситуации, засягащи проблеми в областта на защитата на данните. Те са свързани с прихващането на комуникации[16], с различни форми на наблюдение от страна както на частния, така и на публичния сектор[17] и със защитата срещу съхраняването на лични данни от публичните органи[18]. Правото на зачитане на личния живот не е абсолютно право, понеже упражняването на правото на неприкосновеност на личния живот би могло да изложи на риск други права, като например свободата на изразяване на мнение и достъпа до информация и обратно. Поради това Съдът се стреми да

14 *Пак там*.

15 Съвет на Европа, Европейска конвенция за защита на правата на човека, CETS № 005, 1950 г.

16 Вж. например: ЕСПЧ, *Malone/Обединеното кралство*, № 8691/79, 2 август 1984 г.; ЕСПЧ, *Copland/Обединеното кралство*, № 62617/00, 3 април 2007 г.; или ЕСПЧ, *Mustafa Sezgin Tanrıkulu/Турция*, № 27473/06, 18 юли 2017 г.

17 Вж. например: ЕСПЧ, *Klass и други/Германия*, № 5029/71, 6 септември 1978 г.; ЕСПЧ, *Uzun/Германия*, № 35623/05, 2 септември 2010 г.

18 Вж. например: ЕСПЧ, *Roman Zakharov/Русия* [голям състав], № 47143/06, 4 декември 2015 г.; ЕСПЧ, *Szabó и Vissy/Унгария*, № 37138/14, 12 януари 2016 г.

намери баланс между въпросните различни права. Той е разяснил, че член 8 от ЕКПЧ не само задължава държавите да се въздържат от всякакви действия, които биха могли да нарушат това предвидено в Конвенцията право, но и че при определени обстоятелства те имат и положителни задължения активно да гарантират ефективното зачитане на личния и семейния живот[19]. Много от тези дела ще бъдат разгледани подробно в съответните глави.

1.1.4 Конвенция № 108 на Съвета на Европа

С появата на информационните технологии през 60-те години на XX в. нараства необходимостта от по-подробни правила за защита на физическите лица чрез защита на техните (лични) данни. До средата на 70-те години на XX в. Комитетът на министрите на Съвета на Европа прие различни резолюции относно защитата на личните данни, позовавайки се на член 8 от ЕКПЧ[20]. През 1981 г. беше открита за подписване Конвенцията за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108)[21]. Конвенция № 108 беше и все още продължава да бъде единственият правно обвързващ международен инструмент в областта на защитата на данните.

Конвенция № 108 се прилага за цялостната обработка на данни, извършена в частния и публичния сектор, в т.ч. обработката на данни от съдебни и правоприлагащи органи. Тя защитава лицата срещу злоупотреби, които може да съпровождат обработването на личните данни, и едновременно с това има за цел да регулира трансграничното предоставяне на лични данни. По отношение на обработването на лични данни установените в Конвенцията принципи се отнасят по-специално до добросъвестното и законосъобразното събиране и автоматично обработване на данни, съхранявани за определени легитимни цели. Това означава, че данните не следва да се използват за други несъвместими с тях цели, нито да се съхраняват за по-дълъг срок, отколкото е необходимо. Тези принципи също така се отнасят до качеството на данните, по-специално до това, че данните трябва да бъдат достатъчни,

19 Вж. например: ЕСПЧ, *I/Финландия*, № 20511/03, 17 юли 2008 г.; ЕСПЧ, *K.U./Финландия*, № 2872/02, 2 декември 2008 г.

20 Съвет на Европа, Комитет на министрите (1973 г.), Резолюция (73) 22 относно защитата на неприкосновеността на личния живот на лицата по отношение на електронните бази от данни в частния сектор, 26 септември 1973 г.; Съвет на Европа, Комитет на министрите (1974 г.), Резолюция (74) 29 относно защитата на неприкосновеността на личния живот на лицата по отношение на електронните бази от данни в публичния сектор, 20 септември 1974 г.

21 Съвет на Европа, Конвенция за защита на лицата при автоматизираната обработка на лични данни, Съвет на Европа, CETS № 108, 1981 г.

релевантни, точни и да не бъдат прекомерни спрямо целта (принципа за пропорционалност).

В допълнение към предоставянето на гаранции по отношение на обработването на лични данни и налагането на задължения за сигурност на данните Конвенцията забранява, при липсата на подходящи правни гаранции, обработването на „чувствителни" данни, като например данни относно расата, политическите възгледи, здравословното състояние, религията, сексуалния живот или съдебното досие на дадено лице.

Конвенцията също така утвърждава правото на лицето да бъде осведомено, че за него се съхранява информация и, при необходимост, да поиска нейното коригиране. Ограничаване на правата, гарантирани от Конвенцията, са възможни само при необходимост от защита на по-значими интереси, свързани например със защитата на държавната сигурност и отбраната. В допълнение Конвенцията гарантира свободното движение на лични данни между договарящите се страни и налага някои ограничения върху потоците от данни към държави, в които правната уредба не предоставя равностойна защита.

Следва да се отбележи, че Конвенция № 108 е задължителна за държавите, които са я ратифицирали. Тя не подлежи на съдебен надзор от ЕСПЧ, но се взема под внимание в съдебната практика на ЕСПЧ в контекста на член 8 от ЕКПЧ. През годините Съдът постановява, че защитата на личните данни е важна част от правото на зачитане на личния живот (член 8) и се ръководи от принципите на Конвенция № 108, когато определя дали е налице намеса в това основно право[22].

С цел по-нататъшно развиване на общите принципи и правила, установени в Конвенция № 108, Комитетът на министрите на Съвета на Европа прие няколко препоръки, които не са със задължителен характер. Тези препоръки оказаха влияние върху развитието на законодателството в областта на защитата на личните данни в Европа. Например в продължение на години единственият инструмент в Европа, който даваше насоки за използването на лични данни в сектора на полицията, беше Препоръката за сектора на полицията[23]. Принципите, съдържащи се в препоръката, като например начините

22 Вж. например: ЕСПЧ, *Z/Финландия*, № 22009/93, 25 февруари 1997 г.

23 Съвет на Европа, Комитет на министрите (1987 г.), Препоръка Rec(87)15 до държавите членки за уреждане на използването на лични данни в сектора на полицията, 17 септември 1987 г.

на запазване на файловете с данни и нуждата от прилагане на ясни правила по отношение на лицата, на които е разрешен достъп до тези файлове, бяха допълнително развити и отразени в последващото законодателство на ЕС[24]. По-скорошните препоръки се стремят да отговорят на предизвикателствата на цифровата ера – например относно обработването на лични данни в областта на заетостта (вж. глава 9).

Всички държави членки на ЕС са ратифицирали Конвенция № 108. През 1999 г. бяха предложени изменения в Конвенция № 108, за да може ЕС да стане страна по нея, които обаче не влезнаха в сила[25]. През 2001 г. беше приет Допълнителен протокол към Конвенция № 108. С него бяха въведени разпоредби относно трансграничните потоци от данни към държави, които не са страни по Конвенцията, така наречените трети държави, както и относно задължителното създаване на национални надзорни органи за защита на данните[26].

Конвенция № 108 е открита за присъединяване от държави от Съвета на Европа, които не са страни по нея. Потенциалът на Конвенцията като универсален стандарт и нейният отворен характер служат като основа за насърчаване на защитата на данните в световен мащаб. За момента страни по Конвенция № 108 са 51 държави. Те включват всички държави членки на Съвета на Европа (47 държави), Уругвай — първата държава извън Европа, която се присъедини през август 2013 г., и Мавриций, Сенегал и Тунис, които се присъединиха през 2016 и 2017 г.

Конвенцията наскоро премина процес на осъвременяване. Обществена консултация, проведена през 2011 г., потвърди двете основни цели на този документ: засилването на защитата на неприкосновеността на личния живот в цифровото пространство и укрепването на предвидения в конвенцията

24 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23 ноември 1995 г.

25 Съвет на Европа, Изменения на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (ETS № 108), приети от Комитета на министрите в Страсбург на 15 юни 1999 г.

26 Съвет на Европа, Допълнителен протокол към Конвенцията за защита на лицата при автоматизирана обработка на лични данни, по отношение на надзорните органи и трансграничните информационни потоци, CETS № 181, 2001 г. С модернизацията на Конвенция № 108 този протокол повече не се прилага, тъй като неговите разпоредби бяха осъвременени и включени в модернизирана Конвенция № 108.

механизъм за последващи действия. Процесът на осъвременяване се съсредоточи върху тези цели и беше завършен с приемането на протокол, изменящ Конвенция № 108 (Протокол CETS No. 223). Работата се извърши успоредно с други реформи в международните инструменти за защита на данните и едновременно с реформата на правилата на ЕС за защита на данните, започнала през 2012 г. Регулаторните органи на равнището на Съвета на Европа и на равнището на ЕС положиха всички усилия, за да гарантират последователност и съвместимост между двете правни рамки. Осъвременяването запазва общия и гъвкав характер на конвенцията и укрепва нейния потенциал като универсален инструмент в правото в областта на защитата на данните. То потвърждава и стабилизира важни принципи и предвижда нови права на лицата, като в същото време повишава отговорността на субектите, които обработват лични данни, и гарантира по-добра отчетност. Например лицата, чиито лични данни се обработват, имат право да получат информация за обосновката на това обработване, както и право на възражение срещу него. За да се противодейства на увеличеното използване на профилирането в света на интернет, Конвенцията също така установява правото на лицето да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, без да бъде взето предвид неговото мнение. Ефективното прилагане на правилата за защита на данните от страна на независимите надзорни органи в държавите, които са договарящи се страни, се счита за ключово за практическото прилагане на Конвенцията. За тази цел в модернизираната Конвенция се подчертава необходимостта надзорните органи да разполагат с ефективни правомощия и функции и да са действително независими при изпълнението на своята мисия.

1.1.5 Право на Европейския съюз в областта на защитата на данните

Правото на ЕС се състои от първичното и вторичното право на ЕС. Договорите, а именно Договорът за Европейския съюз (ДЕС) и Договорът за функционирането на Европейския съюз (ДФЕС), са ратифицирани от всички държави членки на ЕС; те формират „първичното право на ЕС“. Регламентите, директивите и решенията на ЕС са приети от институциите на ЕС, на които са били предоставени такива правомощия съгласно договорите; те съставляват „вторичното право на ЕС“.

Защита на данните в първичното право на ЕС

Първоначалните договори на Европейските общности не съдържат никакво позоваване на правата на човека или тяхната защита, тъй като първоначално е било предвидено Европейската икономическа общност да бъде регионална организация, съсредоточена върху икономическата интеграция и създаването на общ пазар. Основен принцип, на който се крепят създаването и развитието на Европейските общности — и който е еднакво валиден и днес — е принципът на предоставената компетентност. Съгласно този принцип ЕС действа единствено в границите на компетентност, която са му предоставили държавите членки, както е отразено в Договорите на ЕС. За разлика от Съвета на Европа, Договорите на ЕС не включват изрична компетентност по въпросите за основните права.

Когато обаче в Съда на ЕС бяха заведени дела за предполагаеми нарушения на правата на човека в области, попадащи в обхвата на правото на ЕС, Съдът на ЕС предостави важно тълкуване на договорите. За да предостави защита на физическите лица, той включи основните права в така наречените общи принципи на европейското право. Според Съда на ЕС тези общи принципи отразяват съдържанието на защитата на правата на човека, установена в националните конституции и договорите за правата на човека, по-специално в ЕКПЧ. Съдът на ЕС заяви, че ще гарантира съответствие на правото на ЕС с тези принципи.

Признавайки, че неговите политики биха могли да окажат въздействие върху правата на човека, и за да се чувстват гражданите по-свързани с ЕС, през 2000 г. Съюзът прие Хартата на основните права на Европейския съюз (Хартата). Тя включва целия спектър от граждански, политически, икономически и социални права на европейските граждани, като излага в синтезиран вид общите за държавите членки конституционни традиции и международни задължения. Правата, описани в Хартата, са групирани в шест раздела: „Достойнство“, „Свободи“, „Равенство“, „Солидарност“, „Права на гражданите“ и „Правосъдие“.

Първоначално само политически документ, Хартата придоби правно обвързващ характер[27] като първично право на ЕС (вж. член 6, параграф 1 от Договора за Европейския съюз) с влизането в сила на Договора от Лисабон на

27 ЕС (2012 г.), Харта на основните права на Европейския съюз, ОВ C 326, 26.10.2012 г.

1 декември 2009 г.[28]. Разпоредбите на Хартата са насочени към институциите и органите на ЕС, като ги задължават да зачитат изброените там права при изпълнението на техните задължения. Разпоредбите на Хартата също така са задължителни за държавите членки, когато прилагат правото на ЕС.

Хартата не само гарантира зачитането на личния и семейния живот (член 7), но също така установява правото на защита на личните данни (член 8). Хартата изрично издига нивото на тази защита в правото на ЕС до това на основно право. Институциите и органите на ЕС трябва да гарантират и да зачитат това право, както правят това държавите членки, когато прилагат правото на Съюза (член 51 от Хартата). Формулиран няколко години след приемането на Директивата за защита на личните данни, член 8 от Хартата трябва да се тълкува като израз на съществуващото преди това право на ЕС в областта на защитата на данните. Поради това в Хартата не само изрично се указва правото на защита на данните в член 8, параграф 1, но също така се посочват основните принципи за защита на данните в член 8, параграф 2. Накрая, член 8, параграф 3 от Хартата изисква прилагането на тези принципи да подлежи на контрол от независим орган.

Приемането на Договора от Лисабон е повратен момент в развитието на правото в областта на защитата на данните не само с издигането на статута на Хартата до задължителен правен документ на равнището на първичното право, но също и с предвиждането на право на защита на личните данни. Това право е изрично предвидено в член 16 от ДФЕС, в частта от Договора, посветена на общите принципи на ЕС. Член 16 също така създава ново правно основание, като предоставя на ЕС законодателна компетентност в областта на защитата на данните. Това е важна промяна, защото правилата на ЕС за защита на данните – по-специално Директивата за защита на личните данни – първоначално се базираха върху правното основание за вътрешния пазар и върху необходимостта от сближаване на националните законодателства, така че свободното движение на данни в рамките на ЕС да не бъде възпрепятствано. Член 16 от ДФЕС понастоящем осигурява независимо правно основание за съвременен, всеобхватен подход към защитата на данните, което обхваща всички въпроси от компетентността на ЕС, включително полицейското и съдебното сътрудничество по наказателноправни въпроси. Член 16 от ДФЕС също така потвърждава, че спазването на правилата за защита на

28 Вж. Европейски общности (2012 г.), Консолидирани текстове на Договора за Европейския съюз, ОВ C 326, 26.10.2012 г., и на Договора за функционирането на Европейския съюз, ОВ C 326, 26.10.2012 г.

данните, приети в съответствие с него, трябва да бъде предмет на контрол от независими надзорни органи. Член 16 е послужил като правно основание за приемането на всеобхватната реформа на правилата за защита на данните през 2016 г., а именно Общия регламент относно защитата на данните и Директивата за защита на данните, обработвани от полицейските и наказателноправните органи (вж. по-долу).

Общият регламент относно защитата на данните

Основният правен инструмент на ЕС за защита на данните от 1995 г. до май 2018 г. е Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (Директивата за защита на личните данни)[29]. Тя беше приета през 1995 г., когато редица държави членки вече бяха приели национални закони за защита на данните[30], в резултат от необходимостта от хармонизиране на тези закони, за да се гарантира високо равнище на защита и свободно движение на лични данни в различните държави членки. Свободното движение на стоки, капитали, услуги и хора в рамките на вътрешния пазар изискваше наличието на свободно движение на данни, което можеше да бъде осъществено само ако държавите членки можеха да разчитат на еднакво високо ниво на защита на данните.

Директивата за защита на личните данни отразява вече съдържащите се в националните законодателства и в Конвенция № 108 принципи за защита на данните, като често ги разширява. Тя се основава на възможността, предвидена в член 11 от Конвенция № 108, за добавяне на инструменти за защита. По-специално въвеждането в Директивата на независимия надзор като инструмент за подобряване на съответствието с правилата за защита на данните се оказа важен принос за ефективното функциониране на европейското право в областта на защитата на данните. Впоследствие, чрез Допълнителния протокол към Конвенция № 108, през 2001 г. тази функция

29 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995 г.

30 Германската провинция Хесен прие първия в света закон за защита на данните през 1970 г.; той се прилага само за тази провинция. Швеция прие *Datalagen* през 1973 г.; Германия прие *Bundesdatenschutzgestez* през 1976 г.; и Франция прие *Loi relatif à l'informatique, aux fichiers et aux libertés* през 1977 г. В Обединеното кралство Законът за защита на личните данни беше приет през 1984 г. Накрая Нидерландия прие *Wet Persoonregistraties* през 1989 г.

бе включена в правото на Съвета на Европа. Това показва тясното взаимодействие между двата инструмента и положителното влияние, което те взаимно си оказват, в течение на годините.

Директивата за защита на личните данни установи подробна и всеобхватна система за защита на личните данни в ЕС. В съответствие с правната система на ЕС обаче директивите не се прилагат директно и трябва да бъдат транспонирани в националните законодателства на държавите членки. Държавите членки неизбежно имат свобода на преценка при транспонирането на разпоредбите на директивата. Въпреки че директивата имаше за цел да осигури пълна хармонизация[31] (и пълна степен на защита), на практика тя беше транспонирана по различен начин в държавите членки. Това доведе до установяването на различни правила за защита на данните в ЕС, с различно тълкуване на определенията и правилата в националните законодателства. Равнищата на правоприлагане и тежестта на санкциите също варираха в различните държави членки. На последно място, след изготвянето на директивата в средата на 90-те години на XX в. в информационните технологии настъпиха значителни промени. Всички тези причини, взети заедно, предизвикаха провеждането на реформа на законодателството за защита на данните в ЕС.

След години на интензивна дискусия реформата доведе до приемането на Общия регламент относно защитата на данните през април 2016 г. Дебатите относно необходимостта от осъвременяване на правилата за защита на личните данни в ЕС започнаха през 2009 г., когато Комисията започна обществена консултация за бъдещата правна рамка за основното право на защита на личните данни. Предложението за регламент беше публикувано от Комисията през януари 2012 г., давайки началото на дълъг законодателен процес на преговори между Европейския парламент и Съвета на ЕС. След приемането му Общият регламент относно защитата на данните предвиждаше двегодишен преходен период. Той става напълно приложим на 25 май 2018 г., когато се отменя Директивата за защита на личните данни.

Приемането на Общия регламент относно защитата на данните през 2016 г. осъвремени законодателството за защита на данните в ЕС, като го направи подходящо за защита на основните права в контекста на икономическите и социалните предизвикателства на цифровата ера. ОРЗД запазва и развива

31 Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г., параграф 29.

основните принципи и права на субекта на данни, които са предвидени в Директивата за защита на личните данни. Освен това той въвежда нови задължения, изискващи от организациите да прилагат защита на данните на етапа на проектирането и по подразбиране, да назначават длъжностно лице за защита на данните при определени обстоятелства, да съблюдават новото право на преносимост на данните и да спазват принципа на отчетност. Съгласно правото на ЕС регламентите се прилагат пряко и няма нужда от национално прилагане. Следователно Общият регламент относно защитата на данните осигурява единен набор от правила за защита на данните в целия ЕС. Това създава хармонизирани правила за защита на данните в целия ЕС, като установява среда на правна сигурност, от която икономическите оператори и физическите лица могат да се възползват като „субекти на данни".

Въпреки че Общият регламент относно защитата на данните е пряко приложим, от държавите членки се очаква да актуализират своите действащи национални законодателства за защита на данните, така че напълно да съответстват на регламента, като също така отразяват свобода на преценка във връзка със специфичните разпоредби в съображение 10. Основните правила и принципи, установени в регламента, и солидните права, които той дава на физическите лица, съставляват голяма част от наръчника и са представени в следващите глави. Регламентът има всеобхватни правила за териториалния обхват. Той се прилага за предприятията, установени на територията на ЕС, но също и за администраторите и обработващите лични данни, които не са установени в ЕС, но предлагат стоки или услуги на субекти на данни в ЕС или наблюдават тяхното поведение. Тъй като няколко чуждестранни технологични предприятия имат ключов дял от европейския пазар и милиони клиенти от ЕС, е важно тези организации да се подчиняват на правилата на ЕС за защитата на данните, за да се осигури защита на физическите лица и да се гарантира равнопоставеност.

Защита на данните в правоприлагането — Директива 2016/680

Отменената Директива за защита на личните данни осигуряваше всеобхватен режим за защита на данните. Този режим сега е допълнително подобрен с приемането на Общия регламент относно защитата на данните. Макар и широко, приложното поле на отменената Директива за защита на личните данни беше ограничено до дейности, които попадат в рамките на вътрешния пазар, и до дейността на публични органи, различни от правоприлагащите. Ето защо се наложи приемането на специални инструменти, за да се постигне

необходимата яснота и баланс между защитата на данните и другите законни интереси и да се отговори на предизвикателствата, които са от особено значение в определени сектори. Такъв е случаят с правилата за обработване на лични данни от правоприлагащите органи.

Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, беше първият правен инструмент на ЕС за регламентиране на този въпрос. Неговите правила бяха приложими само за полицейските и съдебните данни, обменяни между държавите членки. Вътрешното обработване на лични данни от правоприлагащите органи беше изключено от неговото приложно поле.

Директива 2016/680 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[32], наричана Директива за защита на данните, обработвани от полицейските и наказателноправните органи, коригира това положение. Приета успоредно с Общия регламент относно защитата на данните, директивата отмени Рамково решение 2008/977/ПВР и установи всеобхватна система за защита на личните данни в контекста на правоприлагането, като в същото време в нея се признават особеностите на обработването на данни във връзка с обществената сигурност. Докато Общият регламент относно защитата на данните предвижда общи правила за защита на физическите лица във връзка с обработването на техните лични данни и за осигуряване на свободното движение на такива данни в рамките на ЕС, то директивата определя специфични правила за защита на данните в областите на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество. Директива 2016/680 ще се прилага, когато компетентен орган обработва лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления. Когато компетентните органи обработват лични данни за цели, различни от посочените по-горе, ще се прилага общият режим съгласно Общия регламент относно

32 Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. 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, ОВ L 119, 4.5.2016 г.

защитата на данните. За разлика от предишния документ (Рамково решение 2008/977/ПВР на Съвета), приложното поле на Директива 2016/680 включва и вътрешното обработване на лични данни от правоприлагащите органи и не се ограничава само до обмена на такива данни между държавите членки. Освен това директивата цели да постигне баланс между правата на физическите лица и легитимните цели на обработването, свързано със сигурността.

За тази цел Директивата утвърждава правото на защита на личните данни и основните принципи, които следва да се прилагат за обработването на лични данни, като стриктно следва правилата и принципите, залегнали в Общия регламент относно защитата на данните. Правата на физическите лица и задълженията, наложени на администраторите — например във връзка със сигурността на данните, защитата на данните на етапа на проектирането и по подразбиране и уведомленията за нарушения на сигурността на личните данни — са сходни с правилата и задълженията в Общия регламент относно защитата на данните. Директивата също така взема предвид и се опитва да отговори на сериозни нови технологични предизвикателства, които могат да окажат особено обременително въздействие върху лицата, като например използването на техники за профилиране от правоприлагащите органи. По принцип трябва да бъде забранено вземането на решение, основано единствено на автоматизирано обработване, включително профилиране[33]. Освен това то не трябва да се основава на чувствителни данни. Тези принципи са обект на определени изключения, предвидени в директивата. В допълнение, такова обработване не трябва да води до дискриминация на което и да било лице[34].

Директивата също така съдържа правила с цел гарантиране на отчетността на администраторите. Те трябва да определят длъжностно лице за защита на данните, което да наблюдава спазването на правилата за защита на данните, да информира и да съветва предприятията и служителите, извършващи обработване на лични данни, относно техните задължения и да сътрудничи с надзорния орган. Обработването на лични данни в секторите на полицията и наказателното правосъдие сега е обект на надзор от независими надзорни органи. Както общият правен режим за защита на личните данни, така и специалният режим за защита на личните данни в областта на правоприлагането

33 Директива за защита на данните, обработвани от полицейските и наказателноправните органи, член 11, параграф 1.

34 *Пак там*, член 11, параграфи 2 и 3.

и наказателното правосъдие трябва да спазват изискванията на Хартата на основните права на ЕС.

Специалният режим за обработване на лични данни в контекста на полицейското и съдебното сътрудничество, установен в Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, е описан подробно в глава 8.

Директива за правото на неприкосновеност на личния живот и електронни комуникации

В сектора на електронните комуникации също беше счетено за необходимо да бъдат създадени специални правила за защита на личните данни. С развитието на интернет и стационарната и мобилната телефония беше важно да се гарантира зачитането на правата на потребителите на неприкосновеност на личния живот и на поверителност. Директива 2002/58/ЕО[35] 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 електронни комуникации) определя правила относно сигурността на личните данни в тези мрежи, уведомяването за нарушения на сигурността на личните данни и поверителността на съобщенията.

По отношение на сигурността операторите на електронни комуникационни услуги трябва, наред с другото, да гарантират, че достъпът до лични данни е ограничен единствено до упълномощените за това лица и да вземат мерки за предотвратяване на унищожаването, загубата или случайното увреждане на лични данни[36]. В случай на особен риск от нарушение на сигурността на публичната комуникационна мрежа доставчикът трябва да уведоми абонатите относно риска[37]. Ако въпреки предприетите мерки за сигурност възникне нарушение на сигурността, операторите трябва да уведомят компетентния национален орган, на който е поверено изпълнението и прилагането на

35 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. 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 електронни комуникации), ОВ L 201.

36 Директива за правото на неприкосновеност на личния живот и електронни комуникации, член 4, параграф 1.

37 *Пак там*, член 4, параграф 2.

директивата, за нарушението в сигурността на личните данни. В някои случаи от операторите се изисква също така да уведомят физическите лица за нарушения в сигурността на личните данни, а именно когато нарушението има вероятност да повлияе отрицателно върху техните лични данни или върху неприкосновеността на личния им живот[38]. Поверителността на съобщенията изисква слушането, записването, съхранението и другите видове наблюдение или подслушване на съобщения и метаданни да бъдат забранени по принцип. Директивата забранява също така нежеланите съобщения (често наричани „спам"), освен ако потребителите не са дали съгласието си, и съдържа правила за съхранението на „бисквитки" на компютрите и устройствата. Тези основни отрицателни задължения ясно показват, че поверителността на съобщенията е свързана в значителна степен със защитата на правото на зачитане на личния живот, залегнало в член 7 от Хартата, и на правото на защита на личните данни, залегнало в член 8 от Хартата.

През януари 2017 г. Комисията публикува предложение за регламент относно зачитането на личния живот и защитата на личните данни в електронните съобщения, предназначен да замени Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Реформата има за цел да приведе правилата, регламентиращи електронните комуникации, в съответствие с новия режим за защита на данните, установен от Общия регламент относно защитата на данните. Новият регламент ще бъде пряко приложим в целия ЕС; всички лица ще се ползват от еднакво ниво на защита на електронните си съобщения, а в същото време телекомуникационните оператори и предприятията ще спечелят от яснотата, правната сигурност и наличието на единен набор от правила в целия ЕС. Предложените правила за поверителност на електронните съобщения ще се прилагат и за новите участници, предоставящи електронни съобщителни услуги, които не са обхванати от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Тази директива обхващаше само традиционните доставчици на телекомуникационни услуги. С масовото използване на услуги, като Skype, WhatsApp, Facebook Messenger и Viber за изпращане на съобщения или обаждания, тези високотехнологични услуги вече ще попадат в приложното поле на регламента и ще трябва да спазват неговите изисквания за защита на данните, неприкосновеност на личния живот и сигурност. Към момента на публикуването на настоящия наръчник течеше законодателен процес

38 *Пак там*, член 4, параграф 3.

относно правилата за неприкосновеност на личния живот при електронните комуникации.

Регламент № 45/2001

Тъй като Директивата за защита на личните данни можеше да се прилага само в държавите членки на ЕС, бе необходим допълнителен правен инструмент, за да се въведе защита на данните при обработването на лични данни от институциите и органите на ЕС. Регламент (ЕО) № 45/2001 относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (Регламент относно защитата на данните при обработването им от институции на ЕС) изпълнява тази задача[39].

Регламент № 45/2001 стриктно следва принципите на общия режим за защита на данните в ЕС и ги прилага към обработването на данни, извършвано от институциите и органите на ЕС при изпълнението на техните функции. Освен това с него се създава независим надзорен орган, който да наблюдава прилагането на неговите разпоредби – Европейският надзорен орган по защита на данните (ЕНОЗД). На ЕНОЗД са предоставени надзорни правомощия и задължението да наблюдава обработването на лични данни в институциите и органите на ЕС, както и да изслушва и да разследва жалби за предполагаеми нарушения на правилата за защита на личните данни. Той също така предоставя консултации на институциите и органите на ЕС по всички въпроси относно защитата на личните данни, от предложения за ново законодателство до изготвяне на вътрешни правила относно обработването на лични данни.

През януари 2017 г. Европейската комисия представи предложение за нов регламент относно обработването на лични данни от институциите на ЕС, който ще отмени сега действащия. Подобно на реформата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, реформата на Регламент № 45/2001 ще осъвремени и съгласува правилата му с новия режим за защита на личните данни, установен от Общия регламент относно защитата на данните.

39 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

Ролята на Съда на ЕС

Съдът на ЕС е компетентен да определи дали дадена държава членка е изпълнила своите задължения съгласно правото на ЕС в областта на защитата на данните и да тълкува законодателството на ЕС, за да гарантира неговото ефективно и еднакво прилагане във всички държави членки. От приемането на Директивата за защита на личните данни през 1995 г. е натрупана значителна съдебна практика, с която се пояснява обхватът и значението на принципите за защита на личните данни и основното право на защита на личните данни, залегнало в член 8 от Хартата. Макар и директивата да е отменена и сега да е в сила нов правен инструмент – Общият регламент относно защитата на данните, вече съществуващата съдебна практика остава приложима и валидна за тълкуването и прилагането на принципите на ЕС за защита на данните, доколкото основните принципи и понятия от Директивата за защита на личните данни са запазени в ОРЗД.

1.2 Ограничения на правото на защита на личните данни

Ключови въпроси

- Правото на защита на личните данни не е абсолютно право; то може да бъде ограничено, ако това е необходимо за цел от общ интерес или за да се защитят правата и свободите на другите.
- Условията, при които се ограничават правата, свързани със зачитане на неприкосновеността на личния живот и защита на личните данни, са посочени в член 8 от ЕКПЧ и в член 52, параграф 1 от Хартата. Те са развити и се тълкуват посредством съдебната практика на ЕСПЧ и на Съда на ЕС.
- Съгласно правото за защита на данните на Съвета на Европа обработването на лични данни представлява законна намеса в правото на зачитане на неприкосновеността на личния живот и може да бъде извършвано само ако то:
  - е в съответствие със закона;
  - преследва законна цел;
  - зачита същността на основните права и свободи;
  - е необходимо и пропорционално в едно демократично общество за постигане на законна цел.

- Правният ред на ЕС поставя сходни условия относно ограниченията на упражняването на основните права, защитени от Хартата. Всяко ограничение на основно право, включително на защита на личните данни, може да бъде законно само ако то:
  - е в съответствие със закона;
  - зачита същността на правото;
  - е необходимо, при спазване на принципа на пропорционалност; и
  - преследва призната от ЕС цел от общ интерес или необходимостта да се защитят правата на други хора.

Основното право на защита на личните данни съгласно член 8 от Хартата не е абсолютно право, „а трябва да се разглежда по отношение на неговата функция в обществото“[40]. Ето защо в член 52, параграф 1 от Хартата се признава, че върху упражняването на правата, например тези, предвидени в членове 7 и 8 от Хартата, може да бъдат наложени ограничения, при условие че тези ограничения са предвидени в закон, зачитат основното съдържание на тези права и свободи и, при спазване на принципа на пропорционалност, са необходими и действително отговарят на признати от ЕС цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора[41]. В системата на ЕКПЧ защитата на личните данни е гарантирана от член 8, като упражняването на това право може да бъде ограничено, когато това е необходимо за преследване на законна цел. Настоящият раздел се отнася до условията за намеса по ЕКПЧ съгласно тълкуването в съдебната практика на ЕСПЧ, както и до условията за законни ограничения съгласно член 52 от Хартата.

40 Вж. например Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г., параграф 48.

41 *Пак там*, параграф 50.

1.2.1 Изисквания за оправдана намеса съгласно ЕКПЧ

Обработването на лични данни може да представлява намеса в правото на субекта на данни на зачитане на личния живот, защитено от член 8 от ЕКПЧ[42]. Както беше обяснено по-горе (вж. раздел 1.1.1 и раздел 1.1.4), в противоречие с правния ред на ЕС, защитата на личните данни не е утвърдена като отделно основно право в ЕКПЧ. Защитата на личните данни е по-скоро част от правата, защитени във връзка с правото на зачитане на личния живот. Следователно не всяка операция, включваща обработване на лични данни, би могла да попадне в обхвата на член 8 от ЕКПЧ. За да бъде задействан член 8, първо трябва да бъде определено дали е изложен на риск частният интерес или личният живот на дадено лице. В своята съдебна практика ЕСПЧ третира понятието „личен живот" като широко понятие, което покрива дори аспекти от професионалния живот и общественото поведение. Той също така е постановил, че защитата на личните данни е важна част от правото на зачитане на личния живот. Въпреки широкото тълкуване на личния живот обаче не всички видове обработване сами по себе си излагат на риск правата, защитени по член 8.

Когато ЕСПЧ счита, че разглежданата операция по обработване засяга правото на лицата на зачитане на личния живот, той проверява дали намесата е обоснована. Правото на зачитане на личния живот не е абсолютно право, а трябва да бъде балансирано и съгласувано с други законни интереси и права, независимо дали на други лица (частни интереси), или на обществото като цяло (обществени интереси).

Намесата може да бъде обоснована, ако са изпълнени едновременно следните условия:

В съответствие със закона

Според съдебната практика на ЕСПЧ една намеса е в съответствие със закона, ако се основава на разпоредба от националното законодателство, която притежава определени характеристики. Законът трябва да е „достъпен за

42 ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04, № 30566/04, 4 декември 2008 г., параграф 67.

съответното лице и предвидим по отношение на своите последици“[43]. Една разпоредба е предвидима, ако е „формулирана с достатъчна точност, за да позволи на всяко лице — ако е необходимо с подходяща консултация – да съобрази с нея поведението си“[44]. Освен това „степента на точност, изисквана от „закона“ в тази връзка, ще зависи от конкретния въпрос“[45].

Примери: По делото *Rotaru/Румъния*[46] жалбоподателят твърди, че е нарушено правото му на зачитане на личния живот на основание, че румънската разузнавателна служба съхранява и използва досие, съдържащо негова лична информация. ЕСПЧ констатира, че докато националното законодателство допуска събирането, записването и архивирането на секретни досиета с информация, засягаща националната сигурност, в него не се поставят ограничения за упражняването на тези правомощия, което се извършва по усмотрение на органите. Например в националното законодателство не са определени видът информация, която може да бъде обработвана, категориите лица, срещу които могат да бъдат взети мерки за наблюдение, обстоятелствата, при които могат да бъдат взети тези мерки, или процедурата, която трябва да бъде следвана. Поради това Съдът заключава, че националното законодателство не отговаря на изискванията за предвидимост по член 8 от ЕКПЧ и че е налице нарушение на този член.

По делото *Taylor-Sabori/Обединеното кралство*[47] жалбоподателят е бил обект на полицейско наблюдение. Посредством използване на „клонинг“ на пейджъра на жалбоподателя полицията е била

43 ЕСПЧ, *Amann/Швейцария* [голям състав], № 27798/95, 16 февруари 2000 г., параграф 50; вж. също ЕСПЧ, *Kopp/Швейцария*, № 23224/94, 25 март 1998 г., параграф 55, и ЕСПЧ, *Iordachi и други/Молдова*, № 25198/02, 10 февруари 2009 г., параграф 50.

44 ЕСПЧ, *Amann/Швейцария* [голям състав], № 27798/95, 16 февруари 2000 г., параграф 56; вж. също ЕСПЧ, *Malone/Обединеното кралство*, № 8691/79, 2 август 1984 г., параграф 66; ЕСПЧ, *Silver и други/Обединеното кралство*, № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 г., параграф 88.

45 ЕСПЧ, *The Sunday Times/Обединеното кралство*, № 6538/74, 26 април 1979 г., параграф 49; вж. също ЕСПЧ, *Silver и други/Обединеното кралство*, № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 г., параграф 88.

46 ЕСПЧ, *Rotaru/Румъния* [голям състав], № 28341/95, 4 май 2000 г., параграф 57; вж. също ЕСПЧ, *Асоциация за Европейска интеграция и права на човека и Екимджиев/България*, № 62540/00, 28 юни 2007 г.; ЕСПЧ, *Shimovolos/Русия*, № 30194/09, 21 юни 2011 г.; и ЕСПЧ, *Vetter/Франция*, № 59842/00, 31 май 2005 г.

47 ЕСПЧ, *Taylor-Sabori/Обединеното кралство*, № 47114/99, 22 октомври 2002 г.

в състояние да прихваща съобщенията, изпратени до него. След това жалбоподателят е бил арестуван и обвинен в конспирация за доставяне на контролирани наркотици. Част от наказателното преследване срещу него се е състояло в писмени записи на съобщенията от пейджъра от този период, които са били възпроизведени в писмена форма от полицията. Въпреки това по време на съдебния процес срещу жалбоподателя в британския закон не е съществувала разпоредба, която да урежда прихващането на съобщения, предадени чрез частна телекомуникационна система. Поради това намесата в неговите права не е била „в съответствие със закона". ЕСПЧ заключава, че е налице нарушение на член 8 от ЕКПЧ.

Дело *Vukota-Bojić/Швейцария*[48] се отнася до тайно наблюдение над ищец по дело за социално осигуряване от частни детективи, като наблюдението е било възложено от застрахователното дружество на лицето. ЕСПЧ постановява, че въпреки че разглежданата в жалбата мярка за наблюдение е била наредена от частно застрахователно дружество, това дружество е получило от държавата правото да предоставя обезщетения, произтичащи от задължителната медицинска застраховка, и да събира застрахователни премии. Държавата не може да се освободи от отговорност по конвенцията, като делегира задълженията си на частни органи или лица. Националното право е трябвало да предвиди достатъчно гаранции срещу злоупотреби, така че намесата в правата по член 8 от ЕКПЧ да е „в съответствие със закона". В разглеждания случай ЕСПЧ заключава, че е налице нарушение на член 8 от ЕКПЧ, тъй като националното право не е посочило достатъчно ясно обхвата и начина на упражняване на правомощията, предоставени на застрахователните дружества, действащи като публични органи при застрахователни спорове, за извършване на тайно наблюдение на застраховано лице. По-конкретно то не включва достатъчни гаранции срещу злоупотреби.

Преследване на законна цел

Законната цел може да бъде свързана с посочените обществени интереси или с правата и свободите на други лица. Съгласно член 8, параграф 2 от ЕКПЧ

48 ЕСПЧ, *Vukota-Bojić/Швейцария*, № 61838/10, 18 октомври 2016 г., параграф 77.

законните цели, които биха могли да оправдаят намеса, са тези в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

Пример: В делото *Peck/Обединеното кралство*[49] жалбоподателят е направил опит за самоубийство на улицата, като е прерязал вените на ръцете си, без да знае, че камерата на система за видеонаблюдение (CCTV) го е заснела. След като полицията, която е наблюдавала камерите на CCTV, го е спасила, полицейските органи са предали кадрите от CCTV на медиите, които са ги публикували, без да скрият лицето на жалбоподателя. ЕСПЧ констатира, че не са налице уместни или достатъчни причини, които да оправдаят факта, че органите директно са разкрили кадрите на обществеността, без да са получили съгласието на жалбоподателя или без да скрият неговата самоличност. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

Намесата е необходима в едно демократично общество

ЕСПЧ посочва, че „концепцията за необходимост предполага, че намесата съответства на належаща обществена нужда, и по-специално че тя е пропорционална на преследваната законна цел“[50]. При преценката дали дадена мярка е необходима за удовлетворяване на належаща социална нужда ЕСПЧ разглежда нейната относимост и уместност по отношение на преследваната цел. За тази цел съдът взема предвид дали намесата се опитва да реши въпрос, който, ако не бъде решен, може да има неблагоприятни последици за обществото, дали има доказателства, че намесата може да намали тези неблагоприятни последици и каква е общата обществена нагласа по разглеждания въпрос[51]. Например събирането и съхраняването на лични данни от службите за сигурност относно определени лица, за които е установено, че са свързани с терористични движения, би било намеса в тяхното право на зачитане на личния живот, която обаче служи на сериозна, належаща обществена нужда: националната сигурност и борбата с тероризма. Намесата трябва

49 ЕСПЧ, *Peck/Обединеното кралство*, № 44647/98, 28 януари 2003 г., параграф 85.

50 ЕСПЧ, *Leander/Швеция*, № 9248/81, 26 март 1987 г., параграф 58.

51 Работна група за защита на данните по член 29 (Работна група по член 29) (2014 г.), *Становище относно прилагането на концепциите за необходимост и пропорционалност и защитата на данните в сектора на правоприлагането*, WP 211, Брюксел, 27 февруари 2014 г., стр. 7–8.

също така да бъде пропорционална, за да отговори на проверката за необходимост. В съдебната практика на ЕСПЧ пропорционалността се разглежда като част от концепцията за необходимост. Пропорционалността изисква намесата в защитените по ЕКПЧ права да не надхвърля това, което е необходимо за постигането на преследваната законна цел. Сред важните фактори, които трябва да се вземат предвид при извършването на проверката за пропорционалност, са обхватът на намесата, по-специално броят на засегнатите лица, и въведените гаранции или условия за ограничаване на нейния обхват или неблагоприятни последици за правата на физическите лица[52].

Пример: В делото *Khelili/Швейцария*[53] по време на полицейска проверка полицията установява, че жалбоподателката носи визитни картички, на които пише: „Красива жена над 35 би искала да се срещне с мъж за по питие или с цел срещи от време на време. Тел. номер [...]“. Жалбоподателката твърди, че след това разкритие полицията е регистрирала името ѝ в архивите си като проститутка — дейност, която тя категорично отрича. Жалбоподателката отправя искане думата „проститутка“ да бъде изтрита от компютърните регистри. ЕСПЧ принципно признава, че задържането на личните данни на дадено лице на основание, че то би могло да извърши друго правонарушение, би могло при определени обстоятелства да е пропорционално. В случая на жалбоподателката обаче твърдението за незаконна проституция изглежда твърде неясно и общо, като не е подкрепено от конкретни факти, тъй като тя никога не е била обвинена в незаконна проституция и следователно не може да се счита, че въпросното твърдение удовлетворява „належаща обществена нужда“ по смисъла на член 8 от ЕПКЧ. Приемайки това като въпрос, по отношение на който органите трябва да докажат точността на съхранените данни за жалбоподателката, и предвид тежестта на намесата в правата на жалбоподателката, Съдът постановява, че запазването на думата „проститутка“ в полицейските досиета в продължение на години не е било необходимо в едно демократично общество. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

52 *Пак там*, стр. 9—11.

53 ЕСПЧ, *Khelili/Швейцария*, № 16188/07, 18 октомври 2011 г.

Пример: По делото *S. и Marper/Обединеното кралство*[54] и двамата жалбоподатели са били арестувани и обвинени в извършването на престъпление. Полицията е взела техни дактилоскопични отпечатъци и проби от ДНК, както е предвидено в Закона за полицията и доказателствата в наказателния процес. Жалбоподателите никога не са осъждани за престъпленията: единият е оправдан в съда, а наказателното производство срещу втория е било прекратено. Независимо от това техните дактилоскопични отпечатъци, ДНК профили и проби от клетки се пазят и съхраняват от полицията в база данни, а националното законодателство разрешава тяхното запазване без ограничение във времето. Въпреки че Обединеното кралство твърди, че запазването на данните е спомогнало за идентифицирането на бъдещи нарушители и следователно е преследвало легитимната цел за предотвратяване и разкриване на престъпления, ЕСПЧ счита, че намесата в правото на зачитане на личния живот на жалбоподателите е неоправдана. Той припомня, че основните принципи на защитата на лични данни изискват запазването на лични данни да бъде пропорционално на целта на събирането и периодите на запазване на данните да са ограничени. Съдът приема, че разширяването на базата данни, така че тя да включва ДНК профили не само на осъдените лица, но и на всички лица, които са били заподозрени, но не са били осъдени, е могло да допринесе за разкриването и предотвратяването на престъпления в Обединеното кралство. Съдът обаче е бил „изненадан от повсеместното и неизбирателно естество на правомощието за запазване на данни“[55].

Предвид богатата генетична и здравна информация, съдържаща се в пробите от клетки, намесата в правото на личен живот на жалбоподателите е била особено тежка. От арестуваните лица може да се вземат дактилоскопични отпечатъци и проби, които се запазват в полицейските бази данни за неограничен период от време независимо от естеството и тежестта на нарушението, дори за леки нарушения, които не се наказват с лишаване от свобода. Освен това възможностите за заличаване на данните на оправданите лица от базата данни са ограничени. Накрая ЕСПЧ обръща особено внимание на факта, че един от

54 ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04, № 30566/04, 4 декември 2008 г.

55 *Пак там*, параграф 119.

жалбоподателите е бил на единадесет години, когато е бил арестуван. Запазването на личните данни на непълнолетни лица, които не са били осъждани, може да бъде особено вредно предвид тяхната уязвимост и важността на тяхното развитие и интеграцията им в обществото[56]. Съдът единодушно постановява, че запазването им представлява непропорционална намеса в правото на личен живот, която не може да се счита за необходима в едно демократично общество.

Пример: По делото *Leander/Швеция*[57] ЕСЧП постановява, че тайното проучване на лица, които кандидатстват за назначаване на важни постове в областта на националната сигурност, само по себе си не е в противоречие с изискването за необходимост в едно демократично общество. Специалните гаранции, предвидени в националното законодателство за защита на интереса на съответното физическо лице, например контролът, упражняван от Парламента и министъра на правосъдието, са довели до заключението на ЕСПЧ, че шведската система за контрол на персонала отговаря на изискванията на член 8, параграф 2 от ЕКПЧ. Като е взела предвид голямата свобода на преценка, с която разполага, държавата ответник е имала правото да счете, че в случая на жалбоподателя интересите на националната сигурност имат преимущество над личните интереси. Съдът заключава, че не е налице нарушение на член 8 от ЕКПЧ.

1.2.2 Условията за законни ограничения съгласно Хартата на ЕС

Структурата и формулировката на Хартата е различна от тази на ЕКПЧ. В Хартата не се говори за намеса в гарантираните права, а се съдържа разпоредба относно ограничението(ята) при упражняването на правата и свободите, признати от Хартата.

Съгласно член 52, параграф 1 ограниченията при упражняването на правата и свободите, признати от Хартата, и съответно и при упражняването на правото на защита на личните данни са допустими само ако тези ограничения:

56 *Пак там*, параграф 124.

57 ЕСПЧ, *Leander/Швеция*, № 9248/81, 26 март 1987 г., параграфи 59 и 67.

- са предвидени в закон; и
- зачитат основния характер на правото на защита на данните; и
- са необходими, при спазване на принципа на пропорционалност[58]; и
- отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

Тъй като защитата на личните данни е отделно и самостоятелно основно право в правния ред на ЕС, защитено по член 8 от Хартата, всяко обработване на лични данни само по себе си представлява намеса в това право. Няма никакво значение дали въпросните лични данни се отнасят до личния живот на дадено лице, дали са чувствителни или дали на заинтересованото лице е причинено някакво неудобство. За да бъде законосъобразна, намесата трябва да отговаря на всички условия, изброени в член 52, параграф 1 от Хартата.

Ограниченията са предвидени в закон

Ограниченията на правото на защита на личните данни трябва да са предвидени в закон. Това изискване означава, че ограниченията трябва да имат правно основание, което е достъпно по подходящ начин, предвидимо и формулирано с достатъчна точност, за да могат физическите лица да разбират задълженията си и да регулират поведението си. Правното основание трябва също така ясно да определя обхвата и начина на упражняване на правомощието от компетентните органи, за да бъдат защитени лицата срещу произволна намеса. Това тълкуване наподобява изискването за „законна намеса" съгласно съдебната практика на ЕСПЧ[59], като съществуват и аргументи, че на използвания в Хартата израз „предвидено в закона" следва да се придаде същият смисъл като на съответстващия му израз от ЕКПЧ[60]. Съдебната

58 Относно оценката на необходимостта от мерки, ограничаващи основното право на защита на личните данни, вж.: ЕНОЗД (2017 г.), *Necessity Toolkit [Инструментариум за оценяване на необходимостта от мерки, които ограничават основното право на защита на личните данни]*, Брюксел, 11 април 2017 г.

59 ЕНОЗД (2017 г.), *Necessity Toolkit*, Брюксел, 11 април 2017 г, стр. 4; вж. също Съд на ЕС, *Становище 1/15 на Съда (голям състав)*, 26 юли 2017 г.

60 Съд на ЕС, съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], *Заключение на генералния адвокат Saugmandsgaard Øe*, представено на 19 юли 2016 г., параграф 140.

практика на ЕСПЧ, и особено понятието за „качество на закона“, което той е развил през годините, е подходящо съображение, което Съдът на ЕС трябва да вземе под внимание при тълкуването на обхвата на член 52, параграф 1 от Хартата[61].

Ограниченията зачитат същността на правото

В правния ред на ЕС всяко ограничение на основните права, защитени съгласно Хартата, трябва да е съобразено със същността на тези права. Това означава, че не може да бъдат обосновани ограничения, които са толкова обширни и представляват такава сериозна намеса, че лишават основното право от неговото основно съдържание. Ако същността на правото е нарушена, ограничението трябва да се счита за неправомерно, без да е необходима по-нататъшна оценка дали то служи на цел от общ интерес и дали отговаря на критериите за необходимост и пропорционалност.

Пример: Делото *Schrems*[62] се отнася до защитата на физическите лица във връзка с прехвърлянето на техни лични данни към трети държави – в конкретния случай САЩ. Schrems, австрийски гражданин, потребител на Facebook в продължение на няколко години, подава жалба до ирландския надзорен орган за защита на данните с искане същият да обяви за невалидно прехвърлянето на личните му данни от ирландското дъщерно дружество на Facebook към Facebook Inc. и към разположени на територията на САЩ сървъри, където тези данни се обработват. Той твърди, че в светлината на разкритията от 2013 г. на Едуард Сноудън – американски гражданин, подал сигнали за нарушения, относно дейностите по следене на американските служби за наблюдение, правото и практиката на САЩ не предлагат достатъчна защита на личните данни, прехвърляни на територията на САЩ. Сноудън разкри, че Агенцията за национална сигурност е подслушвала директно сървърите на фирми като Facebook и е можела да чете съдържанието на чатове и лични съобщения.

61 Съд на ЕС, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, *Заключение на генералния адвокат Cruz Villalón*, представено на 14 април 2011 г., параграф 100.

62 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

Прехвърлянето на данни към САЩ е било основано на решение на Комисията относно адекватното ниво на защита, прието през 2000 г., което разрешава прехвърляне към американски предприятия, които сами са се сертифицирали, че ще защитават личните данни, прехвърляни от ЕС, и ще спазват така наречените „принципи за сфера на неприкосновеност на личния живот". Когато делото е отнесено до Съда на ЕС, той проверява валидността на решението на Комисията в контекста на Хартата. Съдът припомня, че защитата на основните права в ЕС изисква дерогациите и ограниченията на тези права да се въвеждат в границите на строго необходимото. Според Съда на ЕС правна уредба, осигуряваща общ достъп на публичните органи до съдържанието на електронни съобщения, трябва да се счита за „засягаща съществото съдържание на основното право на зачитане на личния живот, гарантирано с член 7 от Хартата". Правото би било лишено от смисъл, ако публичните органи на САЩ са упълномощени да имат достъп до съобщенията на случаен принцип, без никаква обективна обосновка, основаваща се на конкретни съображения за националната сигурност или предотвратяването на престъпления, когато са засегнати конкретни лица, и ако тези практики за наблюдение не са придружени от подходящи гаранции срещу злоупотреба с власт.

Освен това, Съдът на ЕС отбелязва, че „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", е несъвместима с основното право на ефективна съдебна защита (член 47 от Хартата). Следователно Решението на Комисията относно „сферата на неприкосновеност на личния живот" не осигурява равнище на защита на основните права от страна на САЩ, което по същество е равностойно на равнището, гарантирано в рамките на ЕС, в съответствие с директивата, разглеждана във връзка с Хартата. Поради тази причина Съдът на ЕС обявява решението за невалидно[63].

63 Решението на Съда на ЕС да обяви за невалидно Решение № 520/2000/ЕО на Комисията има и други основания, които ще бъдат разгледани в други раздели на настоящия наръчник. По-конкретно Съдът на ЕС счита, че решението незаконно ограничава правомощията на националните надзорни органи за защита на данните. Освен това в рамките на схемата за „сфера на неприкосновеност на личния живот" лицата не разполагат с никакви съдебни средства за защита, в случай че желаят да получат достъп до засягащи ги лични данни и/или да поправят или заличат такива данни. По този начин е засегната и същността на основното право на ефективна съдебна защита, предвидено в член 47 от Хартата.

Пример: В делото *Digital Rights Ireland*[64] Съдът на ЕС разглежда съвместимостта на Директива 2006/24/ЕО (Директивата за запазване на лични данни) с членове 7 и 8 от Хартата. Директивата задължаваше доставчиците на електронни съобщителни услуги да запазват данни за трафика и местоположението за не по-малко от шест месеца и не повече от 24 месеца, както и да позволяват достъп до тези данни от страна на компетентните национални органи за целите на предотвратяването, разследването, разкриването и преследването на сериозни престъпления. Директивата не позволяваше запазване на съдържанието на електронните съобщения. Съдът на ЕС отбелязва, че данните, които доставчиците е трябвало да запазват в съответствие с директивата, са включвали данни, необходими за проследяване и идентифициране на източника и местоназначението на съобщението, датата, времето и продължителността на съобщението, номерата на изходящите и входящите повиквания и IP-адресите. От тези лични данни, „разгледани в съвкупност, е възможно да се изведат много точни заключения за личния живот на лицата, чиито данни са били запазени, например относно навиците им в ежедневния живот, мястото на постоянно или временно пребиваване, ежедневните им или други пътувания, упражняваните дейности, социалните връзки на тези лица и социалните кръгове, в които се движат".

Следователно запазването на лични данни съгласно директивата представлява особено тежка намеса в правото на неприкосновеност на личния живот и в правото на защита на личните данни. Съдът на ЕС обаче постановява, че тази намеса не е засегнала същността на тези права. Що се отнася до правото на неприкосновеност на личния живот, неговото съществено съдържание не е било засегнато, защото директивата не позволява да се разкрива самото съдържание на електронните съобщения. Същността на основното право на защита на личните данни също не е била засегната, тъй като директивата изисква доставчиците на електронни съобщителни услуги да спазват някои принципи във връзка със защитата и сигурността на данните и да прилагат подходящи технически и организационни мерки за тази цел.

64 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

Ограниченията са необходими и пропорционални

Член 52, параграф 1 от Хартата предвижда, че при спазване на принципа на пропорционалност ограниченията при упражняването на основните права и свободите, признати от Хартата, могат да бъдат налагани само ако са необходими.

Едно ограничение може да е **необходимо**, ако трябва да бъдат приети мерки за постигане на преследваната цел от обществен интерес; необходимостта, както се тълкува от Съда на ЕС, обаче предполага и предприетите мерки да бъдат с по-малка степен на намеса в сравнение с другите възможности за постигане на същата цел. Относно ограниченията на правата на зачитане на личния живот и защита на личните данни Съдът на ЕС прилага строг тест за необходимост, като постановява, че „дерогациите и ограниченията трябва да се въвеждат в границите на строго необходимото". Ако едно ограничение се счита за строго необходимо, трябва също така да се прецени дали то е пропорционално.

Пропорционалност означава, че ползите в резултат от ограничението следва да надхвърлят вредите, които то нанася на упражняването на въпросните основни права[65]. За да се намалят вредите и рисковете за упражняването на правата на неприкосновеност на личния живот и защита на личните данни, е важно ограниченията да съдържат подходящи гаранции.

Пример: В решението по дело *Volker und Markus Schecke*[66] Съдът на ЕС заключава, че с наложеното от тях задължение за публикуване на лични данни относно всяко физическо лице, което е било бенефициент на помощи от определени земеделски фондове, без да се прави разграничение въз основа на съотносими критерии, като периодите, през които те са получавали подобни помощи, честотата или вида и размера на помощите, Съветът и Комисията са надхвърлили границите, наложени от спазването на принципа на пропорционалност.

65 ЕНОЗД (2017 г.), *Necessity Toolkit*, стр. 5.

66 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г., точки 89 и 86.

Поради това Съдът на ЕС прие за необходимо да обяви за невалидни някои разпоредби на Регламент (ЕО) № 1290/2005 на Съвета и да обяви Регламент (ЕО) № 259/2008 за невалиден в неговата цялост[67].

Пример: В делото *Digital Rights Ireland*[68] Съдът на ЕС постановява, че намесата в правото на неприкосновеност на личния живот в резултат от прилагането на директивата за запазване на лични данни не е засегнала същността на това право, тъй като директивата забранява запазването на съдържанието на електронните съобщения. Съдът обаче заключава, че директивата е несъвместима с член 7 и член 8 от Хартата и я обявява за невалидна. Тъй като данните за трафика и местоположението, обобщени и взети в тяхната цялост, биха могли да бъдат анализирани и да представят подробна картина на личния живот на лицата, те представляват тежка намеса в тези права. Съдът на ЕС взема предвид обстоятелството, че директивата изисква запазване на всички метаданни относно фиксираната телефония, мобилната телефония, интернет достъпа, електронната поща по интернет и интернет телефонията, като обхваща всички електронни съобщителни средства, чието използване е широко разпространено в ежедневието на хората. На практика тя представлява намеса, която засяга цялото европейско население. Като се вземат предвид степента и тежестта на тази намеса, според Съда на ЕС запазването на данни за трафика и местоположението би могло да бъде оправдано единствено с цел борба с тежките престъпления. В допълнение, директивата не предвижда никакви обективни критерии, които да гарантират, че достъпът на компетентните национални органи до запазените данни е ограничен до строго необходимото. Освен това тя не съдържа материални и процесуални условия, регламентиращи достъпа и използването на запазените данни от страна на националните органи, нито пък изискване за предварителен контрол от съд или от друг независим орган.

67 Регламент (ЕО) № 1290/2005 на Съвета от 21 юни 2005 г. относно финансирането на Общата селскостопанска политика, ОВ L 209, 11.8.2005 г.; Регламент (ЕО) № 259/2008 на Комисията от 18 март 2008 г. за установяване на подробни правила за прилагане на Регламент (ЕО) № 1290/2005 относно публикуването на информация за получателите на средства от Европейския фонд за гарантиране на земеделието (ЕФГЗ) и Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР), ОВ L 76, 19.3.2008 г.

68 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г., параграф *39*.

Съдът на ЕС достига до подобно заключение и по съединени дела *Tele2 Sverige AB/Post- och telestryrelsen* и *Secretary of State for the Home Department/Tom Watson и други*[69]. Те се отнасят до запазването на данни за трафика и на данни за местонахождението на „всички абонати и регистрирани ползватели, и всички средства за електронни съобщения, както и метаданни", без „диференциране, ограничение или изключение в зависимост от преследваната цел"[70]. В разглеждания случай дали едно лице е било свързано пряко или косвено с тежки криминални престъпления и дали неговите съобщения са били от значение за националната сигурност, не представлява условие за запазване на личните му данни. Като се има предвид липсата както на изискване за връзка между запазваните данни и наличието на заплаха за националната сигурност, така и на ограничения за определен период или географска област, Съдът на ЕС заключава, че националното законодателство надхвърля границите на строго необходимото за целите на борбата срещу тежките престъпления[71].

Европейският надзорен орган по защита на данните е възприел подобен подход по отношение на необходимостта в своя *Necessity Toolkit [Инструментариум за оценяване на необходимостта от мерки, които ограничават основното право на защита на личните данни]*[72]. Инструментариумът има за цел да подпомогне оценяването на съответствието на предлаганите мерки със законодателството на ЕС за защита на личните данни. Той беше разработен, за да подготви по-добре политиците и законодателите на ЕС, отговарящи за подготовката или контрола на мерките, които включват обработване на лични данни и ограничават правото на защита на личните данни и други права и свободи, предвидени в Хартата.

Ограниченията отговарят на цели от общ интерес

За да бъде обосновано, всяко ограничение на упражняването на правата, признати от Хартата, трябва също така действително да отговаря на признати от

69 Съд на ЕС, съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], 21 декември 2016 г., параграфи 105—106.

70 *Пак там*, параграф 105.

71 *Пак там*, параграф 107.

72 ЕНОЗД (2017 г.), *Necessity Toolkit*, Брюксел, 11 април 2017 г.

Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора. Що се отнася до необходимостта да се защитят правата и свободите на другите, правото на защита на личните данни често влиза във взаимодействие с други основни права. В раздел 1.3 е представен подробен анализ на тези взаимодействия. Що се отнася до целите от общ интерес, те включват общите цели на ЕС, утвърдени в член 3 от Договора за Европейския съюз (ДЕС), като например насърчаването на мира и благоденствието на неговите народи, социалната справедливост и защита и установяването на пространство на свобода, сигурност и правосъдие, в което се гарантира свободното движение на хора, заедно с подходящи мерки за предотвратяване и борба с престъпността, както и други цели и интереси, защитени от специфични разпоредби на Договорите[73]. В тази връзка Общият регламент относно защитата на данните допълнително конкретизира член 52, параграф 1 от Хартата: в член 23, параграф 1 от регламента са изброени редица цели от общ интерес, които се считат за законосъобразни за ограничаване на правата на физическите лица, при условие че ограничението е съобразено със същността на правото на защита на личните данни и е необходимо и пропорционално. Сред посочените в регламента цели от обществен интерес са националната сигурност и отбраната, предотвратяването на престъпления, защитата на важни икономически и финансови интереси на ЕС или на държавите членки, общественото здраве и социалната сигурност.

Преследваните от ограничението цели от общ интерес е важно да бъдат определени и обяснени достатъчно подробно, тъй като необходимостта от ограничението ще се оценява спрямо тях. Ясното и подробно описание на целта на ограничението и на предлаганите мерки е от съществено значение, за да може да се извърши оценката дали то е необходимо[74]. Преследваната цел е тясно свързана с необходимостта и пропорционалността на ограничението.

Пример: Делото *Schwarz/Stadt Bochum*[75] се отнася до ограниченията на правото на зачитане на личния живот и правото на защита на личните данни, произтичащи от снемането и съхраняването на пръстови отпечатъци при издаването на паспорти от органите на държавите

73 Разяснения относно Хартата на основните права (2007/C 303/02), ОВ C 303, 14.12.2007 г., стр. 17—35.

74 ЕНОЗД (2017 г.), *Necessity Toolkit*, Брюксел, 11 април 2017 г., стр. 4.

75 Съд на ЕС, C-291/12, *Michael Schwarz/Stadt Bochum*, 17 октомври 2013 г.

членки[76]. Жалбоподателят иска от службите на Stadt Bochum (град Бохум) да му бъде издаден паспорт, но се противопоставя на снемането на пръстовите му отпечатъци, след което службите на Stadt Bochum отказват да му издадат паспорт. След това решение той подава жалба до германски съд да му бъде издаден паспорт, без да се снемат пръстовите му отпечатъци. Германският съд отнася въпроса до Съда на ЕС, като отправя запитване дали е валиден член 1, параграф 2 от Регламент № 2252/2004 относно стандартите за отличителните знаци за сигурност и биометричните данни в паспортите и документите за пътуване, издавани от държавите членки.

Съдът на ЕС посочва, че пръстовите отпечатъци **представляват лични данни**, тъй като обективно съдържат уникална информация за лицата и позволяват тяхното точно идентифициране, а снемането и съхраняването им представляват обработване на лични данни. Това обработване, уредено в член 1, параграф 2 от Регламент № 2252/2004, съставляват засягане на правото на зачитане на личния живот и на защита на личните данни[77]. Член 52, параграф 1 от Хартата обаче допуска ограничаване на упражняването на тези права, стига това ограничаване да е предвидено в закон, да зачита основното съдържание на тези права и ако при спазване на принципа на пропорционалност то е необходимо и ако действително отговаря на признати от Европейския съюз цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

В разглежданото дело Съдът на ЕС първо отбелязва, че ограничението, което произтича от снемането и съхраняването на пръстови отпечатъци при издаването на паспорти, трябва да се счита за **предвидено в закона**, след като тези операции са предвидени в член 1, параграф 2 от Регламент № 2252/2004. Второ, този регламент е предназначен да предотврати фалшифицирането на паспорти и незаконното им използване. Следователно член 1, параграф 2 е въведен, за да предотврати, наред с другото, незаконното влизане на лица на територията на ЕС и по този начин преследва призната от Съюза цел от общ интерес. Трето, от доказателствата, с които разполага Съдът, не следва, а впрочем не се и твърди, че наложените в случая ограничения

76 *Пак там*, параграфи 33–36.

77 *Пак там*, параграфи 27–30.

на упражняването на тези права не зачитат тяхното основно съдържание. Четвърто, съхраняването на пръстови отпечатъци върху носител с висока степен на защита на запаметената информация, предвидено от тази разпоредба, изисква високо развита технология. Такова съхраняване има вероятност да намали риска от фалшифициране на паспортите и да улесни задачата на органите, които отговарят за проверката на автентичността на паспортите на границите на ЕС. Фактът, че посоченият метод не е напълно надежден, не е от решаващо значение. Въпреки че методът не изключва изцяло допускането на неупълномощени лица, достатъчно е, че той снижава значително риска от такова допускане. Предвид горното Съдът на ЕС приема, че снемането и съхраняването на пръстови отпечатъци, посочени в член 1, параграф 2 от Регламент № 2252/2004, са подходящи за постигането на преследваните от този регламент цели и следователно и на целта да се попречи на незаконното влизане на лица на територията на ЕС[78].

След това Съдът на ЕС разглежда **необходимостта** от такова обработване, като отбелязва, че снемането се състои само във вземането на отпечатъка на два пръста, които освен това обичайно са видими за околните, така че не става въпрос за операция, която има интимен характер. Мярката също така не води до физическо или психическо увреждане на заинтересованото лице, както и изготвянето на портретната му снимка. Следва също така да се отбележи, че единствената реална алтернатива на снемането на пръстови отпечатъци, посочена в производството пред Съда, се състои в заснемането на ириса на окото. Нищо обаче в представените пред Съда документи не сочи, че последната дейност засяга в по-малка степен правата, признати от членове 7 и 8 от Хартата, отколкото снемането на пръстови отпечатъци. Освен това, що се отнася до ефикасността на последните два метода, няма съмнение, че равнището на технологична зрялост на този, основан на разпознаването на ириса, не е на равнището на този, основан на пръстовите отпечатъци, а е значително по-скъпа дейност към настоящия момент, отколкото тази по сравняването на пръстовите отпечатъци и поради това – по-неподходяща за всеобщо използване. Съответно на Съда не е известно съществуването на мерки, които биха могли да спомогнат по достатъчно ефикасен начин за целта за защита на паспортите срещу незаконното им използване, като същевременно

78 *Пак там*, параграфи 35–45.

да засягат в по-малка степен правата, признати от членове 7 и 8 от Хартата, от произтичащите в резултат на метода, основан на пръстовите отпечатъци[79].

Съдът на ЕС отбелязва, че член 4, параграф 3 от Регламент № 2252/2004 уточнява изрично, че пръстовите отпечатъци могат да бъдат използвани само с цел проверка на автентичността на паспорта и самоличността на неговия притежател, а член 1, параграф 2 от регламента предвижда съхраняването на пръстови отпечатъци само в същия паспорт, който остава в изключително държане на своя притежател. Следователно регламентът не предоставя правно основание за евентуална централизация на събраните въз основа на него данни или на използването на последните за други цели освен тази, насочена към възпрепятстване незаконното влизане на лица на територията на ЕС[80]. Като се имат предвид всички изложени по-горе съображения, Съдът на ЕС заключава, че при разглеждането на поставения въпрос не се установяват никакви обстоятелства, които могат да засегнат валидността на член 1, параграф 2 от Регламент № 2252/2004.

Връзка между Хартата и ЕКПЧ

Независимо от използваните различни формулировки, условията за законни ограничения на правата, предвидени в член 52, параграф 1 от Хартата, са сходни с тези в член 8, параграф 2 от ЕКПЧ относно правото на зачитане на личния живот. В съдебната си практика Съдът на ЕС и ЕСПЧ често се позовават взаимно на решенията си като част от постоянния диалог между двете съдилища в процеса на търсене на единно тълкуване на правилата за защита на личните данни. Член 52, параграф 3 от Хартата гласи, че „доколкото настоящата Харта съдържа права, съответстващи на права, гарантирани от Европейската конвенция за защита на правата на човека и основните свободи, техният смисъл и обхват са същите като дадените им в посочената Конвенция". Член 8 от Хартата обаче не съответства пряко на някой член от ЕКПЧ[81]. Член 52, параграф 3 от Хартата засяга съдържанието и обхвата на правата, защитени от всяка правна уредба, а не условията за тяхното ограничаване. В по-широкия контекст на диалога и сътрудничеството между двете

79 Съд на ЕС, C-291/12, *Michael Schwarz/Stadt Bochum*, 17 октомври 2013 г., параграфи 46—53.

80 *Пак там*, параграфи 56—61.

81 ЕНОЗД (2017 г.), *Necessity Toolkit*, Брюксел, 11 април 2017 г., стр. 6.

съдилища обаче, в своите анализи Съдът на ЕС може да взема предвид критериите за законни ограничения по член 8 от ЕКПЧ съгласно тяхното тълкуване от ЕСПЧ. Възможен е и обратният сценарий — ЕСПЧ да се позовава на условията за законни ограничения съгласно Хартата. Във всеки случай следва да се има предвид, че в ЕКПЧ няма абсолютен еквивалент на член 8 от Хартата, който да третира защитата на личните данни, и по-специално правата на субекта на данни, законните основания за обработване и надзора от страна на независим орган. Някои компоненти на член 8 от Хартата може да бъдат открити в развитата съдебна практика на ЕСПЧ по член 8 от ЕКПЧ и във връзка с Конвенция № 108[82]. Тази връзка гарантира взаимно вдъхновение между Съда на ЕС и ЕСПЧ по въпросите, свързани със защитата на данните.

1.3 Взаимодействие с други права и законни интереси

Ключови въпроси

- Правото на защита на личните данни често взаимодейства с други права, като свободата на изразяване на мнение и правото да се получава и разпространява информация.
- Това взаимодействие често е противоречиво: както има ситуации, в които правото на защита на личните данни е в конфликт с конкретно право, така има и такива, в които правото на защита на личните данни на практика осигурява зачитането на същото конкретно право. Такъв е случаят например със свободата на изразяване, като се има предвид, че професионалната тайна е компонент на правото на зачитане на личния живот.
- Необходимостта да се защитят правата и свободите на другите е един от критериите, използвани за оценяване на законните ограничения на правото на защита на личните данни.
- Когато става въпрос за различни права, съдилищата трябва да постигнат баланс между тях, за да ги съгласуват.
- Общият регламент относно защитата на данните изисква от държавите членки да съгласуват правото на защита на личните данни с правото на свобода на изразяване и информация.

82 Разяснения относно Хартата на основните права (2007/C 303/02), член 8.

- Държавите членки може също така да приемат конкретни правила в националните си законодателства за съгласуване на правото на защита на личните данни с публичния достъп до официални документи и задълженията за професионална тайна.

Правото на защита на личните данни не е абсолютно; по-горе бяха разгледани подробно условията за законни ограничения на това право. Един от критериите за законни ограничения на правата, признати от законодателството както на Съвета на Европа, така и на ЕС, е намесата в защитата на личните данни да е необходима, за да се защитят правата и свободите на другите. Когато защитата на личните данни взаимодейства с други права, както ЕСПЧ, така и Съдът на ЕС многократно са заявявали, че при прилагането и тълкуването на член 8 от ЕКПЧ и член 8 от Хартата е необходимо постигането на баланс спрямо другите права[83]. Няколко важни примера ще илюстрират как се постига този баланс.

Като допълнение към балансирането на правата от тези съдилища държавите може, ако е необходимо, да приемат законодателство за съгласуване на правото на защита на личните данни с другите права. По тази причина Общият регламент относно защитата на данните предоставя редица области за национална дерогация.

Що се отнася до правото на свобода на изразяване, ОРЗД изисква от държавите членки да съгласуват със закон „правото на защита на личните данни в съответствие с настоящия регламент с правото на свобода на изразяване и информация, включително обработването за журналистически цели и за целите на академичното, художественото или литературното изразяване“[84]. Държавите членки могат също така да приемат закони с цел съгласуване на защитата на данните с публичния достъп до официални документи и задълженията за опазване на професионална тайна, която е защитена като разновидност на правото на зачитане на личния живот[85].

83 ЕСПЧ, *Von Hannover/Германия (№ 2)* [голям състав], № 40660/08 и № 60641/08, 7 февруари 2012 г.; Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г., параграф 48; Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 29 януари 2008 г., параграф 68.

84 ОРЗД, член 85.

85 Пак там, член 86 и член 90.

1.3.1 Свобода на изразяване на мнение

Едно от правата, които взаимодействат най-силно с правото на защита на данните, е правото на свобода на изразяване на мнение.

Свободата на изразяване на мнение е защитена в член 11 от Хартата („Свобода на изразяване на мнение и свобода на информация"). Това право включва „свободата да отстоява своето мнение, да получава и да разпространява информация и идеи без намеса на държавните власти, и независимо от границите". Свободата на информацията съгласно член 11 от Хартата и член 10 от ЕКПЧ защитава правото не само да се съобщава, но и да се *получава* информация.

Ограниченията в свободата на изразяване на мнение трябва да са съобразени с описаните по-горе критерии, предвидени в член 52, параграф 1 от Хартата. Освен това член 11 съответства на член 10 от ЕКПЧ. Съгласно член 52, параграф 3 от Хартата, доколкото тя съдържа права, съответстващи на правата, гарантирани от ЕКПЧ, „техният смисъл и обхват са същите като дадените им в посочената Конвенция". Ограниченията, които могат да бъдат законно наложени на правото, гарантирано в член 11 от Хартата, следователно не могат да превишават предвидените в член 10, параграф 2 от ЕКПЧ, т.е. те трябва да са предвидени от закона и да са необходими в едно демократично общество „за защитата [...] на репутацията или правата на другите". Тези права обхващат най-вече правото на зачитане на личния живот и правото на защита на личните данни.

Съотношението между защитата на личните данни и свободата на изразяване на мнение се урежда в член 85 от Общия регламент относно защитата на данните, озаглавен „Обработване и свобода на изразяване и информация". Съгласно този член държавите членки съгласуват правото на защита на личните данни с правото на свобода на изразяване и информация. По-специално освобождаването и дерогацията от изискванията на конкретни глави на Общия регламент относно защитата на данните се правят за журналистически цели или за целите на академично, художествено или литературно изразяване, за да се съгласува при необходимост правото на защита на личните данни с правото на свобода на изразяване на мнение и свобода на информация.

Пример: В делото *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy*[86] от Съда на ЕС е поискано да определи съотношението между защитата на личните данни и свободата на пресата[87]. Той трябва да разгледа разпространяването от страна на дружество, чрез SMS услуги, на данъчни данни за приблизително 1,2 милиона физически лица, законно получени от финландските данъчни органи. Финландският надзорен орган за защита на данните е издал решение, което изисква дружеството да прекрати разпространяването на тези данни. Дружеството е оспорило това решение в национален съд, който е поискал разяснения от Съда на ЕС относно тълкуването на Директивата за защита на личните данни. По-специално Съдът на ЕС трябва да провери дали обработването на предоставени от данъчните органи лични данни, с цел да се даде възможност на потребителите на мобилни телефони да получават данъчни данни, отнасящи се до други физически лица, трябва да се разглежда като дейност, извършвана единствено за целите на журналистическата дейност. След като стига до заключението, че извършените от дружеството дейности представляват „обработване на лични данни" по смисъла на член 3, параграф 1 от Директивата за защита на личните данни, Съдът на ЕС анализира член 9 от директивата (относно обработването на личните данни и свободата на словото). На първо място той отбелязва значението на правото на свобода на изразяване на мнение във всяко демократично общество и постановява, че понятия, свързани с тази свобода, като журналистиката, следва да бъдат предмет на широко тълкуване. След това той отбелязва, че с цел постигане на баланс между двете основни права дерогациите и ограниченията на правото на защита на данните трябва да се прилагат само дотолкова, доколкото е строго необходимо. При тези обстоятелства Съдът на ЕС постановява, че дейности като тези, извършени от въпросните дружества, отнасящи се до данни от документи, които са обществено достояние съгласно националното законодателство, могат да бъдат класифицирани като

86 Съд на ЕС, C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy* [голям състав], 16 декември 2008 г., параграфи 56, 61 и 62.

87 Делото се отнася до тълкуването на член 9 от Директивата за защита на личните данни — който понастоящем е заменен от член 85 от Общия регламент относно защитата на данните — който гласи: „Държавите членки предвиждат изключения или дерогации от разпоредбите на настоящата глава, глава IV и глава VI относно обработването на лични данни, когато то се извършва единствено за целите на журналистическа дейност или на литературно или художествено изразяване, само ако са необходими за съгласуване на правото на личен живот и правилата, регулиращи свободата на словото."

„журналистически дейности“, ако тяхната цел е разкриване пред обществеността на информация, мнения или идеи, независимо от използвания носител за тяхното предаване. Той постановява също, че тези дейности не са ограничени до медийни дейности и могат да бъдат предприети с търговска цел. Съдът на ЕС обаче оставя на националния съд да определи дали случаят е такъв предвид конкретните факти по делото.

Същото дело е разгледано и от ЕСПЧ, след като националният съд решава, на базата на указанията от Съда на ЕС, че нареждането на надзорния орган за прекратяване на публикуването на цялата данъчна информация представлява обоснована намеса в свободата на изразяване на дружеството. ЕСПЧ потвърждава този подход[88]. Той установява, че макар и да е имало намеса в правото на дружествата да разпространяват информация, то тя е била в съответствие със закона, преследвала е легитимна цел и е била необходима в едно демократично общество.

Съдът припомня критериите от съдебната практика, от които следва да се ръководят националните органи и самият ЕСПЧ, когато балансират свободата на изразяване с правото на зачитане на личния живот. Когато става въпрос за политическа реч или дебат по въпрос от обществен интерес, тогава са налице малко възможности за ограничаване на правото да се получава и разпространява информация, тъй като обществеността има правото да бъде информирана „и това е основно право в едно демократично общество“[89]. Не може обаче да се счита, че статии в пресата, които имат за цел единствено да задоволят любопитството на определена читателска аудитория относно подробности от личния живот на дадено лице, допринасят за дебат от обществен интерес. Дерогацията от правилата за защита на данните за журналистически цели е предназначена да позволи на журналистите да имат достъп до, да събират и да обработват данни, за да могат да извършват журналистическите си дейности. Поради това действително е имало обществен интерес да се предостави достъп и да се позволи на дружествата жалбоподатели да събират и обработват въпросните

88 ЕСПЧ, *Satakunnan Markkinapörssi Oy u Satamedia Oy/Финландия* [голям състав], № 931/13, 27 юни 2017 г.

89 *Пак там*, параграф 169.

големи обеми данъчни данни. За разлика от горното Съдът установява, че не е налице обществен интерес от масовото разпространение на тези необработени данни от вестниците дословно и без никакъв анализ. Информацията за данъчното облагане може да е дала възможност на любопитни членове на обществото да категоризират лицата според техния икономически статут и да задоволят жаждата на обществеността за информация относно личния живот на другите. Не може да се счита, че това допринася за дебат от обществен интерес.

Пример: В делото *Google Spain*[90] Съдът на ЕС разглежда въпроса дали Google е длъжно да заличи остаряла информация относно финансови затруднения на жалбоподателя от списъка на резултатите от търсенето. При извършване на търсене в интернет с търсачката на Google, като се използва името на жалбоподателя, резултатите от търсенето предоставят линкове към стари статии във вестници, в които се споменава връзката му с производства по несъстоятелност. Жалбоподателят счита това за нарушение на правата му на зачитане на личния живот и на защита на личните данни, тъй като производствата са приключили преди години, което прави тези препратки неуместни.

Съдът на ЕС първо пояснява, че интернет търсачките и резултатите от търсенето, предоставящи лични данни, могат да изградят подробен профил на съответното лице. Предвид все по-цифровизиращото се общество изискването личните данни да бъдат точни и при публикуването им да не се надхвърля необходимото, т.е. да се предоставя информация на обществеността, е от основно значение за гарантирането на високо ниво на защита на данните на лицата. Лицето, което управлява търсачката „в качеството си на администратор, трябва да гарантира в рамките на своята отговорност, компетентност и възможности, че посоченото обработване на данни отговаря на изискванията“ на правото на ЕС, за да могат предвидените в него гаранции да разгърнат цялостното си действие. Това означава, че правото на заличаване на лични данни, когато обработването им вече не е необходимо или е остаряло, се разпростира и върху интернет търсачките, за които се е установило, че са и администратори, а не просто обработващи лични данни (вж. раздел 2.3.1).

90 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграфи 81–83.

При разглеждането на въпроса дали Google е трябвало да премахне линковете, свързани с жалбоподателя, Съдът на ЕС постановява, че при определени условия физическите лица имат правото да бъдат заличени техни лични данни от резултатите от търсенето чрез интернет търсачки. Към това право може да се прибегне, когато информацията, отнасяща се до лицето, не е точна, не е адекватна, не е релевантна или е прекомерна по отношение на целите на обработването на данни. Съдът на ЕС признава, че това право не е абсолютно; то трябва да бъде балансирано с други права, по-специално с интересите и правата на широката общественост да има достъп до информацията. Всяко искане за заличаване трябва да се преценява поотделно, за да се потърси баланс между основните права на защита на личните данни и на неприкосновеност на личния живот на субекта на данни, от една страна, и законните интереси на всички интернет потребители, от друга страна. Съдът на ЕС дава насоки относно факторите, които трябва да се вземат предвид при търсенето на баланс. Особено важен фактор е естеството на въпросната информация. Ако информацията е чувствителна за личния живот на лицето и няма обществен интерес към нейната наличност, тогава защитата на данните и неприкосновеността на личния живот биха имали предимство пред правото на широката общественост да има достъп до тази информация. И обратно, ако субектът на данни е обществена личност или информацията е от такъв характер, че достъпът на широката общественост до нея да е оправдан, тогава намесата в основните права на защита на личните данни и неприкосновеност на личния живот е обоснована.

След решението Работната група по член 29 прие насоки за прилагане на решението на Съда на ЕС. Насоките включват списък от общи критерии, които да бъдат използвани от надзорните органи при разглеждането на жалби, свързани с искания за заличаване на данни от страна на физически лица, и от които тези органи да се ръководят при търсенето на баланс между правата[91].

Що се отнася до съгласуването на правото на защита на данните с правото на свобода на изразяване на мнение, ЕСПЧ е издал няколко принципни решения.

91 Работна група по член 29 (2014 г.), *Насоки относно прилагането на решението на Съда на ЕС по дело Google Spain и Google Inc/Agencia Española de Protección de Datos (AEPD) и Mario Costeja González, C-131/12*, WP 225, Брюксел, 26 ноември 2014 г.

Пример: По делото *Axel Springer AG/Германия*[92] ЕСПЧ постановява, че забраната, наложена на дружеството жалбоподател да не публикува статия за арестуването и осъждането на известен актьор, е в нарушение на член 10 от ЕКПЧ. ЕСПЧ отново посочва критериите, установени в съдебната му практика, които трябва да се вземат предвид при балансирането на правото на свобода на изразяване и правото на зачитане на личния живот:

- дали въпросното публикуване на статията е било въпрос от обществен интерес;
- дали съответното лице е публична личност; и
- как е получена информацията и дали е надеждна.

ЕСПЧ констатира, че арестуването и осъждането на актьора е било публичен съдебен факт и поради това е било от обществен интерес; че актьорът е бил достатъчно известен, за да бъде квалифициран като публична личност; и че информацията е била предоставена от прокуратурата и достоверността ѝ не е била оспорена от страните. Поради това ограниченията за публикуване, наложени на дружеството, не са били пропорционални на преследваната законна цел за защита на личния живот на жалбоподателя. Съдът заключава, че е налице нарушение на член 10 от ЕКПЧ.

Пример: Делото *Coudec и Hachette Filipacchi Associés/Франция*[93] се отнася до публикация във френско седмично списание на интервю с г-жа Coste, която твърди, че принцът на Монако Албер е баща на нейния син. В интервюто се описват и връзката на г-жа Coste с принца, и начинът, по който той е реагирал на раждането на детето, придружени със снимки на принца с детето. Принц Албер завежда дело срещу издателството за нарушаване на правото му на защита на личния живот. Френските съдилища постановяват, че публикуването на статията е причинило

92 ЕСПЧ, *Axel Springer AG/Германия* [голям състав], № 39954/08, 7 февруари 2012 г., параграфи 90 и 91.

93 ЕСПЧ, *Coudec и Hachette Filipacchi Associés/Франция* [голям състав], № 40454/07, 10 ноември 2015 г.

необратими вреди на принц Албер и разпореждат издателят да плати обезщетение и да публикува подробностите от съдебното решение на предната корица на списанието.

Издателите на списанието сезират ЕСПЧ, като твърдят, че решението на френските съдилища представлява необоснована намеса в тяхното право на свобода на изразяване. ЕСПЧ трябва да намери баланс между правото на зачитане на личния живот на принц Албер, правото на изразяване на издателя и правото на широката общественост да бъде информирана. Правото на г-жа Coste да сподели историята си с обществеността, както и интересът на детето да има официално установени отношения с баща си също са важни съображения.

ЕСПЧ постановява, че публикуването на интервюто представлява намеса в личния живот на принца, като разглежда въпроса дали намесата е била необходима. Съдът приема, че публикацията засяга обществена личност и въпрос от обществен интерес, тъй като гражданите на Монако имат интерес да знаят за съществуването на дете на принца, защото бъдещето на една наследствена монархия е „неразделно свързано със съществуването на наследници“ и следователно е въпрос от значение за обществеността[94]. Съдът също така отбелязва, че статията е позволила на г-жа Coste и на нейното дете да упражнят правото си на свобода на изразяване. Националните съдилища не са обърнали надлежно внимание на принципите и критериите, развити в съдебната практика на ЕСПЧ относно намирането на баланс между правото на зачитане на личния живот и правото на свобода на изразяване. Съдът заключава, че Франция е нарушила член 10 от ЕКПЧ относно свободата на изразяване на мнение.

В съдебната практика на ЕСПЧ един от най-важните критерии по отношение на балансирането на тези права е дали въпросното изразяване на мнение допринася за дебат от обществен интерес.

94 *Пак там*, параграфи 104–116.

Пример: По делото *Mosley/Обединеното кралство*[95] национален седмичник публикува снимки от интимно естество на жалбоподателя, широко известна фигура, който впоследствие успешно завежда граждански иск срещу издателя и получава обезщетение. Въпреки присъденото парично обезщетение той подава жалба, че продължава да е жертва на нарушението на правото му на неприкосновеност на личния живот, тъй като му е била отказана възможността да поиска съдебно разпореждане преди публикуването на въпросните снимки поради липсата на правно изискване седмичникът да го уведоми преди публикуването.

ЕСПЧ отбелязва, че макар и разпространението на такъв материал да е било по-скоро с развлекателна, отколкото с образователна цел, то несъмнено се ползва от защитата, предвидена в член 10 от ЕКПЧ, но изискванията на член 8 от ЕКПЧ могат да имат превес в случаите, в които информацията е била от частно и интимно естество и нейното разпространение не е било от обществен интерес. Въпреки това е трябвало да се обърне особено внимание при разглеждането на ограниченията, които биха могли да имат функцията на форма на цензура преди публикуването. Що се отнася до възпиращия ефект, който може да бъде породен от изискването за предварително уведомяване, до съмненията за ефективността му и до голямата свобода на преценка в тази област, ЕСПЧ заключава, че съгласно член 8 не е необходимо да съществува изискване за задължително предварително уведомяване. Поради това Съдът заключава, че не е налице нарушение на член 8.

Пример: По делото *Bohlen/Германия*[96] жалбоподателят, известен певец и художествен продуцент, издава автобиографична книга и впоследствие е принуден да премахне някои пасажи от нея поради съдебни решения. Историята е широко отразена в националните медии и една тютюнева компания стартира шеговита рекламна кампания с препратка към това събитие, като използва малкото име на жалбоподателя без неговото съгласие. Жалбоподателят безуспешно подава иск за обезщетение от рекламната агенция, като се позовава на нарушение на правата си по член 8 от ЕКПЧ. ЕСПЧ отново посочва

95 ЕСПЧ, *Mosley/Обединеното кралство*, № 48009/08, 10 май 2011 г., параграфи 129 и 130.

96 ЕСПЧ, *Bohlen/Германия*, № 53495/09, 19 февруари 2015 г., параграфи 45–60.

критериите, от които трябва да се ръководи търсенето на баланс между правото на зачитане на личния живот и правото на свобода на изразяване, и постановява, че не е налице нарушение на член 8. Жалбоподателят е обществена личност и рекламата съдържа препратки не към подробности от личния му живот, а към публично събитие, което вече е отразено в медиите и е част от обществен дебат. Освен това рекламата има хумористичен характер и не съдържа нищо унизително или отрицателно по отношение на жалбоподателя.

Пример: По делото *Biriuk/Литва*[97] жалбоподателката твърди пред ЕСПЧ, че Литва не е изпълнила задължението си да гарантира правото на зачитане на нейния личен живот, защото въпреки че голям вестник е нарушил сериозно неприкосновеността на личния ѝ живот, националните съдилища, които са разглеждали делото, са ѝ присъдили незначителна сума за имуществени вреди. При присъждане на неимуществените вреди националните съдилища са приложили разпоредбите на националното законодателство относно предоставянето на информация на обществеността, които налагат нисък таван на обезщетение за неимуществени вреди, причинени от незаконното разпространение сред обществеността на информация за личния живот на дадено лице от страна на медиите. Делото е възбудено поради публикация на уводна статия в най-големия литовски ежедневник, в която се съобщава, че жалбоподателката е ХИВ позитивна. В статията освен това се критикува поведението на жалбоподателката и се поставят под въпрос нейните морални норми.

ЕСПЧ припомня, че защитата на личните данни, не на последно място на медицинските данни, е от особена важност за правото на зачитане на личния живот съгласно ЕКПЧ. Поверителността на данните относно здравословното състояние е особено важна, тъй като разкриването на медицински данни (в случая ХИВ статута на жалбоподателката) може драстично да засегне личния и семейния живот на лицето, трудовата му заетост и приобщаването му в обществото. Съдът придава особена важност на факта, че според статията във вестника информацията относно ХИВ статута на жалбоподателката е предоставена от медицинския

97 ЕСПЧ, *Biriuk/Литва*, № 23373/03, 25 ноември 2008 г.

персонал в болницата, което е явно нарушение на неговото задължение да пази медицинска тайна. Следователно не е налице законна намеса в правото на личен живот на жалбоподателката.

Статията е публикувана в пресата, а свободата на изразяване също е основно право съгласно ЕКПЧ. При разглеждането на въпроса дали наличието на обществен интерес е оправдавало публикуването на такъв тип информация относно жалбоподателката обаче Съдът констатира, че основната цел на публикацията е била да се увеличат продажбите на вестника чрез удовлетворяване на любопитството на читателя. Не може да се счита, че тази цел допринася за какъвто и да е дебат от общ интерес за обществото. Тъй като това е случай на „възмутителна злоупотреба със свободата на печата“, тежките ограничения за обезщетяването на вредите и ниската сума на обезщетенията за неимуществени вреди, предвидени в националното законодателство, означават, че Литва не е изпълнила позитивното си задължение да защити правото на жалбоподателката на неприкосновеност на личния живот. ЕСПЧ констатира, че е налице нарушение на член 8 от ЕКПЧ.

Правото на свобода на изразяване и правото на защита на личните данни не винаги са в конфликт. Има случаи, в които ефективната защита на личните данни гарантира свободата на изразяване.

Пример: По делото *Tele2 Sverige* Съдът на ЕС постановява, че намесата, предизвикана от Директива 2006/24 (Директивата за запазване на лични данни) в основните права, установени в членове 7 и 8 от Хартата, е „силно изразена и трябва да се счита за особено тежка. Наред с това обстоятелството, че запазването на данните и последващото им използване се осъществяват, без абонатът или регистрираният ползвател да са информирани за това, може да породи усещане в съзнанието на съответните лица, че личният им живот е обект на постоянно наблюдение“. Съдът на ЕС счита също така, че запазването на общо основание на данни за трафик и на данни за местонахождение би могло да даде отражение върху използването на електронните съобщителни средства и „следователно върху упражняваната от тях

свобода на изразяване на мнение, гарантирана от член 11 от Хартата“[98]. В този смисъл, като изискват строги гаранции, че запазването на данни няма да се извършва на общо основание, правилата за защита на данните в крайна сметка допринасят за упражняването на свободата на изразяване.

Що се отнася до правото да се получава информация, което също е част от свободата на изразяване, значението на прозрачността на управлението за функционирането на едно демократично общество се осъзнава във все по-голяма степен. Прозрачността е цел от общ интерес, която следователно би могла да оправдае намеса в правото на защита на личните данни, ако такава намеса е необходима и пропорционална, както е обяснено в раздел 1.2. Вследствие на това през изминалите две десетилетия правото на достъп до документи, съхранявани от публичните органи, беше признато като основно право на всеки гражданин на ЕС, както и на всяко физическо или юридическо лице, което пребивава или е със седалище в държава членка.

Съгласно правото на Съвета на Европа може да се прави позоваване на принципите, установени в Препоръката относно достъпа до официални документи, която е вдъхновила създателите на Конвенцията относно достъпа до официални документи (Конвенция № 205)[99].

Съгласно правото на ЕС правото на достъп до документи е гарантирано в Регламент (ЕО) № 1049/2001 относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (Регламент относно достъпа до документи)[100]. Член 42 от Хартата и член 15, параграф 3 от ДФЕС разшириха това право на достъп „до документите на институциите, органите, службите и агенциите на Съюза, независимо от вида на техния носител“.

98 Съд на ЕС, съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], 21 декември 2016 г. параграфи 37 и 101; Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г., параграф 28.

99 Съвет на Европа, Комитет на министрите (2002 г.), Препоръка Rec(81)19 и Препоръка Rec(2002)2 до държавите членки относно достъпа до официални документи, 21 февруари 2002 г., Съвет на Европа, Конвенция относно достъпа до официални документи, CETS № 205, 18 юни 2009 г. Конвенцията все още не е влязла в сила.

100 Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 година относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията, ОВ L 145, 31.5.2001 г.

Това право може да влезе в противоречие с правото на защита на данните, в случай че достъпът до даден документ би разкрил лични данни на други лица. Член 86 от Общия регламент относно защитата на данните ясно предвижда, че лични данни в официални документи, държани от публични органи или структури, могат да бъдат разкривани от тези органи или структури в съответствие с правото на Съюза[101] или правото на държавата членка, за да се съгласува публичният достъп до официални документи с правото на защита на личните данни в съответствие с регламента.

Поради това, по отношение на исканията за достъп до документи или данни, съхранявани от публичните органи, може да е необходимо балансиране на правото на защита на личните данни на лицата, чиито данни се съдържат в исканите документи.

Пример: По делото *Volker und Markus Schecke u Hartmut Eifert/Land Hessen*[102] Съдът на ЕС трябва да прецени пропорционалността на изискването по законодателството на ЕС публикуване на имената на бенефициентите на селскостопански субсидии от ЕС и на получените от тях суми. Публикуването има за цел да увеличи прозрачността и да допринесе за обществения контрол върху правилното използване на публични средства от страна на администрацията. Няколко бенефициенти са оспорили пропорционалността на това публикуване.

Съдът на ЕС, като отбелязва, че правото на защита на данните не е абсолютно право, заявява, че публикуването в уебсайт на поименни данни относно бенефициентите по двата фонда на ЕС за селскостопански помощи и точните размери на получените от тях суми представлява намеса в личния им живот като цяло, и по-специално в защитата на техните лични данни.

Съдът на ЕС приема, че тази намеса по отношение на членове 7 и 8 от Хартата е предвидена от закона и изпълнява призната от ЕС цел от общ интерес, а именно повишаване на прозрачността на използването на общностни фондове. Съдът на ЕС обаче постановява, че публикуването на имената на физическите лица — бенефициенти на селскостопанска

101 Член 42 от Хартата, член 15, параграф 3 от ДФЕС и Регламент № 1049/2009.

102 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г., параграфи 47—52, 58, 66—67, 75, 86 и 92.

помощ от ЕС, по линия на тези два фонда, както и на точните размери на получените от тях суми представлява непропорционална мярка и не е обосновано от гледна точка на член 52, параграф 1 от Хартата. Съдът признава колко е важно в едно демократично общество данъкоплатците да бъдат информирани относно използването на публичните средства. Тъй като обаче „не би могло да се признае, че целта за прозрачност автоматично има превес над правото на защита на личните данни“[103], институциите на ЕС са били длъжни да намерят баланс между интереса на Съюза относно прозрачността и ограничението в упражняването на правата на неприкосновеност на личния живот и защита на данните, понесено от бенефициентите в резултат на публикацията.

Съдът на ЕС счита, че търсенето на баланс от институциите на ЕС не е извършено по подходящ начин, тъй като е било възможно да се предвидят мерки, които биха засегнали не толкова неблагоприятно основните права на лицата, като в същото време биха допринесли ефективно за целта за прозрачност, преследвана с публикацията. Например вместо обща публикация, засягаща всички бенефициенти, в която се посочват името и точният размер на получените суми от всеки от тях, би могло да се направи разграничение въз основа на подходящи критерии, например периодите, през които тези лица са получили помощта, честотата на получаването ѝ или нейния размер и вид[104]. Поради тази причина Съдът на ЕС обяви за частично недействително законодателството на ЕС относно публикуването на информация, свързана с бенефициентите по европейски земеделски фондове.

Пример: По делото *Rechnungshof/Österreichischer Rundfunk и други*[105] Съдът на ЕС прави преглед на съвместимостта на някои австрийски законодателни актове с правото на ЕС за защита на данните. Законодателството изисква държавните органи да събират и предават данни за доходите за целите на публикуването на името и доходите на служителите от различните публични организации в годишен доклад, който е достъпен за широката общественост. Някои лица са отказали да съобщят данните си, като се позовават на защитата на данните.

103 *Пак там*, параграф 85.

104 *Пак там*, параграф 89.

105 Съд на ЕС, съединени дела C-465/00, C-138/01 и C-139/01, *Rechnungshof/Österreichischer Rundfunk и други и Christa Neukomm и Jospeh Lauermann/Österreichischer Rundfunk*, 20 май 2003 г.

В становището си Съдът на ЕС се опира на защитата на основните права като общ принцип на правото на ЕС и на член 8 от ЕКПЧ, като припомня, че по това време Хартата не е била задължителна. Съдът постановява, че събирането на данни за трудовите доходи на дадено лице, и по-специално съобщаването им на трети страни, попада в обхвата на правото на зачитане на личния живот и представлява нарушение на това право. Намесата би могла да бъде обоснована, ако е в съответствие със закона, преследва легитимна цел и е необходима за постигането на тази цел в едно демократично общество. Съдът на ЕС отбелязва, че австрийското законодателство преследва легитимна цел, тъй като стремежът е заплатите на държавните служители да се запазят в разумни граници — съображение, което е свързано и с икономическото благосъстояние на страната. Интересът на Австрия да гарантира оптималното използване на публичните средства обаче трябва да бъде балансиран с тежестта на намесата в правото на лицата на зачитане на личния им живот.

Като оставя на националните съдилища да установят дали публикуването на данните за доходите на лицата е било необходимо и пропорционално на преследваната от законодателството цел, Съдът на ЕС призовава националния съд да прецени дали тази цел не би могла да бъде постигната също толкова ефективно чрез използването на средства с по-малка степен на намеса. Пример за това би бил личните данни да се предават само на контролните публични органи, а не на широката общественост.

В последващи дела стана очевидно, че намирането на баланс между защитата на данните и достъпа до документи изисква подробен анализ във всеки отделен случай. Нито едно от правата не може автоматично да вземе превес над другото. Съдът на ЕС имаше възможност да даде тълкуване на правото на достъп до документи, съдържащи лични данни, в две дела.

Пример: По делото *Европейска комисия/Bavarian Lager*[106] Съдът на ЕС определя обхвата на защитата на лични данни в контекста на достъпа до документи на институциите на ЕС и връзката между Регламент (ЕО) № 1049/2001 (Регламента относно достъпа до документи)

106 Съд на ЕС, C-28/08 P, *Европейска комисия/The Bavarian Lager Co. Ltd* [голям състав], 29 юни 2010 г.

и Регламент (ЕО) № 45/2001 (Регламента относно защитата на данните при обработването им от институции на ЕС). Bavarian Lager, учредено през 1992 г., внася бутилирана немска бира в Обединеното кралство, предимно за кръчми и барове. То обаче се сблъсква с трудности, тъй като британското законодателство *де факто* облагодетелства националните производители. В отговор на жалбата на Bavarian Lager Европейската комисия завежда дело срещу Обединеното кралство за неизпълнение на неговите задължения, вследствие на което Обединеното кралство изменя спорните разпоредби и ги привежда в съответствие с правото на ЕС. След това Bavarian Lager иска от Комисията, наред с други документи, копие от протокола от събрание, на което са присъствали представители на Комисията, на британските органи и *Confédération des Brasseurs du Marché Commun* (CBMC). Комисията се съгласява да оповести някои документи във връзка със събранието, но заличава пет имена в протокола, тъй като две лица изрично са се противопоставили на оповестяването на тяхната самоличност, а с другите три Комисията не е успяла да установи контакт. С решение от 18 март 2004 г. Комисията отхвърля новото искане на Bavarian Lager за получаване на пълния протокол от събранието, позовавайки се по-специално на защитата на личния живот на тези лица, гарантирана в Регламента относно защитата на данните при обработването им от институции на ЕС.

Тъй като не е удовлетворено от тази позиция, Bavarian Lager подава жалба пред Първоинстанционния съд. Този съд отменя решението на Комисията с решение от 8 ноември 2007 г. (дело T-194/04, *The Bavarian Lager Co. Ltd/Комисия на европейските общности*), като се произнася, че самото вписване на имената на въпросните лица в списъка на лицата, присъствали на събрание, от името на органа, който те представляват, не накърнява неприкосновеността на техния личен живот и не застрашава личния живот на тези лица.

При обжалване от страна на Комисията Съдът на ЕС отменя решението на Първоинстанционния съд. Съдът на ЕС постановява, че Регламентът относно достъпа до документи установява „специфичен засилен режим на защита на лице, чиито лични данни евентуално биха могли да бъдат предоставени на обществеността“. Според Съда на ЕС в случаите, когато чрез искане, основано на Регламента относно достъпа до документи, се цели получаването на достъп до документи, които съдържат лични данни, разпоредбите на Регламента относно защитата на данните при

обработването им от институции на ЕС стават приложими в тяхната цялост. След това Съдът на ЕС заключава, че Комисията е имала право да отхвърли заявлението за достъп до пълния протокол от събранието от октомври 1996 г. При липсата на съгласие от петимата участници в това събрание Комисията е спазила в достатъчна степен задължението си за откритост, като е оповестила версия на въпросния документ, в която техните имена са заличени.

Освен това според Съда на ЕС „тъй като Bavarian Lager не е предоставило никаква изрична и легитимна обосновка, нито убедителен довод, за да докаже необходимостта от предаване на тези лични данни, Комисията не е могла да претегли различните интереси на съответните страни. Тя не е могла и да провери дали няма основания да се предполага, че това предаване би могло да засегне легитимните интереси на субектите на данните", както се изисква от Регламента относно защитата на данните при обработването им от институции на ЕС.

Пример: По делото *Client Earth, PAN Europe/ЕОБХ*[107] Съдът на ЕС разглежда въпроса дали решението на Европейския орган за безопасност на храните (ЕОБХ) да откаже на жалбоподателите пълен достъп до документи е било необходимо за защитата на неприкосновеността на личния живот и правата на защита на данните на лицата, за които документите се отнасят. Документите касаят проект за насоки, изготвен от работната група на ЕОБХ в сътрудничество с външни експерти, относно пускането на пазара на продукти за растителна защита. Първоначално ЕОБХ е разрешил частичен достъп на жалбоподателите, като е отказал достъп до някои работни версии на проекта за насоки. Впоследствие органът е разрешил достъп до версията на проекта, която е съдържала отделните становища на външните експерти. Той обаче е заличил имената на експертите, позовавайки се на член 4, параграф 1, буква б) от Регламент № 45/2001 относно обработването на лични данни от институции и органи на Общността и необходимостта да се защити неприкосновеността на личния живот на външните експерти. На първа инстанция Общият съд на ЕС потвърждава решението на ЕОБХ.

107 Съд на ЕС, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Европейски орган за безопасност на храните (ЕОБХ), Европейска комисия*, 16 юли 2015 г.

При обжалване от страна на жалбоподателите Съдът на ЕС отменя решението на първата инстанция. Съдът на ЕС заключава, че предаването на лични данни в този случай е било необходимо, за да се провери безпристрастността на всеки от външните експерти при изпълнение на научното им задание и за да се гарантира, че процесът на вземане на решения от ЕОБХ продължава да е прозрачен. Според Съда на ЕС ЕОБХ не е определил точно по какъв начин разкриването на имената на външните експерти, които са изразили конкретни становища по проекта за насоки, би могло да засегне техните легитимни интереси. Общият довод, че оповестяването има вероятност да накърни неприкосновеността на личния живот не е достатъчен, ако не е подкрепен от конкретно доказателство във всеки отделен случай.

Съгласно тези решения е необходима конкретна и основателна причина за намеса в правото на защита на данните във връзка с достъпа до документи. Правото на достъп до документи не може автоматично да отменя правото на защита на данните[108].

Този подход е аналогичен на подхода на ЕСПЧ по отношение на неприкосновеността на личния живот и достъпа до документи, както показват решенията по-долу. В решението по делото *Magyar Helsinki* ЕСПЧ посочва, че член 10 не предоставя на физическите лица правото на достъп до информация, притежавана от публичен орган, нито задължава правителството да предаде такава информация на физическите лица. Такова право или задължение обаче би могло да възникне: първо, когато разкриването на информацията е наложено от влязло в сила съдебно разпореждане; второ, когато достъпът до информацията способства за упражняване на правото на лицето на свобода на изразяване — особено свободата да получава и разпространява информация — и когато отказът би засегнал това право[109]. Дали и до каква степен отказът на достъп до информация представлява намеса в свободата на изразяване на заявителя трябва да се оценява за всеки отделен случай и в светлината на конкретните обстоятелства, включително: i) целта на искането за достъп до информация; ii) естеството на търсената информация; iii) ролята на заявителя; и iv) дали информацията е готова и налична.

108 Вж. обаче подробните обсъждания на ЕНОЗД (2011 г.), *Публичен достъп до съдържащи лични данни документи след решението по делото* Bavarian Lager, Брюксел, 24 март 2011 г.

109 ЕСПЧ, *Magyar Helsinki Bizottság/Унгария* [голям състав], № 18030/11, 8 ноември 2016 г., параграф 148.

Пример: По делото *Magyar Helsinki Bizottság/Унгария*[110] жалбоподателят, неправителствена организация в областта на човешките права, иска информация от полицията относно работата на служебен защитник, за да завърши проучване относно функционирането на системата на обществените защитници в Унгария. Полицията отказва да предостави информацията, като изтъква, че тя представлява лични данни, които не подлежат на разкриване. Като прилага посочените по-горе критерии, ЕСПЧ постановява, че е налице намеса в право, защитено съгласно член 10. По-точно жалбоподателят е искал да упражни правото на предоставяне на информация по въпрос от обществен интерес, за тази цел е потърсил достъп до информация и информацията му е била необходима, за да упражни правото си на свобода на изразяване. Информацията относно назначаването на обществени защитници представлява интерес за обществеността. Няма причина за съмнение, че въпросното проучване е съдържало информация, която жалбоподателят се е ангажирал да предостави на обществеността и която обществеността е имала правото да получи. Поради това Съдът е убеден, че достъпът до поисканата информация е бил необходим, за да може жалбоподателят да изпълни задачата си. И накрая, информацията е била готова и налична.

ЕСПЧ заключава, че в този случай отказът на достъп до информация е нарушил самата същност на свободата на получаване на информация. За да достигне до това заключение, той разглежда по-специално целта на исканата информация и нейния принос към важен обществен дебат, естеството на търсената информация и дали тя е от обществен интерес, както и ролята в обществото на жалбоподателя по делото.

В мотивите си Съдът отбелязва, че проучването, предприето от неправителствената организация, се отнася до функционирането на правосъдието и правото на справедливо изслушване, което е право от първостепенно значение съгласно ЕКПЧ. Тъй като исканата информация не включва данни, които не са обществено достояние, правата на неприкосновеност на личния живот на засегнатите субекти на данни (служебните обществени защитници) е нямало да бъдат засегнати, ако полицията беше предоставила достъп на жалбоподателя до информацията. Исканата от жалбоподателя информация е със

110 *Пак там*, параграфи 181, 187–200.

статистически характер и се отнася до това колко пъти служебни защитници са били назначавани да представляват ответниците в публични наказателни производства.

Като се има предвид, че проучването има за цел да допринесе за важен дебат по въпрос от обществен интерес, за Съда всякакви ограничения на предложената публикация на НПО е следвало да бъдат подложени на най-строг контрол. Въпросната информация е от обществен интерес, тъй като общественият интерес обхваща „въпроси, които могат да породят значителни противоречия, които засягат важен обществен въпрос или включват проблем, за който обществеността има интерес да бъде информирана“[111]. Следователно тя със сигурност обхваща дискусия относно правораздаването и справедливия съдебен процес, което е предмет на проучването на жалбоподателя. Като балансира различните права по случая и прилага принципа на пропорционалност, ЕСПЧ постановява, че е налице неоправдано нарушение на правата на жалбоподателя съгласно член 10 от ЕКПЧ.

1.3.2 Професионална тайна

Съгласно националното законодателство за някои съобщения може да е приложимо задължението за професионална тайна. Професионалната тайна може да се разбира като специален етичен ангажимент, който поражда законово задължение, присъщо на определени професии и дейности, които се основават на доверие. Лицата и институциите, които изпълняват тези функции, са длъжни да не разкриват поверителна информация, която са получили в хода на изпълнението на своите задължения. Професионалната тайна е приложима най-вече за медицинската професия и за отношенията между адвокат и клиент, като много от юрисдикциите признават задължение за професионална тайна и във финансовия сектор. Професионалната тайна не е основно право, но е защитена като разновидност на правото на зачитане на личния живот. Например Съдът на ЕС е постановил, че в определени случаи „може да се наложи да се забрани разгласяването на определени сведения, квалифицирани като поверителни, с цел да се защити основното право на дадено предприятие на личен живот, закрепено в член 8 от ЕКПЧ и в член 7 от

111 *Пак там*, параграф 156.

Хартата“[112]. ЕСПЧ е трябвало да се произнесе и дали ограниченията на професионалната тайна представляват нарушение на член 8 от ЕКПЧ, както е показано в посочените примери.

Пример: По делото *Pruteanu/Румъния*[113] жалбоподателят действа като адвокат на търговско дружество, на което е забранено да извършва банкови транзакции вследствие на твърдения за измама. По време на разследването на случая румънските съдилища издават разрешение на органите на прокуратурата да подслушват и записват телефонните разговори на партньор на дружеството за определен период. Записите и подслушванията включват и разговорите му с неговия адвокат.

Г-н Pruteanu твърди, че това е намеса в правото му на зачитане на неговия личен живот и кореспонденция. В своето решение ЕСПЧ подчертава статута и важността на отношенията между адвокат и клиент. Подслушването на разговорите между адвокат и неговия клиент несъмнено е нарушило професионалната тайна, която е в основата на отношенията между тях. В такъв случай адвокатът също е могъл да подаде жалба за намеса в неговото право на зачитане на личния живот и кореспонденция. С оглед на горното Съдът на ЕС постановява, че е налице нарушение на член 8 от ЕКПЧ.

Пример: По делото *Brito Ferrinho Bexiga Villa-Nova/Португалия*[114] жалбоподателката, която е адвокат, отказва да покаже личните си банкови извлечения на данъчните органи, като се позовава на професионалната и банковата тайна. Прокуратурата започва разследване за данъчна измама и отправя искане за разрешение за спиране на действието на професионалната тайна. Националните съдилища разпореждат преустановяване на прилагането на правилата за поверителност и банкова тайна с констатацията, че общественият интерес следва да има преимущество над частните интереси на жалбоподателката.

112 Съд на ЕС, T-462/12 R, *Pilkington Group Ltd/Европейска комисия*, Определение на председателя на Общия съд от 11 март 2013 г., параграф 44.

113 ЕСПЧ, *Pruteanu/Румъния*, № 30181/05, 3 февруари 2015 г.

114 ЕСПЧ, *Brito Ferrinho Bexiga Villa-Nova/Португалия*, № 69436/10, 1 декември 2015 г.

След сезиране на ЕСПЧ Съдът постановява, че достъпът до банковите извлечения на жалбоподателката представлява намеса в правото ѝ на зачитане на професионалната тайна, която попада в обхвата на личния живот. Намесата е имала правно основание, тъй като се основава на Наказателно-процесуалния кодекс и преследва легитимна цел. При разглеждането на необходимостта и пропорционалността на намесата обаче ЕСПЧ изтъква факта, че производството за преустановяване на поверителността е било проведено без участието или знанието на жалбоподателката. Поради това жалбоподателката не е могла да представи своите аргументи. Освен това, макар и националното законодателство да предвижда, че в такива производства трябва да се провеждат консултации с адвокатската колегия, такава консултация не е била проведена. И накрая, жалбоподателката не е разполагала с възможност ефективно да оспори преустановяването на поверителността, нито с някакво средство за защита, чрез което да оспори мярката. Поради липсата на процесуални гаранции и ефективен съдебен контрол върху мярката, преустановяваща задължението за поверителност, ЕСПЧ заключава, че е налице нарушение на член 8 от ЕКПЧ.

Взаимодействието между професионалната тайна и защитата на данните често е противоречиво. От една страна, правилата за защита на данни и гаранциите, установени в законодателството, помагат да се гарантира професионалната тайна. Например правилата, които изискват от администраторите и обработващите лични данни да прилагат строги мерки за сигурност, имат за цел да предотвратят, наред с другото, нарушаването на поверителността на личните данни, защитени от професионалната тайна. Освен това Общият регламент относно защитата на данните на ЕС позволява обработването на здравни данни, представляващи специална категория лични данни, които се нуждаят от по-строга защита, но поставя това обработване в зависимост от съществуването на подходящи и конкретни мерки за защита на правата на субектите на данни, по-специално професионалната тайна[115].

От друга страна, задълженията за професионална тайна, наложени на администраторите и обработващите лични данни по отношение на определени лични данни, могат да ограничат правата на субектите на данни, най-вече

115 Общ регламент относно защитата на данните, член 9, параграф 2, буква з) и член 9, параграф 3.

правото да получават информация. Макар и Общият регламент относно защитата на данните да съдържа обширен списък с информация, която по принцип трябва да се предоставя на субекта на данните, когато личните данни не са получени от него, това изискване за оповестяване не се прилага, когато личните данни трябва да останат поверителни поради задължение за опазване на професионална тайна, което се изисква от националното право или правото на ЕС[116].

Общият регламент относно защитата на данните предвижда възможността държавите членки да приемат със закон конкретни правила, за да гарантират задължението за опазване на професионална тайна или на други равностойни задължения за опазване на тайна и да съгласуват правото на защита на личните данни със задължението за опазване на професионална тайна[117].

ОРЗД предвижда, че държавите членки могат да приемат специални правила относно правомощията на надзорните органи по отношение на администраторите или обработващите лични данни, които са обвързани със задължение за опазване на професионална тайна. Тези специални правила се отнасят до правомощието да получават достъп до помещенията на администратора или обработващия лични данни, до неговото оборудване за обработване и съхраняване на лични данни, когато тези лични данни са били получени в хода на дейност, обхваната от задължението за опазване на тайна. Следователно надзорните органи, на които е поверена защитата на данните, трябва да спазват задълженията за опазване на професионална тайна, които обвързват администраторите и обработващите лични данни. Освен това както по време на мандата си, така и след неговото приключване самите членове на надзорните органи също са обвързани от задължението за опазване на професионална тайна. Поверителна информация може да стане достояние на членовете и персонала на надзорните органи по време на изпълнението на техните задачи. В член 54, параграф 2 от регламента е предвидено ясно, че те са обвързани от задължението за опазване на професионална тайна по отношение на такава поверителна информация.

ОРЗД изисква държавите членки да уведомяват Комисията за правилата, които са приели за съгласуване на защитата на данните и принципите, установени в регламента, със задължението за опазване на професионална тайна.

116 *Пак там*, член 14, параграф 5, буква г).

117 *Пак там*, съображение 164 и член 90.

1.3.3 Свобода на религията и убежденията

Свободата на религията и убежденията е защитена съгласно член 9 от ЕКПЧ (свобода на мисълта, съвестта и религията) и член 10 от Хартата на основните права на Европейския съюз. Лични данни, които разкриват религиозни или философски убеждения, се считат за „чувствителни данни“ както съгласно правото на ЕС, така и съгласно правото на Съвета на Европа, и тяхното обработване и използването им подлежат на засилена защита.

Пример: Жалбоподателят по делото *Sinak Isik/Турция*[118] е член на религиозната общност на алевитите, чиято вяра е повлияна от суфизма и други пред-ислямски религиозни течения и се счита от някои учени за отделна религия, а от други — за част от ислямската религия. Жалбоподателят се оплаква, че против неговото желание личната му карта съдържа поле, в което религията му се посочва като „ислям“, а не като „алеви“. Националните съдилища отхвърлят искането му вероизповеданието в личната му карта да бъде променено на „алеви“ с мотива, че тази дума обозначава подгрупа на исляма, а не отделна религия. Тогава той подава жалба пред ЕСПЧ, че е бил задължен да разкрие вярата си без негово съгласие, тъй като върху личната карта е било задължително да се посочи религията на лицето и това нарушава правото му на свобода на религията и съвестта, особено като се има предвид, че посочването на „ислям“ върху личната му карта е било неправилно.

ЕСПЧ потвърждава, че религиозната свобода включва свободата едно лице да изповядва своята религия колективно, публично и в кръга на лицата, изповядващи същата вяра, но също индивидуално и частно. Приложимото към съответния момент национално законодателство задължава лицата да носят лична карта — документ, който трябва да бъде показван при поискване от всеки публичен орган или частно предприятие, в който документ се посочва тяхното вероизповедание. Това задължение не отчита, че в правото едно лице да изповядва религията си се съдържа и обратното право, т.е. че едно лице не е длъжно да разкрива убежденията си. Макар и правителството да твърди, че националното законодателство е било променено, така че лицата да могат да изискват полето за религия в личните им карти да

118 ЕСПЧ, *Sinan Işık/Турция*, № 21924/05, 2 февруари 2010 г.

бъде оставено празно, според Съда самият факт, че трябва да се подава молба за заличаване на религиозната принадлежност, би могъл да представлява разкриване на информация за отношението на лицето към религията. Освен това когато личните карти имат поле, указващо религията, оставянето му празно носи специално значение, тъй като притежателите на лична карта без информация относно религията биха се откроили от онези, които имат карта, показваща техните убеждения. ЕСПЧ заключава, че националното законодателство е в нарушение на член 9 от ЕКПЧ.

Дейността на църквите и религиозните сдружения или общности обаче може да изисква обработването на личната информация на техните членове, за да се осигури възможност за комуникация и организиране на дейностите в религиозната общност. Поради тази причина църквите и религиозните сдружения често прилагат правила относно обработването на лични данни. В съответствие с член 91 от Общия регламент относно защитата на данните, когато такива правила са цялостни, те може да продължат да се прилагат, при условие че са приведени в съответствие с разпоредбите на регламента. Църквите и религиозните сдружения, които прилагат такива правила, подлежат на контрол от страна на независим надзорен орган, който може да е специален за тях, при условие че изпълняват изискванията на Общия регламент относно защитата на данните за тези органи[119].

Религиозните организации може да извършват обработване на лични данни по няколко причини — например за да поддържат връзка със своите паства или да информират за религиозни празници или благотворителни мероприятия. В някои държави църквите трябва да поддържат регистри на членовете си за данъчни цели, тъй като членството в религиозни учреждения може да повлияе на дължимите от физическите лица данъци. Във всеки случай съгласно европейското право данни, разкриващи религиозни убеждения, са чувствителни данни и църквите трябва да отговарят за тяхното съхраняване и обработване, особено като се има предвид че информацията, обработвана от религиозните организации, често касае деца, възрастни хора или други уязвими членове на обществото.

119 Общ регламент относно защитата на данните, член 91, параграф 2.

1.3.4 Свобода на изкуствата и науките

Друго право, което трябва да бъде балансирано спрямо правата на неприкосновеност на личния живот и на защита на данните, е свободата на изкуствата и науките, изрично защитена съгласно член 13 от Хартата на основните права на Европейския съюз. Това право произтича основно от свободата на мисълта и на изразяване на мнение и трябва да се упражнява, като се взема предвид член 1 от Хартата („Човешко достойнство"). ЕСПЧ счита, че свободата на изкуствата е защитена съгласно член 10 от ЕКПЧ[120]. Правото, гарантирано от член 13 от Хартата, също може да е предмет на ограниченията в съответствие с член 52, параграф 1 от Хартата, който може да се тълкува и през призмата на член 10, параграф 2 от ЕКПЧ[121].

Пример: По дело *Vereinigung bildender Kunstler/Австрия*[122] австрийските съдилища забраняват на сдружението жалбоподател да продължи да излага на показ картина, която съдържа фотоизображения на главите на редица публични личности в сексуални пози. Австрийски парламентарист, чиято снимка е била използвана в картината, предявява иск срещу сдружението жалбоподател, като иска съдебна възбрана срещу показването на картината. Националният съд издава заповед за възбрана. ЕСПЧ отново посочва, че член 10 от ЕКПЧ е приложим по отношение на разпространяването на идеи, които обиждат, шокират или смущават държавата или определена част от населението. Лицата, които създават, представят, разпространяват или показват произведения на изкуството, допринасят за обмена на идеи и мнения и държавата има задължението да не накърнява неправомерно свободата им на изразяване. Като се има предвид, че картината е колаж и са използвани само фотоизображения на главите на лицата и че телата им са изобразени по нереалистичен и преувеличен начин, който очевидно не цели да отразява или дори да загатва реалността, ЕСПЧ заявява още, че „картината едва ли би могла да се разбира като представяща подробности от личния живот на [изобразеното лице], а по-скоро е свързана с неговото обществено положение като политик" и че „в това си качество [изобразеното лице] е трябвало да прояви по-голяма толерантност по отношение на

120 ЕСПЧ, *Müller и други/Швейцария*, № 10737/84, 24 май 1988 г.

121 Разяснения относно Хартата на основните права, ОВ C 303, 14.12.2007 г.

122 ЕСПЧ, *Vereinigung bildender Künstler/Австрия*, № 68354/01, 25 януари 2007 г., параграфи 26 и 34.

критиките“. Претегляйки различните изложени на опасност интереси, ЕСПЧ установява, че неограничената възбрана на по-нататъшното показване на картината е непропорционална. Съдът заключава, че е налице нарушение на член 10 от ЕКПЧ.

Европейското право в областта на защитата на данните признава също така специалното значение на науката за обществото. Общият регламент относно защитата на данните и модернизираната Конвенция № 108 разрешават запазването на личните данни за по-дълги срокове, доколкото те ще бъдат обработвани единствено за целите на научни или исторически изследвания. Освен това, и независимо от първоначалната цел на конкретно обработване на личните данни, по-нататъшното им използване за научни изследвания не се счита за несъвместимо с първоначалната цел[123]. В същото време трябва да се прилагат подходящи гаранции по отношение на такова обработване на данни, за да се защитят правата и свободите на субектите на данните. Правото на ЕС или на държавите членки може да предвижда дерогации от правата на субекта на данни, като например на правото на достъп, на коригиране, на ограничаване на обработването и на възражение, когато става въпрос за обработването на лични данни за научни изследвания, исторически или статистически цели (вж. също раздел 6.1 и раздел 9.4).

1.3.5 Защита на интелектуалната собственост

Правото на защита на собствеността е установено в член 1 от Първия протокол към ЕКПЧ, както и в член 17, параграф 1 от Хартата на основните права на ЕС. Важен аспект на правото на собственост, който е от особено значение за защитата на данните, е защитата на интелектуалната собственост, изрично посочена в член 17, параграф 2 от Хартата. Няколко директиви в правния ред на ЕС имат за цел ефективна защита на интелектуалната собственост, и по-специално на авторското право. Интелектуалната собственост обхваща не само литературната и художествената собственост, но и патентите, търговските марки и сродните права.

Както ясно показва съдебната практика на Съда на ЕС, защитата на основното право на собственост трябва да бъде балансирана спрямо защитата на други

123 Общ регламент относно защитата на данните, член 5, параграф 1, буква б) и модернизираната Конвенция № 108, чл. 5, параграф 4, буква б).

основни права, по-специално на правото на защита на данните[124]. Има дела, в които институции за защита на авторското право са поискали от интернет доставчиците да разкрият самоличността на потребителите на интернет платформи за споделяне на файлове.Такива платформи често правят възможно за интернет потребителите да изтеглят безплатно музикални произведения, въпреки че тези произведения са защитени с авторско право.

Пример: Делото *Promusicae/Telefónica de España*[125] се отнася до отказа на испански доставчик на услуги за достъп до интернет, Telefónica, да разкрие на Promusicae, организация с нестопанска цел, в която членуват музикални продуценти и издатели на музикални и аудиовизуални звукозаписи, личните данни на определени лица, на които то е предоставяло услуги за достъп до интернет. Promusicae иска разкриването на тази информация, за да може да предяви граждански искове срещу тези лица, за които твърди, че използват програма за споделяне на файлове, която им позволява достъп до звукозаписи, върху които членовете на Promusicae притежават имуществени права на използване.

Испанският съд сезира Съда на ЕС, като задава въпроса дали съгласно общностното право тези лични данни трябва да бъдат оповестени в рамките на гражданско производство, за да се осигури ефективна защита на авторското право. Той се позовава на директиви 2000/31, 2001/29 и 2004/48, тълкувани също така в контекста на членове 17 и 47 от Хартата. Съдът заключава, че тези три директиви, както и Директивата за правото на неприкосновеност на личния живот и електронни комуникации (Директива 2002/58/ЕО), не изключват възможността държавите членки да предвидят задължение за разкриване на лични данни в рамките на гражданско производство, за да осигурят ефективна защита на авторското право.

124 Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 29 януари 2008 г., параграфи 62—68.

125 *Пак там*, параграфи 54 и 60.

Съдът на ЕС посочва, че така делото повдига въпроса за необходимото съчетаване на изискванията, свързани със защита на различните основни права, а именно правото на зачитане на личния живот и правата на защита на собствеността, и правото на ефективни правни средства за защита.

Съдът заключава, че „при транспониране на посочените по-горе директиви държавите членки трябва да следят за тълкуване на последните, което позволява да се осигури подходящо равновесие между различните основни права, защитени от общностния правов ред. На следващо място, при въвеждане на мерките за транспониране на тези директиви органите и юрисдикциите на държавите членки са длъжни не само да тълкуват националното си право по начин, който да съответства на посочените директиви, но и да не допускат да се основават на тълкуване, което би влязло в конфликт с посочените основни права или с другите общи принципи на общностното право, като принципа на пропорционалност“[126].

Пример: Делото *Bonnier Audio AB и други/Perfect Communication Sweden AB*[127] се отнася до баланса между правата на интелектуална собственост и защитата на личните данни. Bonnier Audio и др. – пет издателски компании, притежаващи авторски права върху 27 аудиокниги – предявяват иск пред шведския съд, като твърдят, че авторските им права са били нарушени чрез използването на FTP сървър (протокол за трансфер на файлове, който позволява обмен на файлове и прехвърляне на данни по интернет). Bonnier Audio и др. искат от съда доставчикът на интернет услуги да разкрие името и адреса на лицето, използвало IP адреса, от който са били прехвърлени въпросните файлове. Доставчикът на интернет услуги – ePhone, възразява срещу искането, като твърди, че това е в нарушение на Директива 2006/24 (Директивата за запазване на лични данни, обявена за невалидна през 2014 г.).

126 *Пак там*, параграфи 65 и 68; вж. също Съд на ЕС, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 февруари 2012 г.

127 Съд на ЕС, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 април 2012 г.

Шведският съд сезира Съда на ЕС, като отправя въпроса дали Директива 2006/24 изключва прилагането на национална разпоредба, която е приета въз основа на член 8 от Директива 2004/48 (Директивата относно упражняване на правата на интелектуална собственост) и допуска издаването на съдебно разпореждане доставчиците на интернет услуги да предоставят на носителите на авторските права информация за абонатите, за чиито IP адреси се твърди, че са използвани за извършване на нарушението. Във връзка с този въпрос се приема, че лицето, което иска издаване на разпореждането, е представило достатъчно данни за нарушаването на конкретно авторско право и че тази мярка е пропорционална.

Съдът на ЕС посочва, че Директива 2006/24 се отнася изключително до обработването и запазването на данни, създадени от доставчиците на електронни съобщителни услуги за целите на разследването, разкриването и преследването на сериозни престъпления, както и до предоставянето на тези данни на компетентните национални органи. Поради тази причина национална разпоредба, с която се транспонира Директивата относно упражняване на правата на интелектуална собственост, е извън приложното поле на Директива 2006/24 и следователно нейното прилагане не се изключва от директивата[128].

Що се отнася до съобщаването на въпросното име и адрес, поискани от жалбоподателите, Съдът на ЕС постановява, че такова действие представлява обработване на лични данни и попада в приложното поле на Директива 2002/58 (Директивата за правото на неприкосновеност на личния живот и електронни комуникации). Съдът също така отбелязва, че съобщаването на тези данни се иска в рамките на гражданско производство, в полза на носителя на авторското право с цел да се осигури ефективна защита на това право, и следователно поради своя предмет искането попада в приложното поле на Директива 2004/48[129].

Съдът на ЕС заключава, че директиви 2002/58 и 2004/48 трябва да се тълкуват в смисъл, че допускат национално законодателство като разглежданото в главното производство, доколкото това

128 *Пак там*, параграфи 40–41.

129 *Пак там*, параграфи 52–54. Вж. също Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 29 януари 2008 г., параграф 58.

законодателство позволява на националната юрисдикция, която е сезирана с искане да се издаде разпореждане за разкриване на лични данни, да претегли съответните противоположни интереси, като съобрази обстоятелствата на всеки конкретен случай и надлежно отчете изискванията, произтичащи от принципа на пропорционалност.

1.3.6 Защита на данните и икономически интереси

В цифровата ера или ерата на големите информационни масиви данните се описват като „новото гориво" на икономиката за стимулиране на иновациите и творческата дейност[130]. Много дружества са изградили стабилни бизнес модели, свързани с обработването на данни, и това обработване често обхваща лични данни. Някои дружества може да считат, че специфичните правила, свързани със защитата на личните данни, могат на практика да доведат до прекалено тежки задължения, които биха могли да засегнат техните икономически интереси. Следователно възниква въпросът дали икономическите интереси на администраторите и обработващите лични данни или на широката общественост биха могли да оправдаят ограничаване на правото на защита на личните данни.

Пример: В делото *Google Spain*[131] Съдът на ЕС постановява, че при известни условия физическите лица имат правото да изискват интернет търсачките да заличат резултати от търсенето от техните регистри. В мотивите си Съдът на ЕС посочва факта, че от използването на интернет търсачки и от списъка на резултатите от търсенето може да се изгради подробен профил на дадено физическо лице. Тази информация може да е свързана с редица аспекти от личния живот на физическото лице и не би могла да бъде лесно открита или обединена без търсачка. Следователно тя представлява потенциално сериозна намеса в основните права на субектите на данни на неприкосновеност на личния живот и на защита на личните данни.

130 Вж. например *Financial Times* (2016), „Data is the new oil... who's going to own it?", 16 ноември 2016 г.

131 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г.

Съдът на ЕС след това разглежда дали намесата може да бъде оправдана. По отношение на икономическия интерес на дружеството, което управлява интернет търсачка, при това обработване на данни Съдът на ЕС заявява, че „се налага изводът, че то [вмешателството] не може да се обоснове единствено с икономическия интерес на лицето, което управлява интернет търсачка, при това обработване на данни", и че основните права по членове 7 и 8 от Хартата имат „по принцип" предимство пред този икономически интерес и пред интереса на широката общественост да намери посочената информация при търсене, отнасящо се до името на въпросното лице[132].

Едно от главните съображения на европейското право в областта на защитата на данните е да предостави на физическите лица повече контрол върху личните им данни. Особено в цифровата ера има дисбаланс между правомощията на стопанските предприятия, които обработват и имат достъп до огромни масиви от лични данни, и правомощията на лицата, на които принадлежат тези лични данни, да контролират своята информация. Съдът на ЕС възприема индивидуален подход към всеки отделен случай, когато търси баланс между защитата на данните и икономическите интереси — като например интересите на трети страни във връзка с дружествата с ограничена отговорност, чрез акции или по друг начин, както се вижда в решението по делото *Manni*.

Пример: Делото *Manni*[133] се отнася до включването на лични данни на физическо лице в публичен търговски регистър. Г-н Manni е поискал от Търговската палата на Лече да заличи негови лични данни от нейния регистър, след като разбрал, че негови потенциални клиенти ще направят справка в регистъра и ще видят, че е бил управител на дружество, което е било обявено в несъстоятелност преди повече от десет години. Тази информация създала предубеждения в потенциалните му клиенти и би могла да има отрицателно въздействие върху търговските му интереси.

132 *Пак там*, параграфи 81 и 97.

133 Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 март 2017 г.

Съдът на ЕС е призован да определи дали правото на ЕС в този случай признава право на изтриване на данните. За да достигне до заключение, Съдът балансира правилата на ЕС относно защитата на данните и търговския интерес на г-н Manni да бъде заличена информацията относно несъстоятелността на бившето му дружество с обществения интерес за достъп до информация. Съдът обръща надлежно внимание на факта, че оповестяването в публичния регистър на дружествата е предвидено в закон, и по-специално в директива на ЕС, която цели да направи информацията за дружествата по-леснодостъпна за трети страни. Оповестяването е важно, за да се защитят интересите на трети страни, които биха искали да работят с определено дружество, защото дружествата с ограничена отговорност, чрез акции или по друг начин, предлагат като гаранция на третите лица само своите активи. Следователно „основните документи на дружеството следва да бъдат оповестявани, за да могат третите лица да установят тяхното съдържание и друга информация във връзка с дружеството, особено данни за лицата, упълномощени да задължават дружеството“[134].

Предвид важността на легитимната цел, която преследва регистърът, Съдът на ЕС постановява, че г-н Manni не е имал право на изтриване на личните си данни, тъй като необходимостта да се защитят интересите на третите лица спрямо дружествата с ограничена отговорност, чрез акции или по друг начин, и да се гарантират правната сигурност, добросъвестността на търговските сделки и доброто функциониране на вътрешния пазар имат преимущество пред неговите права съгласно законодателството за защита на данните. Това важи по-специално с оглед на факта, че физическите лица, които избират да участват в икономическия обмен посредством дружество с ограничена отговорност, чрез акции или по друг начин, са наясно, че са задължени да оповестяват данните във връзка със самоличността си и функциите си в това дружество.

Като намира, че не са налице основания за изтриване на данните в този случай, Съдът на ЕС признава правото на възражение спрямо обработването, като отбелязва: „не може да се изключи, че е възможно да съществуват особени случаи, при които неопровержими законови основания, свързани с конкретното положение на съответното лице,

134 *Пак там*, параграф 49.

обосновават по изключение достъпът до вписаните в регистъра лични данни, отнасящи се до него, да бъде ограничен – след изтичането на достатъчно дълъг срок [...] – до третите лица, които могат да докажат особен интерес от консултирането им"[135].

Съдът на ЕС постановява, че националните съдилища са в правото си да преценят във всеки случай, с оглед на всички съотносими обстоятелства, евентуалното наличие или липса на неопровержими законови основания, които биха могли да обосновят по изключение ограничаването на достъпа на трети страни до данните, съдържащи се в дружествените регистри. Съдът обаче пояснява, че в случая на г-н Manni само по себе си твърдението, че оповестяването на личните му данни в регистъра е засегнало неговата клиентела, не може да бъде считано за такова неопровержимо законово основание. Потенциалните клиенти на г-н Manni имат законен интерес от информацията относно несъстоятелността на предишното му дружество.

Намесата в основните права на г-н Manni и на други включени в регистъра лица по отношение на зачитането на личния им живот и защитата на личните им данни, гарантирани в членове 7 и 8 от Хартата, е служила на цел от общ интерес и е била необходима и пропорционална.

Затова в делото *Manni* Съдът на ЕС постановява, че правата на защита на личните данни и на неприкосновеност на личния живот нямат предимство пред интереса на трети страни да получат достъп до информацията в дружествения регистър относно акционерни дружества и дружества с ограничена отговорност.

135 *Пак там*, параграф 60.

2

Терминология в областта на защитата на данните

ЕС	Обхванати въпроси	СЕ
Лични данни		
Общ регламент относно защитата на данните, член 4, параграф 1 Общ регламент относно защитата на данните, член 4, параграф 5 и член 5, параграф 1, буква д) Общ регламент относно защитата на данните, член 9 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 2010 г. Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU* [голям състав], 2008 г. Съд на ЕС, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 г. Съд на ЕС, C-582/14, *Patrick Breyer/ Bundesrepublik Deutschland*, 2016 г. Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* и *Minister vor Immigratie, Integratie en Asiel/M u S*, 2014 г.	**Правно определение на защитата на данните**	Модернизирана Конвенция № 108, член 2, буква а) ЕСПЧ, *Bernh Larsen Holding AS и други/ Норвегия*, № 24117/08, 2013 г. ЕСПЧ, *Uzun/Германия*, № 35623/05, 2010 г. ЕСПЧ, *Amann/Швейцария* [голям състав], № 27798/95, 2000 г.

ЕС	Обхванати въпроси	СЕ
Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 2003 г.	**Специални категории лични данни (чувствителни данни)**	Модернизирана Конвенция № 108, член 6, параграф 1
Съд на ЕС, C-434/16, *Peter Nowak/ Data Protection Commissioner*, 2017 г.	**Анонимизирани данни и псевдонимизирани данни**	Модернизирана Конвенция № 108, член 5, параграф 4, буква д) Обяснителен доклад към Модернизирана Конвенция № 108, параграф 50
Обработване на данни		
Общ регламент относно защитата на данните, член 4, параграф 2 Съд на ЕС, C-212/13 *František Ryneš/ Úřad pro ochranu osobních údajů*, 2014 г. Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017 г. Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 2003 г. Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 2014 г.	**Определения**	Модернизирана Конвенция № 108, член 2, букви б) и в)
Потребители на данни		
Общ регламент относно защитата на данните, член 4, параграф 7 Съд на ЕС, C-212/13, *František Ryneš/ Úřad pro ochranu osobních údajů*, 2014 г. Съд на ЕС, C-1318/12, *Google Spain SL u Google Inc./Agencia Española de Protección de Datos (AEPD) u Mario Costeja González* [голям състав], 2014 г.	**Администратор**	Модернизирана Конвенция № 108, член 2, буква г) Препоръка относно профилирането, член 1, буква ж)*

ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните, член 4, параграф 8	**Обработващ лични данни**	Модернизирана Конвенция № 108, член 2, буква е) Препоръка относно профилирането, член 1, буква з)
Общ регламент относно защитата на данните, член 4, параграф 9	**Получател**	Модернизирана Конвенция № 108, член 2, буква д)
Общ регламент относно защитата на данните, член 4, параграф 10	**Трета страна**	
Съгласие		
Общ регламент относно защитата на данните, член 4, параграф 11 и член 7 Съд на ЕС, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 2011 г. Съд на ЕС, C-536/15, *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*, 2017 г.	**Определение и изисквания за валидно съгласие**	Модернизирана Конвенция № 108, член 5, параграф 2 Препоръка относно медицинските данни, член 6, както и различни последващи препоръки ЕСПЧ, *Elberte/Латвия*, № 61243/08, 2015 г.

*Бележка: * Съвет на Европа: Комитет на министрите (2010 г.), Препоръка CM/Rec(2010)13 на Комитета на министрите до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране (Препоръка относно профилирането), 23 ноември 2010 г.*

2.1 Лични данни

Ключови въпроси

- Данните са лични данни, ако са свързани с идентифицирано лице или лице, което може да бъде идентифицирано, т.е. „субекта на данни“.
- За да се определи дали дадено физическо лице може да бъде идентифицирано, администратор или друго лице следва да вземе предвид всички разумни средства, които има вероятност да бъдат използвани, като например подбирането на лица за извършване на проверка, за да идентифицират пряко или непряко физическото лице.
- Автентификация означава доказване, че дадено лице притежава определена самоличност и/или е получило разрешение за извършването на определени дейности.

- Има специални категории данни, така наречените чувствителни данни, изброени в модернизираната Конвенция № 108 и в правото на ЕС в областта на защитата на данните, които изискват засилена защита и поради това са обект на специален правен режим.
- Данните са анонимизирани, ако повече не могат да бъдат свързани с идентифицирано лице или лице, което може да бъде идентифицирано.
- Псевдонимизацията е мярка, чрез която личните данни не могат да бъдат свързани със субекта на данни без допълнителна информация, която се съхранява отделно. „Ключът", който дава възможност за повторна идентификация на субектите на данни, трябва да бъде съхраняван отделно и да е защитен. Данните, които са преминали през процес на псевдонимизация, остават лични данни. В правото на ЕС няма понятие „псевдонимизирани данни".
- Принципите и правилата за защита на данните не се прилагат за анонимизираната информация. Те обаче се прилагат за псевдонимизираните данни.

2.1.1 Основни аспекти на понятието „лични данни"

Съгласно правото на ЕС, както и **съгласно правото на Съвета на Европа** „личните данни" се определят като информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано[136]. Те се отнасят до информация за лице, чиято самоличност е напълно изяснена или може да бъде установена от допълнителна информация. За да се определи дали дадено лице може да бъде идентифицирано, администратор или друго лице трябва да вземе предвид всички разумни средства, които има вероятност да бъдат използвани, за да идентифицират пряко или непряко физическото лице, като например подбирането на лица за извършване на проверка, което дава възможност за различно третиране на едно лице в сравнение с друго[137].

Ако се обработват данни относно такова лице, то се нарича „субект на данни".

136 Общ регламент относно защитата на данните, член 4, параграф 1; модернизирана Конвенция № 108, член 2, буква а).

137 Общ регламент относно защитата на данните, съображение 26.

Субектът на данни

Съгласно правото на ЕС физическите лица са единствените, които се ползват от правилата за защита на данните[138], като само живите личности са защитени съгласно европейското право за защита на данните[139]. Общият регламент относно защитата на данните (ОРЗД) определя личните данни като всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

Правото на Съвета на Европа, и най-вече модернизираната Конвенция № 108, също засяга защитата на физическите лица във връзка с обработването на техните лични данни. И в него „лични данни" е всяка информация, свързана с идентифицирано или подлежащо на идентифициране лице. В правото за защита на данните това физическо лице или лице, както е посочено съответно в ОРЗД и модернизираната Конвенция № 108, се нарича субект на данни.

Юридическите лица също се ползват от известна защита. Съществува съдебна практика на ЕСПЧ от произнесени решения по жалби на юридически лица, свързани с предполагаемо нарушение на правото им на защита по отношение на използването на техните данни съгласно член 8 от ЕКПЧ. Член 8 от ЕКПЧ обхваща правото на зачитане както на личния и семейния живот, така и на жилището и кореспонденцията. Поради това Съдът може да разглежда случаите, като се позовава на правото на неприкосновеност на жилището и кореспонденцията, а не на правото на неприкосновеност на личния живот.

Пример: Делото *Bernh Larsen Holding AS и други/Норвегия*[140] касае жалба от три норвежки дружества относно решение на данъчните органи, по силата на което от тях се изисква да предоставят на данъчните одитори копие на всички данни от компютърния сървър, който трите дружества са използвали съвместно.

138 *Пак там*, член 1.

139 *Пак там*, съображение 27. Вж. също Работна група по член 29 (2007 г.), *Становище 4/2007 относно понятието „лични данни"*, WP 136, 20 юни 2007 г., стр. 22.

140 ЕСПЧ, *Bernh Larsen Holding AS и други/Норвегия*, № 24117/08, 14 март 2013 г. Вж. обаче и ЕСПЧ, *Liberty и други/Обединеното кралство*, № 58243/00, 1 юли 2008 г.

ЕСПЧ установява, че такова задължение на дружествата жалбоподатели представлява намеса в правото им на неприкосновеност на „жилището“ и „кореспонденцията“ съгласно член 8 от ЕКПЧ. Съдът обаче счита, че данъчните органи са имали ефективни и адекватни гаранции срещу злоупотреба: дружествата жалбоподатели са били уведомени предварително; те са присъствали и са били в състояние да изложат своите доводи по време на намесата на място; материалът е трябвало да бъде унищожен след приключването на данъчната ревизия. При тези обстоятелства е бил осигурен подходящ баланс между правото на дружествата жалбоподатели на неприкосновеност на „жилището“ и „кореспонденцията“ и техния интерес да защитят неприкосновеността на личния живот на хората, работещи за тях, от една страна, и обществения интерес по отношение на осигуряването на ефективна инспекция за целите на проверката за установяване на данъчни задължения, от друга страна. Съдът постановява, че поради тази причина не е налице нарушение на член 8.

Съгласно модернизираната Конвенция № 108 защитата на данните се свързва основно със защитата на физически лица; въпреки това договарящите се страни могат да разширят обхвата на защитата на данните и до юридически лица, като например дружества и асоциации, които попадат в обхвата на националното им законодателство. В обяснителния доклад към модернизираната конвенция се посочва, че националното право може да защитава легитимните интереси на юридическите лица чрез разширяване на приложното поле на Конвенцията, така че да бъдат обхванати и тези субекти[141]. **Правото на ЕС в областта на защитата на данните** не обхваща обработването на данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и неговите данни за връзка[142]. Директивата за неприкосновеността на личния живот и електронни комуникации обаче защитава поверителността на съобщенията и законните интереси на юридическите лица по отношение на нарастващия капацитет за автоматизирано съхраняване и обработване на лични данни, отнасящи се до абонатите и потребителите[143]. Проектът за регламент относно неприкосновеността на личния живот

141 Обяснителен доклад към модернизираната Конвенция № 108, параграф 30.

142 Общ регламент относно защитата на данните, съображение 14.

143 Директива за неприкосновеността на личния живот и електронни комуникации, съображение 7 и член 1, параграф 2.

и електронните комуникации също разширява защитата, така че да бъдат обхванати и юридическите лица.

Пример: По делото *Volker und Markus Schecke GbR/Land Hessen*[144] Съдът на ЕС, позовавайки се на публикуването на лични данни за бенефициентите на селскостопански помощи, постановява, че „юридическите лица могат да се позоват на защитата по членове 7 и 8 от Хартата по отношение на подобно идентифициране само доколкото в наименованието на юридическото лице се идентифицират едно или повече физически лица. [...] Зачитането на правото на личен живот с оглед на обработката на лични данни, признато с членове 7 и 8 от Хартата, се отнася до всяка информация относно идентифицирано или подлежащо на идентификация физическо лице“[145].

Съпоставяйки интереса на ЕС да гарантира прозрачност при разпределянето на помощта, от една страна, и основните права на неприкосновеност на личния живот и защита на данните на лицата, които са се възползвали от помощта, от друга страна, Съдът на ЕС счита, че намесата в тези основни права е била непропорционална. Съдът счита, че целта за прозрачност е можела да бъде постигната ефективно чрез мерки, които са с по-малка степен на намеса в правата на засегнатите физически лица. Когато обаче разглежда пропорционалността на публикуването на информация, засягаща юридическите лица, получили помощи, Съдът на ЕС достига до различно заключение, като постановява, че такова публикуване не надхвърля границите на принципа на пропорционалност. Съдът посочва, че „тежестта на накърняването на правото на защита на личните данни е различна за юридическите и за физическите лица“[146]. Юридическите лица са подложени на задължение за публикуване на повече отнасящи се до тях данни. Съдът на ЕС счита, че задължението на националните органи да проверяват преди въпросното публикуване на данни за всяко юридическо лице — бенефициент, дали от неговото наименование могат да се идентифицират физически лица, би довело до несъразмерна административна натовареност на тези власти.

144 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г., параграф 53.

145 *Пак там*, параграфи 52—53.

146 *Пак там,* параграф 87.

Следователно при законодателството, което изисква публикуването на данни относно юридическите лица да е на общо основание, е постигнат необходимият баланс между съответните конкуриращи се интереси.

Естество на данните

Всеки вид информация може да представлява лични данни, при условие че тя е свързана с дадено идентифицирано лице или лице, което може да бъде идентифицирано.

Пример: Оценката на ръководител за работата на служител, съхранявана в личното досие на служителя, представлява лични данни за него. Това е така, макар че тази оценка може просто да отразява, частично или изцяло, личното мнение на ръководителя, като например следното: „служителят не е отдаден на работата си“ — и факти, които не са необорими, като: „служителят е отсъствал от работа пет седмици през последните шест месеца“.

Личните данни обхващат информация, отнасяща се до личния живот на лицето, който включва също така професионални дейности, както и информация относно обществения живот на лицето.

В делото *Amann*[147] ЕСПЧ дава тълкуване на термина „лични данни“ като понятие, което не се ограничава само до въпроси от сферата на личния живот на лицето. Това значение на термина „лични данни“ важи и за ОРЗД.

Пример: В решението по дело *Volker und Markus Schecke u Hartmut Eifert/Land Hessen*[148] Съдът на ЕС постановява, че „в това отношение е без значение фактът, че публикуваните данни се отнасят до професионални дейности [...]. В тази връзка Европейският съд по правата на човека приема относно тълкуването на член 8 от Конвенцията (ЕКЧП), че

147 Вж. ЕСПЧ, *Amann/Швейцария* [голям състав], № 27798/95, 16 февруари 2000 г., параграф 65.

148 Съд на ЕС, съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г., параграф 59.

изразът „личен живот“ не трябва да се тълкува ограничително и че „никакво принципно съображение не позволява да се изключат професионалните дейности [...] от понятието „личен живот“.

Пример: В решението си по съединени дела *YS/Minister voor Immigratie, Integratie en Asiel* и *Minister voor Immigratie, Integratie en Asiel/M u S*[149] съдът на ЕС постановява, че правният анализ, съдържащ се в проекта за решение на Службата по имиграция и натурализация, която обработва молбите за издаване на разрешение за пребиваване, не представлява сам по себе си лични данни, макар наистина да съдържа такива.

Съдебната практика на ЕСПЧ по отношение на член 8 от ЕКПЧ потвърждава, че действително е трудно да се разграничат напълно въпросите на личния и професионалния живот[150].

Пример: В делото *Bărbulescu/Румъния*[151] жалбоподателят е бил уволнен, защото е използвал интернета на своя работодател през работно време в нарушение на вътрешните правила. Неговият работодател е следил съобщенията му и в хода на националното производство са били представени записи, съдържащи съобщения от изцяло личен характер. Като се произнася, че член 8 е приложим, ЕСПЧ оставя открит въпроса дали ограничителните правила на работодателя са оставили у жалбоподателя разумно очакване за неприкосновеност на личния живот, но постановява, че указанията на работодателя не може да сведат личния социален живот на работното място до нула. Що се отнася до въпросите по същество, на договарящите се страни е трябвало да се предостави широка свобода на преценка при оценяването на необходимостта от установяване на правна рамка, уреждаща условията, при които работодателят може да регулира съобщенията от непрофесионален характер — електронни или други — на своите служители на работното място. Все пак националните органи е трябвало да гарантират, че въвеждането от страна на работодателя на мерки за следене на кореспонденцията и другите

149 Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister vor Immigratie, Integratie en Asiel/M u S*, 17 юли 2014 г., параграф 39.

150 Вж. например ЕСПЧ, *Rotaru/Румъния* [голям състав], № 28341/95, 4 май 2000 г., параграф 43; ЕСПЧ, *Niemietz/Германия*, № 13710/88, 16 декември 1992 г., параграф 29.

151 ЕСПЧ, *Bărbulescu/Румъния* [голям състав], № 61496/08, 5 септември 2017 г., параграф 121.

съобщения, независимо от обхвата и продължителността на тези мерки, е придружено от подходящи и достатъчни гаранции срещу злоупотреби. Пропорционалността и процедурните гаранции срещу всякакви форми на произвол са важни и ЕСПЧ определи редица фактори, които са от значение при дадените обстоятелства. Тези фактори например включват обхвата на следенето на служителите от страна на работодателя и степента на навлизане в личния живот на служителя, последствията за служителя и дали са предвидени подходящи гаранции. Освен това националните органи е трябвало да гарантират, че служителят, чиито съобщения са били следени, има достъп до правни средства за защита пред съдебен орган, който разполага с компетентност да се произнася, поне по същество, дали са спазени определените критерии и дали са законосъобразни оспорваните мерки. В този случай ЕСПЧ констатира нарушение на член 8, тъй като националните органи не са осигурили подходяща защита на правото на жалбоподателя на зачитане на личния живот и кореспонденцията и следователно не са успели да постигнат справедлив баланс между различните засегнати интереси.

Съгласно правото на ЕС, както и **съгласно правото на Съвета на Европа** в определена информация се съдържат данни за дадено лице, ако:

- лицето е идентифицирано или може да бъде идентифицирано в тази информация; или

- лицето, въпреки че не е идентифицирано, може да бъде определено чрез тази информация по такъв начин, че е възможно да се открие за кой субект на данни става въпрос при продължаване на проучването.

И двата вида информация са защитени по един и същ начин от европейското право в областта на защитата на данните. Възможността за пряко или непряко идентифициране на физическите лица изисква непрекъсната оценка, „като се отчитат съществуващата технология към момента на обработването и развитието на технологиите“[152]. ЕСПЧ многократно е заявявал, че понятието „лични данни“ по смисъла на ЕКПЧ е същото като в Конвенция № 108, особено що

152 Общ регламент относно защитата на данните, съображение 26.

се отнася до условието за информация относно идентифицирани или подлежащи на идентификация лица[153].

ОРЗД предвижда, че физическо лице може да бъде идентифицирано, когато то „може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор, като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице“[154]. Следователно идентификацията изисква елементи, които описват лицето по такъв начин, че то се различава от всички останали и се разпознава като физическо лице. Името на даден човек е основен пример за такива елементи на описание и може директно да идентифицира лицето. В някои случаи други характеристики могат да имат подобен ефект като този на името, давайки възможност за непряко идентифициране на лицето. Телефонен номер, номер на социална осигуровка или регистрационен номер на превозно средство са все примери за информация, по която може да се идентифицира дадено лице. Възможно е да се използват определени способи — като например компютризирани досиета, „бисквитки“ и инструменти за наблюдение на трафика по интернет — за да се определят физическите лица чрез идентифициране на тяхното поведение или навици. Както е обяснено в становище на Работната група по член 29, „дори без да се събират сведения за името и адреса на лицето, е възможно това лице да се категоризира въз основа на социално-икономически, психологически, философски или други критерии и да му се припишат определени решения, тъй като точката за контакт с лицето (компютърът) вече не налага разкриване на самоличността му в тесния смисъл на думата“[155]. Определението за лични данни по правото както на Съвета на Европа, така и на ЕС е достатъчно широко, за да покрие всички възможности за идентификация (и следователно всички степени на възможността за идентифициране).

153 Вж. ЕСПЧ, *Amann/Швейцария* [голям състав], № 27798/95, 16 февруари 2000 г., параграф 65.

154 Общ регламент относно защитата на данните, член 4, параграф 1.

155 Работна група по член 29 (2007 г.), *Становище 4/2007 относно понятието лични данни*, WP 136, 20 юни 2007 г., стр. 15.

Пример: По дело *Promusicae/Telefónica de España*[156] Съдът на ЕС посочва, че „не се оспорва, че поисканото от Promusicae съобщаване на имената и адресите на определени лица, ползващи [определена интернет платформа за споделяне на файлове], включва предоставяне на лични данни, т.е. на сведения относно точно идентифицирани или подлежащи на идентификация физически лица, съгласно определението в член 2, буква а) от Директива 95/46 [понастоящем член 4, параграф 1 от ОРЗД]. Съобщаването на тези сведения, които според Promusicae са съхранявани от Telefónica, като последното не оспорва това обстоятелство, представлява обработка на лични данни“[157].

Пример: Делото *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] се отнася до отказа на доставчика на интернет услуги Scarlet да въведе система за филтриране на електронни съобщения посредством софтуери за обмен на архиви, за да се възпрепятства обменът на файлове, който нарушава авторските права, защитени от SABAM, дружество за управление на авторски права, което представлява авторите, композиторите и издателите на музикални произведения. Съдът на ЕС постановява, че IP адресите на ползвателите „са защитени лични данни, тъй като позволяват точното идентифициране на ползвателите“.

Тъй като много от имената не са уникални, установяването на самоличността на дадено лице може да изисква допълнителни характеристики, за да се гарантира, че лицето не е сбъркано с някой друг. Понякога може да се наложи да се съчетаят преки и непреки характеристики, за да се идентифицира лицето, за което се отнася информацията. Често се използват датата и мястото на раждане. В допълнение в някои държави са въведени персонализирани номера за по-добро разпознаване на гражданите. Прехвърлените данъчни данни[159], данните за кандидат за разрешение за пребиваване, съдър-

156 Съд на ЕС, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 29 януари 2008 г., параграф 45.

157 Предходна Директива 95/46, член 2, буква б), понастоящем Общ регламент относно защитата на данните, член 4, параграф 2.

158 Съд на ЕС, C-70/10,*Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 ноември 2011 г., параграф 51.

159 Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 1 октомври 2015 г.

жащи се в административен документ[160], и документите относно банкови и доверителни отношения[161] могат да бъдат лични данни. Биометричните данни, като дактилоскопични отпечатъци, цифрови снимки или сканиране на ириса, данни за местоположението и онлайн идентификатор придобиват все по-голямо значение за идентификацията на лица в технологичната ера.

За приложимостта на европейското законодателство в областта на защитата на данни обаче няма нужда от действителна идентификация на субекта на данните; достатъчно е въпросното лице да може да бъде идентифицирано. Счита се, че едно лице може да бъде идентифицирано, ако са налице достатъчно елементи, с помощта на които лицето може да бъде пряко или непряко идентифицирано[162]. Съгласно съображение 26 от ОРЗД критерият е дали е вероятно, че разумни средства за идентификация ще бъдат на разположение и ще бъдат администрирани от предвидените ползватели на данните; това включва и информация, притежавана от получателите — трети страни (вж. раздел 2.3.2).

Пример: Местен орган решава да събира данни за автомобили, движещи се с превишена скорост по местните улици. Колите се заснемат, като автоматично се записват времето и мястото, за да се предоставят данните на компетентния орган, който съответно налага глоби на нарушителите на ограниченията на скоростта. Субект на данни подава жалба, като твърди, че местният орган не разполага с правно основание съгласно законодателството за защита на данните да събира такива данни. Местният орган твърди, че не събира лични данни. Той заявява, че регистрационните номера са анонимни. Местният орган не разполага с юридически правомощия за достъп до общия регистър на превозните средства, за да идентифицира собственика на автомобила или водача.

Този аргумент не отговаря на съображение 26 от ОРЗД. Предвид факта, че целта на събирането на данни е ясно да се идентифицират водачите, които карат с превишена скорост и подлежат на глоба, е предвидимо, че ще се направи опит за идентификация. Въпреки че местните органи не

160 Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister vor Immigratie, Integratie en Asiel/M и S*, 17 юли 2014 г.

161 ЕСПЧ, *M.N.и други/Сан Марино*, № 28005/12, 7 юли 2015 г.

162 Общ регламент относно защитата на данните, член 4, параграф 1.

разполагат пряко със средства за идентификация, те предават данните на компетентния орган, полицията, който разполага с такива средства. Съображение 26 също изрично включва сценарий, при който може да се предвиди, че следващите получатели на данни, които са различни от непосредствените ползватели на данните, може да се опитат да идентифицират лицето. В контекста на съображение 26 действието на местния орган се равнява на събирането на данни за определяеми лица и следователно изисква законно основание съгласно правото за защита на данните.

За „да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития“[163].

Пример: В делото *Breyer/Bundesrepublik Deutschland*[164] Съдът на ЕС разглежда понятието непряка идентификация на субектите на данни. Делото се отнася до динамични IP адреси, които се сменят при всяко ново свързване в интернет. Уебсайтовете, поддържани от германските федерални институции, са регистрирали и съхранявали динамични IP адреси, за да предотвратят кибератаки и за да стартират при необходимост наказателни производства. Единствено доставчикът на интернет услуги на г-н Breyer е разполагал с допълнителната информация, необходима, за да бъде той идентифициран.

Съдът на ЕС счита, че динамичен IP адрес, запазен от доставчик на онлайн медийни услуги при влизане на дадено лице в интернет сайт, до който доставчикът предоставя достъп, представлява лични данни, когато единствено трета страна — в случая доставчикът на интернет услуги — притежава допълнителната информация, необходима, за да бъде идентифицирано лицето[165]. Той постановява, че за да могат определени данни да се считат за „лични“, „не се изисква цялата

163 *Пак там*, съображение 26.

164 Съд на ЕС, C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19 октомври 2016 г., параграф 43.

165 Предходна 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, член 2, буква а).

информация, която позволява идентифицирането на съответното лице, да трябва да се намира в ръцете на едно-единствено лице". Ползвателите на динамичен IP адрес, запазен от доставчик на интернет услуги, могат да бъдат идентифицирани с помощта на други лица в определени ситуации, например в рамките на наказателно преследване в случай на кибератаки[166]. Според Съда на ЕС когато доставчикът „разполага със законни средства, позволяващи му да идентифицира съответното лице благодарение на допълнителната информация, с която разполага доставчикът на интернет услуги на това лице", това представлява „средство, което би могло да бъде използвано разумно за идентифицирането на съответното лице". Следователно такива данни се считат за лични данни.

Съгласно правото на Съвета на Европа възможността за идентифициране се разбира по подобен начин. Обяснителният доклад към модернизираната Конвенция № 108 включва подобно описание: понятието „определяемо" не се отнася само до гражданската или юридическата идентичност на лицето като такава, а също и до всичко, което може да позволи едно лице да бъде „индивидуализирано" или отделено от другите и в резултат да бъде третирано различно. „Индивидуализацията" може да бъде извършена например чрез позоваване конкретно на лицето или на устройство или комбинация от устройства (компютър, мобилен телефон, камера, устройства за компютърни игри и т.н.), свързани с идентификационен номер, псевдоним, биометрични или генетични данни, данни за местоположение, IP адрес или друг идентификатор[167]. Едно лице не се счита за „определяемо", ако идентифицирането му изисква необосновано много време, усилия или ресурси. Такъв е случаят например, когато идентифицирането на субекта на данни би изисквало изключително сложни, продължителни и скъпи действия. Необосноваността на разхода на време, усилия или ресурси трябва да се оценява във всеки отделен случай, като се вземат предвид фактори, като целта на обработването, разходите и ползите от идентифицирането, вида администратор и използваната технология[168].

166 Съд на ЕС, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 ноември 2011 г., параграфи 47–48.

167 Обяснителен доклад към модернизираната Конвенция № 108, параграф 18.

168 *Пак там*, параграф 17.

Що се отнася до формата, под която се съхраняват или използват личните данни, важно е да се отбележи, че тя не е от значение при прилагането на правото в областта на защитата на личните данни. Писмената или устната комуникация може да съдържа лични данни, както и образи[169], включително кадри от системи за видеонаблюдение (CCTV)[170] или звук[171]. Електронно записваната информация, както и информацията на хартиен носител също може да представлява лични данни. Дори клетките на човешката тъкан — които „записват" ДНК-то на лицето, могат да бъдат източници, от които могат да се извлекат биометрични данни[172], тъй като данните са свързани с наследени или придобити генетични белези на лицата, дават уникална информация за отличителните черти или здравето на тези лица и са получени от анализ на биологична проба от въпросното лице[173].

Анонимизация

Според принципа за ограничен период на запазване на данните, съдържащ се както в ОРЗД, така и в модернизираната Конвенция № 108 (и обсъдени по-подробно в глава 3), данните трябва да се съхраняват „във вид, позволяващ идентифицирането на заинтересованите лица за период, не по-дълъг от необходимия за целта, за която са запаметени"[174]. Следователно данните би трябвало да бъдат изтрити или анонимизирани, ако администраторът иска да ги съхранява, след като те вече не са необходими и вече не служат за тяхната първоначална цел.

Анонимизирането на данни означава, че всички идентифицируеми елементи са били премахнати от определен набор лични данни, така че субектът на

169 ЕСПЧ, *Von Hannover/Германия*, № 59320/00, 24 юни 2004 г.; ЕСПЧ, *Sciacca/Италия*, № 50774/99, 11 януари 2005 г.; Съд на ЕС, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 декември 2014 г.

170 ЕСПЧ, *Peck/Обединеното кралство*, № 44647/98, 28 януари 2003 г.; ЕСПЧ, *Köpke/Германия* (реш.), № 420/07, 5 октомври 2010 г.; ЕНОЗД (2010 г.), *Насоки на ЕНОЗД относно видео наблюдението*, 17 март 2010 г.

171 ЕСПЧ, *P.G. и J.H./Обединеното кралство*, № 44787/98, 25 септември 2001 г., параграфи 59—60; ЕСПЧ, *Wisse/Франция*, № 71611/01, 20 декември 2005 г. (текст на френски език).

172 Вж. Работна група по член 29 (2007 г.), *Становище 4/2007 относно понятието „лични данни"*, WP 136, 20 юни 2007 г., стр. 9; Съвет на Европа, Препоръка Rec(2006) 4 на Комитета на министрите към държавите членки относно научните изследвания в областта на биологичните материали от човешки произход, 15 март 2006 г.

173 Общ регламент относно защитата на данните, член 4, параграф 13.

174 *Пак там*, член 5, параграф 1, буква д); модернизирана Конвенция № 108, член 5, параграф 4, буква д).

данни вече не може да бъде идентифициран[175]. В своето Становище 05/2014 Работната група по член 29 анализира ефективността и ограниченията на различните техники за анонимизиране[176]. Тя признава потенциалната стойност на тези техники, но подчертава, че някои техники не работят непременно във всички случаи. За да се намери оптималното решение в дадена ситуация, за всеки отделен случай следва да се определи подходящият процес на анонимизация. Независимо от използваната техника трябва необратимо да бъде предотвратена възможността за идентификация. Това означава, че за да бъдат анонимизирани данните, в тях не може да бъде оставен никакъв елемент, който би могъл при полагането на разумни усилия да послужи за повторната идентификация на въпросното(ите) лице(а)[177]. Рискът от повторна идентификация може да бъде оценен, като се вземе предвид „необходимото време, усилия или ресурси с оглед на естеството на данните, контекста на тяхното използване, съществуващите технологии за повторна идентификация и свързаните с това разходи“[178].

Когато данните са анонимизирани успешно, те вече не са лични данни и към тях вече не се прилага законодателството за защита на данните.

ОРЗД предвижда, че лицето или организацията, които контролират обработването на лични данни, не са задължени да поддържат, да се сдобият или да обработват допълнителна информация, за да идентифицират субекта на данни с единствената цел да бъде спазен регламентът. Това правило обаче има едно важно изключение: всеки път когато субектът на данни, с цел да упражни правата си на достъп, коригиране, изтриване, ограничаване на обработването и преносимост на данните, предоставя допълнителна информация на администратора, която позволява идентификацията му, тези данни, които преди това са били анонимизирани, стават отново лични данни[179].

175 Общ регламент относно защитата на данните, съображение 26.

176 Работна група по член 29 (2014 г.), *Становище 05/2014 относно техниките за анонимизиране*, WP 216, 10 април 2014 г.

177 Общ регламент относно защитата на данните, съображение 26.

178 Съвет на Европа, Консултативен комитет на Конвенция № 108 (2017 г.), *Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви*, 23 януари 2017 г., параграф 6.2.

179 Общ регламент относно защитата на данните, член 11.

Псевдонимизация

Личните данни съдържат идентификатори, като име, дата на раждане, пол, адрес или други елементи, които биха могли да доведат до идентификация. Процесът на псевдонимизация на лични данни означава, че тези идентификатори се заменят от псевдоним.

Правото на ЕС определя „псевдонимизацията" като „обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано"[180]. За разлика от анонимизираните, псевдонимизираните данни продължават да бъдат лични данни и следователно са предмет на законодателството за защита на данните. Макар че псевдонимизацията може да намали рисковете за сигурността за субектите на данни, тя не се изключва от обхвата на ОРЗД.

ОРЗД признава различни приложения на псевдонимизацията като подходяща техническа мярка за засилване на защитата на данните и тя е изрично упомената по отношение на проектирането и сигурността на обработването на данните[181]. Тя е подходяща гаранция и във връзка с обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни[182].

Псевдонимизацията не е изрично упомената в правното определение на модернизираната Конвенция № 108 на **Съвета на Европа**. В обяснителния доклад към модернизираната Конвенция № 108 обаче ясно се посочва, че „използването на псевдоним или на някакъв цифров идентификатор/цифрова идентичност не води до анонимизиране на данните, тъй като субектът на данни все пак може да бъде определяем или индивидуализиран"[183]. Един от начините да се псевдонимизират данните е като бъдат криптирани. След като данните се псевдонимизират, връзката със самоличността съществува под

180 *Пак там*, член 4, параграф 5.

181 *Пак там*, член 25, параграф 1.

182 *Пак там*, член 6, параграф 4.

183 Обяснителен доклад към модернизираната Конвенция № 108, параграф 18.

формата на псевдоним плюс ключ за декриптиране. Без такъв ключ е трудно да се идентифицират псевдонимизираните данни. За тези, които имат право да използват ключа за декриптиране обаче, е лесно да направят повторна идентификация. По-специално трябва да се предотврати използването на ключовете за криптиране от неупълномощени лица. Следователно „псевдонимизираните данни [...] трябва да се считат за лични данни [...]“, които попадат в обхвата на модернизираната Конвенция № 108[184].

Автентификация

Това е процедура, при която дадено лице може да докаже, че притежава определена самоличност и/или е оторизирано да извършва определени дейности, като влизане в зона за сигурност или теглене на пари от банкова сметка. Автентификацията може да се постигне чрез сравняване на биометрични данни, като снимка или дактилоскопични отпечатъци в паспорт, с данните на лицето, представящо се за него, например при имиграционен контрол[185]; или чрез изискване на информация, която е известна само на лицето с определена самоличност или оторизация, като например личния идентификационен номер (ЛИН) или парола; или като се изисква представянето на определен знак или символ, който трябва да се притежава единствено от лице с определена идентичност или оторизация, например специална чип карта или ключ за банков сейф. Отделно от паролите или чип картите, понякога заедно с ПИН кодовете, електронните подписи са инструмент, който е особено подходящ за идентификация или автентификация на дадено лице при електронни комуникации.

2.1.2 Специални категории лични данни

Съгласно правото на ЕС, както и на **Съвета на Европа**, има специални категории лични данни, които — поради своето естество — при обработването могат да представляват риск за субектите на данни и се нуждаят от засилена защита. Такива данни са предмет на забранителен принцип и има ограничен брой условия, при които това обработване е законосъобразно.

184 *Пак там*.

185 *Пак там,* параграфи 56—57.

В рамките на модернизираната Конвенция № 108 (член 6) и ОРЗД (член 9) за чувствителни се считат следните категории данни:

- лични данни, разкриващи расов или етнически произход;
- лични данни, разкриващи политически възгледи, религиозни или други убеждения, включително философски убеждения;
- лични данни, разкриващи членството в професионални съюзи;
- генетични и биометрични данни, обработвани с цел идентифициране на дадено лице;
- лични данни, свързани със здравето, сексуалния живот или сексуалната ориентация.

Пример: Делото *Bodil Lindqvist*[186] се отнася до позоваването в интернет страница на различни лица по име или по друг начин, например чрез телефонен номер или данни за развлеченията им. Съдът на ЕС посочва, че „споменаването на факта, че едно лице е наранило стъпалото си и по медицински съображения работи на половин работен ден, съставлява лични данни, засягащи здравето“[187].

Лични данни, свързани с присъди и нарушения

Модернизираната Конвенция № 108 включва личните данни, свързани с престъпления, наказателни производства и присъди, и свързаните с тях мерки за сигурност в списъка на специалните категории лични данни[188]. В рамките на ОРЗД личните данни, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност, не са споменати като такива в списъка на специалните категории данни, а са разгледани в отделен член. Член 10 от ОРЗД предвижда, че обработването на такива лични данни се извършва само „под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи

186 Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г., параграф 51.

187 Предходна Директива 95/46/ЕО, член 8, параграф 1, понастоящем Общ регламент относно защитата на данните, член 9, параграф 1.

188 Модернизирана Конвенция № 108, член 6, параграф 1.

гаранции за правата и свободите на субектите на данни“. От друга страна, пълен регистър на присъдите по наказателни дела могат да се поддържат само под контрола на точно определени официални органи[189]. В ЕС обработването на лични данни в контекста на правоприлагането се урежда от специален правен инструмент — Директива 2016/680/ЕС[190]. Директивата определя специфични правила за защита на данните, които са задължителни за компетентните органи, когато обработват лични данни специално за да предотвратят, разследват, разкрият и преследват наказателно престъпления (вж. раздел 8.2.1).

2.2 Обработване на данни

Ключови въпроси

- „Обработването на данни“ се отнася до всяка операция, извършвана с лични данни.
- Терминът „обработване“ обхваща както автоматизираното, така и неавтоматизираното обработване.
- Съгласно правото на ЕС „обработването“ се отнася и до ръчното обработване в структурирани системи за обработване на данни по регистри.
- Съгласно правото на Съвета на Европа значението на термина „обработване“ може да бъде разширено от националното законодателство, така че да включва ръчното обработване.

2.2.1 Понятието „обработване на данни“

Понятието „обработване на лични данни“ е определено изчерпателно **както съгласно правото на ЕС, така и съгласно правото на Съвета на Европа:** „обработване на лични данни“ [...] означава всяка операция [...], като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни,

189 Общ регламент относно защитата на данните, член 10.

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

подреждане или комбиниране, ограничаване, изтриване или унищожаване“[191] на лични данни. Модернизираната Конвенция № 108 добавя към определението и запазването на лични данни[192].

Пример: В делото *František Ryneš*[193] г-н Ryneš е записал образите на две лица, които счупили прозорци на дома му, чрез домашна система за видеонаблюдение, която е инсталирал, за да защити собствеността си. Съдът на ЕС определя, че видеонаблюдение, включващо запис и съхранение на лични данни, представлява автоматизирано обработване на лични данни, което попада в обхвата на правото на ЕС в областта на защитата на данните.

Пример: По делото *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*[194] г-н Manni е поискал личните му данни да бъдат заличени от регистъра на дружество, специализирано в оценката на риска („rating“), който го свързва с несъстоятелността на дружество за недвижими имоти, като по този начин оказва отрицателно въздействие върху доброто му име. Съдът на ЕС постановява, че „като вписва и съхранява посочените сведения в регистъра и при необходимост ги съобщава на трети лица по тяхна молба, органът, на който е възложено воденето на този регистър, извършва „обработване на лични данни“, на което е „администратор“.

Пример: Работодателите събират и обработват данни за своите служители, включително информация, свързана с техните заплати. Трудовите договори им дават правно основание да правят това законно.

Работодателите ще трябва да изпратят данните за заплатите на своите служители на данъчните органи. Това предаване на данни също ще представлява „обработване“ по смисъла на този термин в модернизираната Конвенция № 108 и в ОРЗД. Правното основание

191 Общ регламент относно защитата на данните, член 4, параграф 2. Вж. също модернизирана Конвенция № 108, член 2, буква б).

192 Модернизирана Конвенция № 108, член 2, буква б).

193 Съд на ЕС, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 декември 2014 г., параграф 25.

194 Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 март 2017 г., параграф 35.

за такова разкриване на данни обаче не са трудовите договори. Трябва да има допълнително правно основание за операциите по обработване, водещи до предаването на данни за заплатите от работодателя на данъчните органи. Това правно основание обикновено се съдържа в разпоредбите на националното данъчно законодателство. Без такива разпоредби — и при липсата на друго законово основание за обработването — това предаване на лични данни би представлявало незаконно обработване.

2.2.2 Автоматизирано обработване на данни

Защитата на данните съгласно модернизираната Конвенция № 108 и ОРЗД се прилага напълно към автоматизираното обработване на данни.

Съгласно **правото на ЕС** автоматизираното обработване на данни се отнася до операциите, извършвани с „лични данни изцяло или частично с автоматични средства“[195]. Модернизираната Конвенция № 108 съдържа сходно определение[196]. На практика това означава, че всяко обработване на лични данни с автоматични средства с помощта например на персонален компютър, мобилно устройство или рутер попада в обхвата на правилата за защита на данните както на ЕС, така и на Съвета на Европа.

Пример: Делото *Bodil Lindqvist*[197] се отнася до позоваването в интернет страница на различни лица по име или по друг начин, например чрез телефонен номер или данни за развлеченията им. Съдът на ЕС постановява, че „операция, състояща се в позоваването в интернет страница на различни лица и определянето им или по име, или по друг начин, например чрез телефонен номер или данни, свързани с условията им на работа и развлеченията им, представлява „автоматизирана изцяло или отчасти обработка на лични данни“ по смисъла на член 3, параграф 1 от Директива 95/46[198].

195 Общ регламент относно защитата на данните, член 2, параграф 1 и член 4, параграф 2.

196 Модернизирана Конвенция № 108, член 2, букви б) и в); Обяснителен доклад към модернизираната Конвенция № 108, параграф 21.

197 Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г., параграф 27.

198 Общ регламент относно защитата на данните, член 2, параграф 1.

Пример: В делото *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] г-н González е поискал да бъде премахната или изменена съществуваща връзка между неговото име в интернет търсачката на Гугъл и две страници на всекидневник, съдържащи обява за продажба на недвижимо имущество на търг по повод на възбрана, наложена за събиране на вземания в областта на социалното осигуряване. Съдът на ЕС постановява, че „с автоматизираното, постоянно и систематично обхождане на интернет в търсене на публикуваната в него информация лицето, което управлява интернет търсачка, „събира" такива данни и ги „извлича", „записва" и „организира" впоследствие посредством програмите си за индексиране, „съхранява" данните на сървърите си и евентуално ги „разкрива" и „предоставя" на ползвателите на търсачката под формата на списъци на резултатите от извършените търсения"[200]. Съдът на ЕС заключава, че такива действия представляват „обработване", „независимо че лицето, което управлява интернет търсачката, прилага тези операции и към други видове информация, без да прави разграничение между същата информация и личните данни".

2.2.3 Неавтоматизирано обработване на данни

Ръчното обработване на данни също изисква защита на данните.

Защитата на данните **съгласно правото на ЕС** по никакъв начин не се ограничава до автоматизираното обработване на данни. Съответно съгласно правото на ЕС защитата на данни се прилага спрямо обработването на лични данни в ръчна система за обработване на данни по регистри, която представлява специално структурирано досие на хартиен носител[201]. Структурирана система за обработване на данни по регистри е система, която категоризира дадена съвкупност от лични данни, като ги прави достъпни съгласно определени критерии. Например ако работодателят поддържа на хартиен носител досие, озаглавено „отпуски на персонала", което съдържа всички данни за отпуските, които служителите са ползвали през последната година, и е подредено

199 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г.

200 *Пак там*, параграф 28.

201 Общ регламент относно защитата на данните, член 2, параграф 1.

по азбучен ред, досието ще представлява ръчна система за обработване на данни по регистри, която е предмет на правилата на ЕС за защита на данните. Причината за това разширяване на обхвата на защитата на данните е следната:

- досиетата на хартиен носител могат да бъдат структурирани по начин, който прави намирането на информация бързо и лесно;

- съхраняването на лични данни в структурирани досиета на хартиен носител прави лесно заобикалянето на ограниченията, предвидени от законодателството по отношение на автоматизираното обработване на данни[202].

Съгласно **правото на Съвета на Европа** в определението за автоматизирано обработване на данни се отчита, че между отделните автоматизирани операции може да са необходими няколко етапа на ръчно използване на личните данни[203]. Член 2, буква в) от модернизираната Конвенция № 108 гласи, че „когато не се използва автоматизирано обработване, обработване на данни означава операция или набор от операции, извършвани с лични данни в рамките на структуриран набор от такива данни, които са достъпни или могат да бъдат извлечени в съответствие със специални критерии“.

2.3 Ползватели на лични данни

Ключови въпроси

- Всяко лице, което определя средствата и целите на обработването на личните данни на други лица, е „администратор“ съгласно правото за защитата на данните; ако няколко лица взимат това решение заедно, те могат да бъдат „съвместни администратори“.

- „Обработващ лични данни“ е физическо или юридическо лице, което обработва лични данни от името на администратора.

- Обработващият лични данни става администратор, ако сам определя средствата и целите на обработването на данните.

- Всяко лице, пред което се разкриват лични данни, е „получател“.

202 Общ регламент относно защитата на данните, съображение 15.

203 Модернизирана Конвенция № 108, член 2, букви б) и в).

- „Трета страна“ е физическо или юридическо лице, различно от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.
- Съгласието като правно основание за обработване на лични данни трябва да е свободно изразено, информирано, конкретно и недвусмислено указание за волята на лицето посредством ясно утвърдителен акт, изразяващ съгласие за обработването.
- За обработването на специални категории данни въз основа на дадено съгласие е необходимо предоставянето на изрично съгласие.

2.3.1 Администратори и обработващи лични данни

Най-важната последица от това да се изпълнява ролята на администратор или на обработващ лични данни е правната отговорност за изпълнение на съответните задължения съгласно правото за защита на данните. В частния сектор това обикновено са физически или юридически лица; в публичния сектор това обикновено са органи. Има съществено разграничение между администратора на данни и обработващия лични данни: първият е физическо или юридическо лице, което определя целите и средствата на обработването, докато вторият е физическо или юридическо лице, което обработва данните от името на администратора, като следва строги указания. По принцип администраторът на данни трябва да упражнява контрол върху обработването и да носи отговорност за това, включително юридическа отговорност. С реформата на правилата за защита на данните обаче обработващите лични данни вече имат задължение да спазват много от изискванията, които се отнасят до администраторите. Например съгласно ОРЗД обработващите лични данни трябва да поддържат регистър на всички категории дейности по обработването, за да докажат спазването на задълженията си съгласно регламента[204]. От обработващите лични данни се изисква също така да прилагат подходящи технически и организационни мерки, за да гарантират сигурността на обработването[205], да назначават длъжностно лице по защита на данните при опре-

204 Общ регламент относно защитата на данните, член 30, параграф 2.

205 *Пак там*, член 32.

делени ситуации[206] и да уведомяват администратора за нарушения на сигурността на данните[207].

Дали едно лице има възможността да решава и да определя целта и средствата на обработването, ще зависи от фактическите елементи или обстоятелствата по случая. Съгласно определението за администратор в ОРЗД физическите лица, юридическите лица и всички други органи могат да бъдат администратори. Работната група по член 29 обаче подчертава, че за да се предложи на лицата по-стабилен субект, чрез който да упражняват правата си, „трябва да се предпочете като администратор да бъде посочено дружеството или органът като такъв, вместо конкретно лице в рамките на дружеството или органа“[208]. Например дружество, което продава медицински доставки на практикуващи лекари, е администраторът, който изготвя и поддържа дистрибуционния списък на всички практикуващи лекари в дадена област, а не мениджърът по продажбите, който в действителност използва и поддържа списъка.

Пример: Когато отделът по маркетинг на дружеството Sunshine планира да обработва данни за пазарно проучване, администраторът на това обработване ще бъде самото дружество Sunshine, а не служителите на отдела по маркетинг. Отделът по маркетинг не може да бъде администратор, тъй като той не се ползва с отделен юридически статут.

Физическите лица могат да бъдат администратори съгласно правото както на ЕС, така и на Съвета на Европа. Когато обаче обработват данни за други лица относно изцяло лична дейност или дейност в рамките на домакинството, физическите лица не попадат в обхвата на правилата на ОРЗД и модернизираната Конвенция № 108 и не се считат за администратори на лични данни[209]. Лице, което поддържа кореспонденция, личен дневник, описващ случки с приятели и колеги, и здравно досие на членове на семейството, може да бъде изключено от обхвата на правилата за защита на данните, тъй като тези дейности могат да бъдат изцяло лични или просто в рамките на

206 *Пак там*, член 37.

207 *Пак там*, член 33, параграф 2.

208 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г.

209 Общ регламент относно защитата на данните, съображение 18 и член 2, параграф 2, буква в); модернизирана Конвенция № 108, член 3, параграф 2.

домакинството. В ОРЗД също така се посочва, че личните дейности или дейностите в рамките на домакинството биха могли да включват и участието в социални мрежи и онлайн дейности, предприети в контекста на тези дейности[210]. И обратното, правилата за защита на данните се прилагат в пълна степен за администраторите и обработващите лични данни, които осигуряват средствата за обработване на лични данни при лични дейности или дейности в рамките на домакинството (например платформите на социални мрежи)[211].

Достъпът на гражданите до интернет и възможността да използват платформи за електронна търговия, социални мрежи и блогове, за да споделят лична информация за себе си и за други лица, все повече затруднява разграничаването на обработването на данни при лични дейности и при дейности, които не са лични[212]. От конкретните обстоятелства зависи дали дейностите са изцяло лични, или в рамките на домакинството[213]. Дейности, които имат професионални или търговски аспекти, не могат да попаднат в обхвата на изключението за дейности в рамките на домакинството[214]. Следователно когато мащабът и честотата на обработването на данни предполагат професионална или целодневна дейност, частното лице би могло да се счита за администратор. Освен професионалния или търговския характер на дейността по обработването на данни, друг фактор, който трябва да се вземе предвид, е дали личните данни се предоставят на голям брой лица, които очевидно не спадат към сферата на личния живот на лицето. От съдебната практика във връзка с Директивата за защита на личните данни става ясно, че правото за защита на данните е приложимо, когато частно лице публикува данни за други лица в публичен уебсайт, докато използва интернет. Съдът на ЕС още не се е произнасял относно подобни факти съгласно ОРЗД, където са предвидени повече насоки по темите, които могат да бъдат считани извън обхвата на законодателството за защита на данните поради „изключението за дейности в рамките на домакинството", като например използването на социални медии за лични цели.

210 Общ регламент относно защитата на данните, съображение 18.

211 *Пак там*, съображение 18; Обяснителен доклад към модернизираната Конвенция № 108, параграф 29.

212 Вж. изявлението на Работната група по член 29 по дискусиите относно пакета с реформи за защита на данните (2013 г.), *приложение 2: Предложения и изменения относно изключението за лични дейности или дейности в рамките на домакинството,* 27 февруари 2013 г.

213 Обяснителен доклад към модернизираната Конвенция № 108, параграф 28.

214 Вж. Общ регламент относно защитата на данните, съображение 18, и Обяснителен доклад към модернизираната Конвенция № 108, параграф 27.

Пример: Делото *Bodil Lindqvist*[215] се отнася до позоваването в интернет страница на различни лица по име или по друг начин, например чрез телефонен номер или данни за развлеченията им. Съдът на ЕС счита, че: „действие, състоящо се в позоваването в интернет страница на различни лица и определянето им или по име, или по друг начин [...], представлява „автоматизирана изцяло или отчасти обработка на лични данни“ по смисъла на член 3, параграф 1 от Директивата за защита на личните данни[216].

Такова обработване на лични данни не попада в категорията на чисто личните дейности или дейностите в рамките на домакинството, които са извън обхвата на правилата за защита на личните данни в ЕС, тъй като това изключение „трябва [...] да се тълкува като отнасящо се единствено до дейностите, които са част от личния или семейния живот на физическите лица, като очевидно не е такъв случаят с обработването на лични данни, което обхваща публикуването им в интернет, с което те стават достъпни за неопределен брой лица“[217].

Според Съда на ЕС видеозаписите от частно инсталирана камера за наблюдение също могат при определени обстоятелства да попаднат в обхвата на законодателството на ЕС в областта на защитата на данните.

Пример: В делото *František Ryneš*[218] г-н Ryneš е записал образите на две лица, които счупили прозорци на дома му, чрез домашна система за видеонаблюдение, която е инсталирал, за да защити собствеността си. Записите след това били предадени в полицията и използвани в рамките на образуваното наказателно производство.

215 Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г.

216 *Пак там*, параграф 27; предходна Директива 95/46/ЕО, член 3, параграф 1, понастоящем Общ регламент относно защитата на данните, член 2, параграф 1.

217 Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г., параграф 47.

218 Съд на ЕС, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 декември 2014 г., параграф 33.

Съдът на ЕС посочва, че „доколкото видеонаблюдение [...] 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“ [...]“[219].

Администратор

Съгласно правото на ЕС администраторът е определен като структура, която „сама или съвместно с други определя целите и средствата за обработването на лични данни“[220]. С решение на администратора се определят причината за и начинът на обработване на данните.

Съгласно правото на Съвета на Европа модернизираната Конвенция № 108 определя „администратора“ като „физическо или юридическо лице, публичен орган, служба, агенция или друга структура, която сама или съвместно с други има правомощия да взема решения относно обработването на данни“[221]. Тези правомощия за вземане на решения се отнасят до целите и средствата за обработването, както и до категориите данни, подлежащи на обработване, и достъпа до тях[222]. Дали тези правомощия произтичат от правно основание или от фактически обстоятелства, трябва да се решава за всеки случай поотделно[223].

Пример: Делото *Google Spain*[224] е заведено от испански гражданин, подал искане Google да заличи стара публикация в ежедневник относно неговата финансова история.

Към Съда на ЕС е отправен въпросът дали Google, в качеството си на управляващ интернет търсачката, се явява „администратор“ на данни по смисъла на член 2, буква г) от Директивата за защита на личните

219 Предходна Директива 95/46/ЕО, член 3, параграф 2, второ тире, понастоящем Общ регламент относно защитата на данните, член 2, параграф 2, буква в).

220 Общ регламент относно защитата на данните, член 4, параграф 7.

221 Модернизирана Конвенция № 108, член 2, буква г).

222 Обяснителен доклад към модернизираната Конвенция № 108, параграф 22.

223 *Пак там*.

224 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г.

данни[225]. Съдът на ЕС приема широко по съдържанието си определение на понятието „администратор“, за да се гарантира „ефикасна и пълна защита на съответните лица“[226]. Съдът на ЕС приема, че управляващият интернет търсачката е определял целите и средствата на дейността и е направил данните, въведени на страници в интернет от издатели на уебсайтове, достъпни за всеки потребител на интернет, който извършва търсене по името на субекта на данните[227]. Поради това Съдът на ЕС определя, че Google може да се счита за „администратор“[228].

Когато администратор или обработващ лични данни е установен извън ЕС, това дружество трябва да определи писмено представител в ЕС[229]. В ОРЗД се подчертава, че представителят трябва да е установен „в една от държавите членки, в която се намират субектите на данни, чиито лични данни се обработват във връзка с предлагането на стоки или услуги или чието поведение се наблюдава“[230]. Ако не бъде определен представител, все пак биха могли да бъдат предприети правни действия срещу самия администратор или обработващ личните данни[231].

Съвместно обработване на лични данни от повече от един администратор

В ОРЗД е предвидено, че когато двама или повече администратори съвместно определят целите и средствата на обработването, те се считат за съвместни администратори. Това означава, че те решават заедно да обработват данни с определена обща цел[232]. В обяснителния доклад към модернизира-

225 Общ регламент относно защитата на данните, член 4, параграф 7; Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграф 21.

226 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграф 34.

227 *Пак там*, параграфи 35–40.

228 *Пак там*, параграф 41.

229 Общ регламент относно защитата на данните, член 27, параграф 1.

230 *Пак там*, член 27, параграф 3.

231 *Пак там*, член 27, параграф 5.

232 *Пак там*, член 4, параграф 7 и член 26.

ната Конвенция № 108 се посочва, че множество администратори или съвместно администриране са възможни и в **рамката на Съвета на Европа**[233].

Работната група по член 29 посочва, че съвместното обработване на данни от повече от един администратор може да приеме различни форми и че участието на различните администратори в дейностите по упражняване на контрол може да не е разпределено поравно[234]. Тази гъвкавост позволява да се предприемат действия по отношение на все по-сложните реалности в областта на обработването на данни[235]. Поради това съвместните администратори трябва да определят в конкретно споразумение съответните си отговорности по спазването на задълженията, произтичащи от регламента[236].

Съвместното обработване на лични данни от повече от един администратор води до съвместна отговорност за дейността по обработването[237]. В рамките на **правото на ЕС** това означава, че от всеки администратор или обработващ лични данни може да се търси отговорност за цялата вреда, причинена от обработването от съвместни администратори, за да се гарантира действително обезщетение на субекта на данни[238].

Пример: База данни, съвместно управлявана от няколко кредитни институции при работата им с техни неизправни клиенти, е често срещан пример за съвместно обработване на лични данни от повече от един администратор. Когато някой кандидатства за кредитиране от банка, която е един от съвместните администратори, банките проверяват базата данни, за да получат информация при вземането на информирани решения за кредитоспособността на кандидата.

В правните разпоредби не е изрично записано дали съвместното обработване на лични данни от повече от един администратор изисква целта да бъде

233 Модернизирана Конвенция № 108, член 2, буква г); Обяснителен доклад към модернизираната Конвенция № 108, параграф 22.

234 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 19.

235 *Пак там*.

236 Общ регламент относно защитата на данните, съображение 79.

237 *Пак там*, параграф 21.

238 *Пак там*, член 82, параграф 4.

една и съща за всеки един от администраторите, или е достатъчно техните цели да се припокриват само частично. За момента все още не съществува приложима съдебна практика на европейско равнище. В становището си от 2010 г. относно администраторите и обработващите данни Работната група по член 29 посочва, че съвместните администратори могат да споделят всички цели и средства на дадено обработване или могат да споделят само някои цели или средства, или пък част от тях[239]. Докато първото би означавало много тясна връзка между различните участници, второто би показало по-слаба връзка между тях.

Работната група по член 29 се застъпва за по-широко тълкуване на понятието за съвместно обработване на лични данни от повече от един администратор с цел да се даде възможност за известна гъвкавост, за да бъдат взети предвид по-сложните ситуации, които възникват по отношение на обработването на данни[240]. Дело, свързано с Дружеството за световна междубанкова финансова телекомуникация (SWIFT), илюстрира позицията на Работната група.

Пример: В така нареченото дело SWIFT европейските банкови институции са използвали SWIFT, първоначално като обработващи лични данни, за да осъществяват трансфера на данни в хода на банковите транзакции. SWIFT е разкрило на Министерството на финансите на САЩ данни за банкови транзакции, съхранявани в изчислителен център в Съединените американски щати (САЩ), без това да му е било изрично разпоредено от европейските банкови институции, които са използвали услугите му. При оценяване на законосъобразността на тази ситуация Работната група по член 29 е стигнала до заключението, че европейските банкови институции, използващи SWIFT, както и самото дружество SWIFT е трябвало да се разглеждат като съвместни администратори, отговорни пред европейските клиенти за разкриването на техни данни на органите на САЩ[241].

239 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 19.

240 *Пак там*.

241 Работна група по член 29 (2006 г.), *Становище 10/2006 относно обработката на лични данни от Дружеството за световна междубанкова финансова телекомуникация (SWIFT)*, WP 128, Брюксел, 22 ноември 2006 г.

Обработващ лични данни

Съгласно правото на ЕС „обработващ лични данни“ означава лице, което обработва лични данни от името на администратор[242]. Дейностите, възложени на един обработващ лични данни, може да бъдат ограничени до много специфична задача или цел или може да са доста общи и всеобхватни.

Съгласно правото на Съвета на Европа значението на понятието „обработващ лични данни“ е същото като в правото на ЕС[243].

Обработващите лични данни лица, освен че обработват данни за други лица, ще бъдат и администратори по отношение на обработването, което извършват за свои собствени цели, например администрирането на своите собствени служители, продажби и сметки.

Пример: Дружеството Everready е специализирано в областта на обработването на данни за управление на човешките ресурси на други дружества. В тази си функция Everready е обработващ лични данни. Когато обаче Everready обработва данните на собствените си служители, то е администратор на операциите по обработването на данни за целите на изпълнението на своите задължения като работодател.

Връзка между администратора и обработващия лични данни

Както е видно, администраторът е този, който определя целите и средствата на обработването. В ОРЗД ясно се посочва, че обработващият лични данни може да обработва лични данни само по нареждане на администратора, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка[244]. Договорът между администратора и обработващия лични данни е съществен елемент от техните отношения и е законово изискване[245].

242 Общ регламент относно защитата на данните, член 4, параграф 8.

243 Модернизирана Конвенция № 108, член 2, буква е).

244 Общ регламент относно защитата на данните, член 29.

245 *Пак там*, член 28, параграф 3.

Пример: Директорът на дружеството Sunshine решава, че дружеството Cloudy, специалист по съхранение на данни в облак, следва да управлява данните на клиентите на Sunshine. Дружеството Sunshine продължава да бъде администраторът на данните, а дружеството Cloudy е само обработващ лични данни, тъй като според договора Cloudy може да използва данните на клиентите на дружеството Sunshine само за определени от Sunshine цели.

Дори ако правомощието за определяне на средствата на обработването е делегирано на обработващ лични данни, администраторът трябва да може да упражнява в подходяща степен контрол върху решенията на обработващия лични данни по отношение на средствата на обработването. Цялостната отговорност се носи от администратора, който трябва да упражнява надзор над обработващите лични данни, за да гарантира, че техните решения съответстват на законодателството за защита на данните и на собствените му указания.

Освен това ако обработващият лични данни не зачита определените от администратора условия по отношение на обработването на данните, то обработващият лични данни се превръща в администратор поне в степента, в която е нарушил указанията на администратора. Това най-вероятно ще превърне обработващия лични данни в администратор, който действа незаконосъобразно. От своя страна, първоначалният администратор ще трябва да обясни как е било възможно обработващият лични данни да наруши неговите нареждания[246]. Действително, има тенденция Работната група по член 29 в такива случаи да приема, че е налице съвместно обработване на лични данни от повече от един администратор, тъй като това осигурява най-добра защита на интересите на субектите на данни[247].

Също така може да съществуват проблеми във връзка с разпределянето на отговорността в случаите, в които администраторът е малко предприятие, а обработващият лични данни е голяма корпорация, която има правомощието да диктува условията за своите услуги. При такива обстоятелства

246 *Пак там*, член 82, параграф 2.

247 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 25; Работна група по член 29 (2006 г.), *Становище 10/2006 относно обработката на лични данни от Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Брюксел, 22 ноември 2006 г.

обаче Работната група по член 29 твърди, че стандартът по отношение на отговорността не следва да се занижава въз основа на липсата на икономическо равновесие и че трябва да се запази разбирането за понятието „администратор“[248].

За по-голяма яснота и прозрачност отношенията между администратора и обработващия лични данни трябва да бъдат подробно документирани в писмен договор[249]. В договора трябва, по-специално, да са включени предметът, естеството, целта и продължителността на обработването, видът лични данни и категориите субекти на данни. В него трябва също така да са уредени задълженията и правата на администратора и на обработващия лични данни, като например изискванията относно поверителността и сигурността. Липсата на такъв договор е нарушение на задължението на администратора да предостави писмена документация за взаимните задължения и може да доведе до санкции. Когато е причинена вреда в резултат на действие извън законосъобразните указания на администратора или в противоречие с тях, отговорност носи не само администраторът, но и обработващият лични данни[250]. Обработващият лични данни трябва да поддържа регистър на всички категории дейности по обработването, извършени от името на администратора[251]. Тези регистри трябва да се предоставят на надзорния орган при поискване, тъй като и администраторът, и обработващият лични данни трябва да си сътрудничат с този орган при изпълнението на своите задачи[252]. Администраторите и обработващите лични данни също така имат възможността да се придържат към одобрен кодекс за поведение или механизъм за сертифициране, за да докажат, че спазват изискванията на ОРЗД[253].

Обработващите лични данни може да проявят желание да делегират определени задачи на други обработващи лични данни, действащи като подизпълнители. По закон това е допустимо, при условие че са предвидени подходящи договорни клаузи между администратора и обработващия лични данни, включително дали е необходимо разрешението на администратора за всеки

248 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни“ и „лице, което обработва данните“*, WP 169, Брюксел, 16 февруари 2010 г., стр. 26.

249 Общ регламент относно защитата на данните, член 28, параграфи 3 и 9.

250 *Пак там*, член 82, параграф 2.

251 *Пак там*, член 30, параграф 2.

252 *Пак там*, член 30, параграф 4 и член 31.

253 *Пак там*, член 28, параграф 5 и член 42, параграф 4.

отделен случай или дали информирането само по себе си е достатъчно. ОРЗД предвижда, че първоначалният обработващ данните продължава да носи пълна отговорност пред администратора, когато другият обработващ лични данни не изпълни задълженията си, свързани със защита на данните[254].

Съгласно правото на Съвета на Европа обясненото по-горе тълкуване на понятията „администратор" и „обработващ лични данни" е напълно приложимо[255].

2.3.2 Получатели и трети страни

Разликата между тези две категории лица или субекти, които бяха въведени с Директивата за защита на личните данни, се състои най-вече във връзката им с администратора, а оттам и в разрешението им за достъп до съхраняваните от администратора лични данни.

„Трета страна" е лице, различно от администратора или обработващия лични данни. Съгласно член 4, параграф 10 от ОРЗД „трета страна" означава „физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни". Това означава, че лица, работещи за организация, която е различна от администратора, дори ако тя принадлежи към същата група или холдинг, са (или принадлежат към) „трета страна". От друга страна, клоновете на банка, която обработва сметки на клиент под прякото ръководство на своето главно управление, не са „трети страни"[256].

Терминът „получател" е по-широк от термина „трета страна". По смисъла на член 4, параграф 9 от ОРЗД „получател" означава „физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не". Този получател може да бъде или лице извън организацията на администратора, или обработващият лични данни — тогава той би бил трета страна, или някой вътре

254 *Пак там,* член 28, параграф 4.

255 Вж. например модернизираната Конвенция № 108, член 2, букви б) и е); Препоръка относно профилирането, член 1.

256 Работна група по член 29 (2010 г.), *Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните"*, WP 169, Брюксел, 16 февруари 2010 г., стр. 31.

в организацията на администратора или обработващия лични данни, като например служител или друг отдел в рамките на същото дружество или орган.

Разграничението между получатели и трети страни е важно само заради условията за законосъобразно разкриване на данни. Служителите на даден администратор или обработващ лични данни могат да бъдат получатели на лични данни без наличието на допълнително правно изискване, ако участват в операциите по обработване, извършвани от администратора или обработващия лични данни. На третата страна, тъй като е отделен от администратора или обработващия лични данни субект, не е разрешено да използва личните данни, обработвани от администратора, освен при наличието на специални правни основания в конкретния случай.

Пример: Служител на администратора, който използва лични данни в рамките на изпълнение на задачите, възложени му от работодателя, е получател на данните, но не е трета страна, тъй като той използва данните от името на и съгласно указанията на администратора. Например ако работодател разкрие на отдела си по човешки ресурси лични данни за своите служители във връзка с предстоящи оценки на тяхната работа, служителите на отдела по човешки ресурси ще бъдат получатели на лични данни, тъй като данните са им били разкрити в хода на обработването им за администратора.

Ако обаче организацията предоставя данни за служителите си на дружество за обучение, което ще ги използва, за да създаде програма за обучение на персонала, обучаващото дружество е трета страна. Причината е, че дружеството за обучение няма конкретна легитимност или правомощие (което в случая с отдела по човешки ресурси произтича от трудовите правоотношения с администратора) да обработва тези лични данни. С други думи, те не са получили информацията в рамките на трудови правоотношения с администратора на данните.

2.4 Съгласие

Ключови въпроси

- Съгласието, като правно основание за обработване на лични данни, трябва да е свободно изразено, информирано, конкретно и недвусмислено указание за волята на лицето посредством ясен утвърдителен акт, изразяващ съгласие за обработването.
- Обработването на специални категории данни изисква изрично съгласие.

Както ще бъде подробно разгледано в глава 4, съгласието е едно от шестте законни основания за обработването на лични данни. „Съгласие“ означава „всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните“[257].

Правото на ЕС предвижда няколко елемента, при наличието на които дадено съгласие е валидно, с които се цели да се гарантира, че субектите на данни действително са имали намерение да дадат съгласието си за конкретно използване на техните данни[258]:

- Съгласието трябва да бъде дадено чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на личните му данни. Този акт може да бъде действие или изявление.
- Субектът на данни трябва да има правото да оттегли съгласието си по всяко време.
- В рамките на писмена декларация, която обхваща и други въпроси, като „условия на услугата“, исканията за съгласие трябва да са на ясен и разбираем език и в разбираема и леснодостъпна форма, като се прави ясно разграничение между съгласието и другите въпроси; ако част от тази декларация нарушава ОРЗД, тя не е обвързваща.

Съгласието е валидно в контекста на законодателството за защита на данните само ако са изпълнени всички тези изисквания. Администраторът трябва да

257 Общ регламент относно защитата на данните, член 4, параграф 11. Вж. също модернизираната Конвенция № 108, член 5, параграф 2.

258 Общ регламент относно защитата на данните, член 7.

може да докаже, че субектът на данни е дал съгласие за обработване на личните му данни[259]. Елементите на валидното съгласие ще бъдат разгледани допълнително в раздел 4.1.1 относно законните основания за обработване на лични данни.

В Конвенция № 108 не се съдържа определение за съгласие; такова е дадено в националното законодателство. Съгласно **правото на Съвета на Европа** обаче елементите на валидното съгласие съвпадат с обяснените по-горе[260].

Допълнителните изисквания за валидно съгласие съгласно гражданското право, каквото е изискването за правоспособност, естествено също се прилагат в контекста на защита на данните, тъй като те са основни правни предпоставки. Невалидното съгласие на лица, които нямат правоспособност, ще доведе до липса на правно основание за обработване на данни за тези лица. Що се отнася до правоспособността на непълнолетните лица да сключват договори, ОРЗД предвижда, че неговите правила за минималната възраст за получаване на валидно съгласие не засягат общото договорно право на държавите членки[261].

Съгласието трябва да бъде изразено ясно, така че да не оставя никакво съмнение относно намерението на субекта на данни[262]. Съгласието трябва да бъде изрично, когато се отнася до обработването на чувствителни данни, и да бъде устно или писмено[263]. Последното може да бъде направено по електронен път[264]. Според **правото** както на **ЕС**, така и на **Съвета на Европа** съгласието за обработване на лични данни на дадено лице трябва да бъде изразено чрез изявление или ясно потвърждаващо действие[265]. Следователно съгласието не може да произтича от мълчание, предварително отметнати полета, предварително попълнени формуляри или липса на действие[266].

259 *Пак там,* член 7, параграф 1.

260 Модернизирана Конвенция № 108, член 5, параграф 2; Обяснителен доклад към модернизираната Конвенция № 108, параграфи 42–45.

261 Общ регламент относно защитата на данните, член 8, параграф 3.

262 *Пак там*, член 6, параграф 1, буква а) и член 9, параграф 2, буква а).

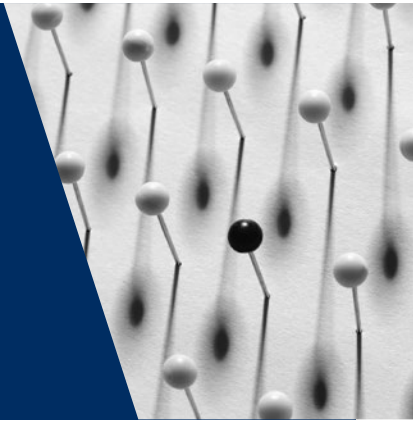
263 *Пак там*, съображение 32.

264 *Пак там*.

265 *Пак там*, член 4, параграф 11; Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

266 Общ регламент относно защитата на данните, съображение 32; Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

3 Основни принципи на европейското право в областта на защитата на данните



ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните, член 5, параграф 1, буква а)	**Принципът на законосъобразност**	Модернизирана Конвенция № 108, член 5, параграф 3
Общ регламент относно защитата на данните, член 5, параграф 1, буква а)	**Принципът на добросъвестност**	Модернизирана Конвенция № 108, член 5, параграф 4, буква а) ЕСПЧ, *К.Н. и други/Словакия*, № 32881/04, 2009 г.
Общ регламент относно защитата на данните, член 5, параграф 1, буква а) Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 2015 г.	**Принципът на прозрачност**	Модернизирана Конвенция № 108, член 5, параграф 4, буква а) и член 8 ЕСПЧ, *Haralambie/Румъния*, № 21737/03, 2009 г.
Общ регламент относно защитата на данните, член 5, параграф 1, буква б)	**Принципът на ограничение на целите**	Модернизирана Конвенция № 108, член 5, параграф 4, буква б)
Общ регламент относно защитата на данните, член 5, параграф 1, буква в) Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и Kärntner Landesregierung и други* [голям състав], 2014 г.	**Принципът на свеждане на данните до минимум**	Модернизирана Конвенция № 108, член 5, параграф 4, буква в)

ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните, член 5, параграф 1, буква г) Съд на ЕС, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 2009 г.	**Принципът на точност на данните**	Модернизирана Конвенция № 108, член 5, параграф 4, буква г)
Общ регламент относно защитата на данните, член 5, параграф 1, буква д) Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и Kärntner Landesregierung и други* [голям състав], 2014 г.	**Принципът на ограничение на съхранението**	Модернизирана Конвенция № 108, член 5, параграф 4, буква д) ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 2008 г.
Общ регламент относно защитата на данните, член 5, параграф 1, буква е) и член 32	**Принципът на сигурност на данните (цялостност и поверителност)**	Модернизирана Конвенция № 108, член 7
Общ регламент относно защитата на данните, член 5, параграф 2	**Принципът на отчетност**	Модернизирана Конвенция № 108, член 10

Член 5 от Общия регламент относно защитата на данните установява принципите, които регламентират обработването на лични данни. Тези принципи включват:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите;
- свеждане на данните до минимум;
- точност на данните;
- ограничение на съхранението;
- цялостност и поверителност.

Принципите служат като отправна точка за по-подробни разпоредби в следващите членове от регламента. Те се споменават и в членове 5, 7, 8 и 10 от

модернизираната Конвенция № 108. Цялото последващо законодателство в областта на защитата на данните на ниво Съвет на Европа или ЕС трябва да отговаря на тези принципи и те трябва да се вземат предвид при тълкуването на това законодателство. Съгласно правото на ЕС ограничения на принципите за обработване на лични данни са разрешени само до степента, в която отговарят на правата и задълженията, предвидени в членове 12—22, и трябва да зачитат същността на основните права и свободи. Всякакви изключения от и ограничения на тези основни принципи може да бъдат предвидени на ниво ЕС или на национално равнище[267]; те трябва да бъдат предвидени от закона, с тях да се преследва законна цел и да представляват необходими и пропорционални мерки в едно демократично общество[268]. Трябва да бъдат изпълнени всичките три условия.

3.1 Законосъобразност, добросъвестност и прозрачност на принципите за обработване на данни

Ключови въпроси

- Принципите на законосъобразност, добросъвестност и прозрачност са приложими за всяко обработване на лични данни.
- Съгласно ОРЗД законосъобразността изисква да е налице поне едно от следните условия:
  - съгласие на субекта на данните;
  - необходимост за сключване на договор;
  - законово задължение;
  - необходимост да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;
  - необходимост за изпълнение на задача от обществен интерес;

267 Модернизирана Конвенция № 108, член 11, параграф 1; Общ регламент относно защитата на данните, член 23, параграф 1.

268 Общ регламент относно защитата на данните, член 23, параграф 1.

  - необходимост за целите на легитимните интереси на администратора или на трета страна с изключение на случаите, когато пред тези интереси имат преимущество интересите и правата на субекта на данните.

- Обработването на лични данни следва да се прави по добросъвестен начин.
  - Субектът на данните трябва да бъде информиран за риска, за да се гарантира, че обработването няма да има непредвидими отрицателни последици.
- Обработването на лични данни следва да се прави по прозрачен начин.
  - Администраторите трябва да информират субектите на данните, преди да обработват техните данни, наред с другите подробности и относно целта на обработването и относно самоличността и адреса на администратора.
  - Информацията за операциите по обработване трябва да бъде предоставена на ясен и разбираем език, така че субектите на данните да могат лесно да разберат правилата, рисковете, гаранциите и правата, свързани с това обработване.
  - Субектите на данните имат право на достъп до своите данни във всички случаи, в които те биват обработвани.

3.1.1 Законосъобразност на обработването

Правото на ЕС и на Съвета на Европа в областта на защитата на данните изисква личните данни да бъдат обработвани законосъобразно[269]. Законосъобразното обработване изисква съгласието на субекта на данните или друго легитимно основание, предвидено в законодателството за защита на данните[270]. Член 6, параграф 1 от ОРЗД включва пет законови основания за обработване в допълнение към съгласието, т.е. когато обработването на лични данни е необходимо за изпълнението на договор, за изпълнението на задача, извършвана при упражняване на публични правомощия, за спазване на законово задължение, за целите на легитимните интереси на администратора или на трета страна или ако е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данни. Това ще бъде разгледано по-подробно в раздел 4.1.

269 Модернизирана Конвенция № 108, член 5, параграф 3; Общ регламент относно защитата на данните, член 5, параграф 1, буква а).

270 Харта на основните права на Европейския съюз, член 8, параграф 2; Общ регламент относно защитата на данните, съображение 40 и членове 6—9; модернизирана Конвенция № 108, член 5, параграф 2; Обяснителен доклад към модернизираната Конвенция № 108, параграф 41.

3.1.2 Добросъвестност на обработването

В допълнение към законосъобразното обработване правото на ЕС и на Съвета на Европа в областта на защитата на данните изисква личните данни да бъдат обработвани добросъвестно[271]. Принципът на добросъвестно обработване регламентира предимно взаимоотношенията между администратора и субекта на данните.

Администраторите следва да уведомят субектите на данните и широката общественост, че ще обработват данните по законосъобразен и прозрачен начин и трябва да могат да докажат, че операциите по обработване са в съответствие с ОРЗД. Операциите по обработване не трябва да се извършват тайно и субектите на данни следва да са уведомени за потенциалните рискове. Освен това администраторите, доколкото е възможно, трябва да действат по начин, който точно да съответства на желанията на субекта на данни, особено когато неговото съгласие представлява правното основание за обработването на данните.

Пример: В делото *К.Н и други/Словакия*[272] жалбоподателките — жени от ромски етнически произход — са били на лечение в две болници в Източна Словакия по време на бременност и раждане. След това нито една от тях не е успяла отново да зачене дете въпреки неднократните опити. Националните съдилища са издали нареждане на болниците да разрешат на жалбоподателките и представляващите ги лица да разгледат и направят писмени извадки от медицинските документи, но са отхвърлили искането им да фотокопират документите с твърдението, че това е с цел да се предотврати злоупотреба с тях. Положителните задължения на държавите съгласно член 8 от ЕКПЧ непременно включват задължение на субектите на данни да бъдат предоставяни копия от техните досиета с данни. Държавата е тази, която е трябвало да определи условията за копиране на досиетата с лични данни или, когато е уместно, да представи убедителни причини за отказа да се извърши това. В случая на жалбоподателките националните съдилища са обосновали забраната за изготвяне на копия на медицинските документи от страна на жалбоподателките

271 Общ регламент относно защитата на данните, член 5, параграф 1, буква а); модернизирана Конвенция № 108, член 5, параграф 4, буква а).

272 ЕСПЧ, *К.Н. и други/Словакия*, № 32881/04, 28 април 2009 г.

главно чрез необходимостта да се защити съответната информация от злоупотреба. ЕСПЧ обаче не счита, че жалбоподателките, които при всички случаи са имали достъп до пълните медицински досиета, биха могли да злоупотребят с информация, касаеща тях самите. Освен това рискът от такава злоупотреба е било възможно да бъде предотвратен по начин, различен от отказа на жалбоподателките да направят копия на досиетата, например чрез ограничаване на броя на лицата, имащи право на достъп до досиетата. Държавата не е успяла да докаже съществуването на достатъчно убедителни причини на жалбоподателките да бъде отказан ефективен достъп до информация, касаеща тяхното здраве. Съдът заключава, че е налице нарушение на член 8.

По отношение на интернет услугите функционалностите на системите за обработване на данни трябва да направят възможно субектите на данни действително да разбират какво се случва с техните данни. Във всеки случай принципът на добросъвестност надхвърля задълженията за прозрачност и би могъл да бъде свързан и с обработването на лични данни по етичен начин.

Пример: Изследователският отдел на университет провежда експеримент, като анализира промените в настроението на 50 души. Те са помолени да записват мислите си в електронен файл в определен момент всеки час. 50-те лица са дали съгласието си за този конкретен проект и за този конкретен начин, по който университетът да използва данните. Изследователският отдел скоро открива, че електронното регистриране на мислите ще е много полезно за друг проект, насочен към психическото здраве, който се координира от друг екип. Въпреки че като администратор университетът е можел да използва същите данни за работата на друг екип, без да предприема по-нататъшни стъпки за осигуряване на законосъобразността на обработването на тези данни, като се има предвид, че целите са съвместими, университетът е уведомил лицата и е поискал ново съгласие в съответствие с етичния си кодекс относно проучванията и принципа на добросъвестно обработване.

3.1.3 Прозрачност на обработването

Правото на ЕС и на Съвета на Европа в областта на защитата на данните изисква обработването на лични данни да се извършва „по прозрачен начин по отношение на субекта на данните“[273].

Този принцип създава задължение за администратора да вземе всички подходящи мерки, за да могат субектите на данни — потребители или клиенти — да бъдат информирани относно това как се използват техните данни[274]. Прозрачността може да се отнася до информацията, предоставяна на лицето, преди да започне обработването[275], информацията, която следва да бъде леснодостъпна за субектите на данни по време на обработването[276], но също и информацията, предоставяна на субектите на данни след искане за достъп до техните собствени данни[277].

Пример: В делото *Haralambie/Румъния*[278] на жалбоподателя е предоставен достъп до информацията, която секретната служба е съхранявала за него, едва пет години след неговото искане. ЕСПЧ отново заявява, че лицата с лични досиета, съхранявани от публични органи, имат жизненоважен интерес да разполагат с възможност за достъп до тези досиета. Органите са имали задължение да осигурят ефективна процедура за получаване на достъп до такава информация. ЕСПЧ счита, че нито количеството на предадените досиета, нито недостатъците в системата за архивиране оправдават забавянето от пет години да се удовлетвори искането на жалбоподателя за достъп до неговото досие. Органите не са осигурили ефективна и достъпна процедура за жалбоподателя, за да му дадат възможност да получи достъп до неговото лично досие в разумен срок. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

273 Общ регламент относно защитата на данните, член 5, параграф 1, буква а); модернизирана Конвенция № 108, член 5, параграф 4, буква а) и член 8.

274 Общ регламент относно защитата на данните, член 12.

275 *Пак там,* членове 13 и 14.

276 Работна група по член 29, *Становище 2/2017 относно обработването на данни на работното място*, WP 249, стр. 23.

277 Общ регламент относно защитата на данните, член 15.

278 ЕСПЧ, *Haralambie/Румъния*, № 21737/03, 27 октомври 2009 г.

Операциите по обработването трябва да бъдат обяснени на субектите на данни по леснодостъпен начин, който да гарантира, че те разбират какво ще се случи с данните им. Това означава, че субектът на данни трябва да знае конкретната цел на обработването на лични данни в момента на събирането им[279]. Прозрачността на обработването изисква да се използва ясен и разбираем език[280]. На заинтересованите лица трябва са ясни рисковете, правилата, гаранциите и правата, свързани с обработването на личните им данни[281].

В **правото на Съвета на Европа** също така се уточнява, че администраторът задължително трябва да предоставя по активен начин на субектите на данни определена съществена информация. Информацията относно наименованието и адреса на администратора (или на съвместните администратори), правното основание и целта на обработването на данни, категориите на обработваните данни и получателите, както и средствата за упражняване на правата могат да бъдат предоставяни на субектите на данни във всякакъв подходящ формат (чрез уебсайт, чрез технически средства върху персонални устройства и т.н.), стига информацията да бъде представяна на субекта на данни добросъвестно и ефективно. Представената информация следва да бъде леснодостъпна, четима, разбираема и пригодена към съответните субекти на данни (например на разбираем за деца език, когато това е необходимо). Трябва да бъде предоставяна и всяка допълнителна информация, която е необходима, за да се гарантира добросъвестно обработване на данните, или която е от полза за тази цел, като например периодът на запазване на данните, причините за обработването на данните или информация за предаването на данни на получател в друга страна по договора или трета страна (включително дали тази конкретна трета страна предоставя подходящо ниво на защита или какви са мерките, предприети от администратора за гарантиране на това подходящо ниво на защита на данните)[282].

В съответствие с правото на достъп[283] субектът на данни има правото, при поискване, да бъде уведомен от администратора дали се обработват негови данни и ако това е така, кои данни са предмет на такова обработване[284]. Освен

279 Общ регламент относно защитата на данните, съображение 39.

280 *Пак там*.

281 *Пак там*.

282 Обяснителен доклад към модернизираната Конвенция № 108, параграф 68.

283 Общ регламент относно защитата на данните, член 15.

284 Модернизирана Конвенция № 108, член 8 и член 9, параграф 1, буква б).

това в съответствие с правото на информация[285] лицата, чиито данни се обработват, трябва да бъдат уведомявани активно от администраторите или от обработващите лични данни, по принцип преди да започне дейността по обработване, наред с другите подробности и относно целите, продължителността и средствата на обработване.

Пример: Делото *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*[286] се отнася до предаването на данъчни данни за доходите на самонаети лица от Националната агенция за управление на данъците на Националната здравноосигурителна каса на Румъния, въз основа на които е било изискано плащане на просрочени здравноосигурителни вноски. Към Съда на ЕС се отправя искането да определи дали субектите на данни е следвало да бъдат предварително уведомени за самоличността на администратора на данни и за целта на предаването на данните, преди тези данни да бъдат обработени от Националната здравноосигурителна каса. Съдът на ЕС постановява, че когато структура на публичната администрация на държава членка предава лични данни на друга структура на публичната администрация, която подлага тези данни на последващо обработване, субектите на данни трябва да бъдат уведомени за това предаване или обработване.

В някои ситуации са разрешени дерогации от задължението за уведомяване на субектите на данни относно обработването и те ще бъдат разгледани по-подробно в раздел 6.1 за правата на субектите на данни.

3.2 Принципът на ограничение на целите

Ключови въпроси

- Целта на обработването на данните трябва да бъде определенапреди да започне обработването.

285 Общ регламент относно защитата на данните, членове 13 и 14.

286 Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 1 октомври 2015 г., параграфи 28—46.

- Данните не може да се обработват по-нататък по начин, който е несъвместим с първоначалната цел, макар че Общият регламент относно защитата на данните предвижда изключения от това правило за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели.
- По същество принципът на ограничение на целите означава, че всяко обработване на лични данни трябва да се извършва за конкретна, ясно определена цел и само за конкретни допълнителни цели, които са съвместими с първоначалната цел.

Принципът на ограничение на целите е един от основните принципи на европейското право в областта на защитата на данните. Той е тясно свързан с прозрачността, предвидимостта и потребителския контрол: ако целта на обработването е достатъчно конкретна и ясна, физическите лица знаят какво да очакват и прозрачността и правната сигурност са по-големи. В същото време ясното очертаване на целта е важно, за да могат субектите на данни ефективно да упражняват правата си, като например правото на възражение срещу обработването[287].

Принципът изисква всяко обработване на лични данни да се извършва за конкретна, ясно определена цел и само за допълнителни цели, които са съвместими с първоначалната цел[288]. Следователно обработването на лични данни за неопределени и/или неограничени цели е незаконосъобразно. Обработването на лични данни без определена цел, само въз основа на съображението, че те може да бъдат полезни някога в бъдещето, също не е законосъобразно. Законосъобразността на обработването на лични данни ще зависи от целта на обработването, която трябва да е изрично указана, конкретна и легитимна.

Всяка нова цел за обработване на данните, която не е съвместима с първоначалната цел, трябва да има свое собствено конкретно правно основание и не може да се основава на факта, че данните са били първоначално получени или обработени с друга законна цел. От своя страна законосъобразното обработване е ограничено до първоначално определената си цел и всяка нова цел на обработването изисква отделно ново правно основание. Например разкриването на лични данни на трети страни за нова цел трябва да

287 Работна група по член 29 (2013 г.), *Становище 3/2013 относно ограничението на целите*, WP 203, 2 април 2013 г.

288 Общ регламент относно защитата на данните, член 5, параграф 1, буква б).

бъде внимателно обмислено, тъй като такова разкриване най-вероятно ще се нуждае от допълнително правно основание, различно от това за събирането на данните.

Пример: Авиокомпания събира данни от своите пътници, за да направи резервации, с цел правилното осъществяване на полета. Авиокомпанията се нуждае от данни за: номерата на местата на пътниците, специалните физически ограничения, като например необходимостта от инвалидни колички, и специалните изисквания по отношение на храната, като например кошер или халал. Ако към авиокомпаниите бъде отправено искане да предадат данните, които се съдържат в резервационните данни на пътниците, на имиграционните органи на летището при приземяването, тогава тези данни се използват за целите на имиграционния контрол, които са различни от първоначалната цел за събиране на данните. Предаването на тези данни на имиграционните органи следователно ще изисква ново и отделно правно основание.

Когато се разглеждат обхватът и ограниченията на конкретна цел, в модернизираната Конвенция № 108 и Общия регламент относно защитата на данните се разчита на понятието за съвместимост: използването на данни за съвместими цели е разрешено въз основа на първоначалното правно основание. Следователно обработването на данните по-нататък не може да се извършва по начин, който е неочакван, неподходящ или предизвикващ възражения по отношение на субекта на данните[289]. За да оцени дали по-нататъшното обработване може да се счита за съвместимо, администраторът следва да вземе предвид (наред с другите неща) следното:

- „всички връзки между тези цели и целите на предвиденото по-нататъшно обработване;

- в какъв контекст са събрани личните данни, по-специално основателните очаквания на субектите на данните въз основа на техните взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни;

289 Обяснителен доклад към модернизираната Конвенция № 108, параграф 49.

- естеството им;
- последствията от предвиденото по-нататъшно обработване на данни за субектите на данни; и
- наличието на подходящи гаранции при операциите по първоначалното и предвиденото по-нататъшно обработване“[290]. Това може да бъде извършено например чрез криптиране или псевдонимизация.

Пример: В хода на управлението на връзките с клиенти дружеството Sunshine придобива данни за тях (CRM данни). След това то предава тези данни на дружеството за директен маркетинг Moonlight, което иска да ги използва за подпомагане на маркетинговите кампании на трети дружества. Предаването на данните от дружеството Sunshine за целите на маркетинга на други дружества представлява последващо използване на данните за нова цел, която е несъвместима с управлението на връзките с клиенти – първоначалната цел на дружество Sunshine, за която са били събрани данните на клиентите. Предаването на данните на дружеството Moonlight следователно се нуждае от свое собствено правно основание.

За разлика от това, използването от дружеството Sunshine на CRM данните за негови собствени маркетингови цели, т.е. изпращането на маркетингови съобщения до собствени клиенти за собствени продукти на дружеството, по принцип се приема за съвместима цел.

В Общия регламент относно защитата на данните и в модернизираната Конвенция № 108 се посочва, че „по-нататъшното обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели“ се счита *a priori* за съвместимо с първоначалната цел[291]. Когато обаче се извършва по-нататъшно обработване на лични данни, трябва да бъдат въведени подходящи гаранции, като

290 Общ регламент относно защитата на данните, съображение 50 и член 6, параграф 4; Обяснителен доклад към модернизираната Конвенция № 108, параграф 49.

291 Общ регламент относно защитата на данните, член 5, параграф 1, буква б); модернизирана Конвенция № 108, член 5, параграф 4, буква б). Пример за такива национални разпоредби е австрийският Закон за защита на данните (*Datenschutzgesetz*), Federal Law Gazette (Федерален държавен вестник) I № 165/1999, параграф 46.

анонимизация, криптиране или псевдонимизация на данните, както и ограничение на достъпа до тях[292]. В Общия регламент относно защитата на данните е добавено, че „когато субектът на данните е дал съгласието си или когато обработването се основава на правото на Съюза или правото на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество, за да се гарантират, по-специално, важни цели от широк обществен интерес, на администратора следва да се позволи да обработва по-нататък личните данни, независимо от съвместимостта на целите“[293]. Следователно когато се предприема по-нататъшно обработване, субектът на данни следва да бъде информиран за целите, както и за неговите права, като например правото на възражение[294].

Пример: Дружеството Sunshine събира и съхранява данни за управление на връзките с клиенти (CRM данни) за своите клиенти. По-нататъшното използване на тези данни от дружеството Sunshine за статистически анализ на поведението на неговите клиенти по отношение на закупуването на стоки е допустимо, тъй като статистиката е съвместима цел. Не се изисква допълнително правно основание, като например съгласието на субектите на данните. За по-нататъшното обработване на личните данни за статистически цели обаче дружеството Sunshine трябва да въведе подходящи гаранции за правата и свободите на субектите на данни. Техническите и организационните мерки, които Sunshine трябва да приложи, може да включват псевдонимизация.

292 Общ регламент относно защитата на данните, член 6, параграф 4; модернизирана Конвенция № 108, член 5, параграф 4, буква б); Обяснителен доклад към модернизираната Конвенция № 108, параграф 50.

293 Общ регламент относно защитата на данните, съображение 50.

294 *Пак там*.

3.3 Принципът на свеждане на данните до минимум

Ключови въпроси

- Обработването на данни трябва да бъде ограничено до необходимото за постигане на легитимна цел.
- Личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства.
- Обработването на данни не може да води до непропорционална намеса в интересите, правата и свободите, които засяга.

Следва да бъдат обработвани само данни, които са „подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се [събират и/или] обработват [впоследствие]“[295]. Категориите на избраните данни за обработване трябва да бъдат необходими за постигане на обявената обща цел на операциите по обработването, а администраторът средва стриктно да ограничава събирането на данните до такава информация, която е директно свързана с конкретната цел на обработването.

Пример: В делото *Digital Rights Ireland*[296] Съдът на ЕС разглежда валидността на Директивата за запазване на лични данни, чиято цел е да хармонизира разпоредбите на националното право относно запазването на лични данни, създадени или обработени от общественодостъпни електронни съобщителни услуги или мрежи с цел евентуалното им предаване на компетентните органи за борба с тежки престъпления, като организирана престъпност и тероризъм. Въпреки че това е прието за причина, която действително удовлетворява цел от общ интерес, обстоятелството, че Директивата се прилага общо „за всички лица, за всички електронни съобщителни средства, както

295 Модернизирана Конвенция № 108, член 5, параграф 4, буква в); Общ регламент относно защитата на данните, член 5, параграф 1, буква в).

296 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

и за всички данни за трафик, без да въвежда никакво разграничаване, ограничаване или изключение с оглед на целта за борба с тежките престъпления“ е счетено за проблематично[297].

Освен това, чрез използването на специална технология за подобряване на неприкосновеността на личния живот понякога е възможно въобще да се избегне използването на лични данни или да се използват мерки за намаляване на възможността данните да се свържат с даден субект на данни (например чрез псевдонимизация), което води до решение, благоприятстващо неприкосновеността на личния живот. Това е особено подходящо в по-широкообхватни системи за обработване на данни.

Пример: Градският съвет предлага карта с чип за редовните потребители на градската обществена транспортна система срещу определена такса. Върху картата е изписано името на потребителя, като то се съдържа също и в електронна форма в чипа. Винаги когато се използва автобус или трамвай, картата с чип трябва да бъде поставена пред монтираните четящи устройства, например в автобуси и трамваи. Данните, прочетени от устройството, се проверяват електронно в база данни, съдържаща имената на хората, които са закупили карта за пътуване.

Тази система не спазва по оптимален начин принципа за свеждане на данните до минимум: проверката на това дали на дадено лице е разрешено да използва транспортната система може да се извърши, без да се сравняват личните данни в чипа на картата с база данни. Например би било достатъчно наличието на специален електронен образ, като например бар код, в чипа на картата, който при поставяне пред четящото устройство би потвърдил дали картата е валидна, или не. Такава система няма да записва кой е използвал дадено транспортно средство и по кое време. Това ще бъде оптималното решение по смисъла на принципа за свеждане на данните до минимум, тъй като този принцип спазва задължението събирането на данни да бъде сведено до минимум.

297 *Пак там*, параграфи 44 и 57.

В член 5, параграф 1 от модернизираната Конвенция № 108 се съдържа изискване за пропорционалност по отношение на обработването на лични данни във връзка с преследваната легитимна цел. Трябва да има справедлив баланс между всички засегнати интереси на всички етапи от обработването. Това означава, че „лични данни, които са подходящи и свързани, но биха наложили непропорционална намеса в засегнатите основни права и свободи, следва да се считат за прекомерни“[298].

3.4 Принципът на точност на данните

Ключови въпроси

- Принципът на точност на данните трябва да бъде прилаган от администратора във всички операции по обработването.
- Данни, които са неточни, трябва да бъдат своевременно изтрити или коригирани.
- Може да се наложи данните да се проверяват редовно и да бъдат поддържани в актуален вид, за да се осигури точността им.

Администратор, който съхранява лични данни, не трябва да ги използва, преди да е предприел необходимите стъпки за гарантиране на тяхната точност и актуалност[299].

Задължението за гарантиране на точността на данните трябва да бъде разглеждано в зависимост от целта за обработване на данните.

Пример: В делото *Rijkeboer*[300] Съдът на ЕС разглежда искането на нидерландски гражданин да получи информация от общинската администрация на град Амстердам относно самоличността на лицата, на които съхраняваните от общината данни за него са били съобщени през двете преходни години, а също и съдържанието на разкритите

298 Обяснителен доклад към модернизираната Конвенция № 108, параграф 52; Общ регламент относно защитата на данните, член 5, параграф 1, буква в).

299 Общ регламент относно защитата на данните, член 5, параграф 1, буква г); модернизирана Конвенция № 108, член 5, параграф 4, буква г).

300 Съд на ЕС, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 7 май 2009 г.

данни. Съдът е постановил, че това „право на зачитане на личния живот предполага съответното физическо лице да може да се убеди, че личните му данни се обработват по точен и законосъобразен начин, т.е. в частност че основните данни, които се отнасят до него, са точни и че са адресирани до оправомощени за това получатели“. Съдът на ЕС след това се позовава на преамбюла на Директивата за защита на личните данни, където се посочва, че субектите на данни трябва да може да упражняват правото си на достъп до личните си данни, за да могат да проверят тяхната точност[301].

Също така може да има случаи, при които актуализирането на съхранените данни е забранено от закона, тъй като целта на съхраняването на данните принципно се състои в документирането на събития като историческа „моментна снимка“.

Пример: Медицинските документи за операция не трябва да бъдат променяни, с други думи, „актуализирани“, дори ако по-късно се окаже, че посочените в тях констатации са били погрешни. При такива обстоятелства може да бъдат направени само допълнения към бележките в документите, стига да са ясно отбелязани като допълнения, направени на по-късен етап.

От друга страна, има ситуации, при които редовните проверки на точността на данните, включително актуализирането, са абсолютно необходими поради потенциалната вреда, която може да бъде нанесена на субекта на данни, ако данните останат неточни.

Пример: Ако някой иска да сключи договор за кредит с банкова институция, банката обикновено проверява кредитоспособността на бъдещия клиент. За тази цел са на разположение специални бази данни, съдържащи данни за кредитната история на частни лица. Ако такава база данни предоставя неточни или неактуални данни за дадено лице, за това лице може да има отрицателни последици. Следователно администраторите на такива бази данни трябва да положат специални усилия за спазване на принципа на точност на данните.

301 Предишно съображение 41, преамбюл към Директива 95/46/ЕО.

3.5 Принципът на ограничение на съхранението

Ключови въпроси

- Принципът на ограничение на съхранението означава, че личните данни трябва да бъдат изтрити или анонимизирани в момента, в който те вече не са необходими за целите, за които са били събрани.

Член 5, параграф 1, буква д) от ОРЗД, а също така член 5, параграф 4, буква д) от модернизираната Конвенция № 108 изискват личните данни да бъдат „съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни“. Следователно данните трябва да бъдат изтрити или анонимизирани, когато тези цели бъдат изпълнени. За тази цел „администраторът следва да установи срокове за тяхното изтриване или периодичен преглед“, за да се гарантира, че срокът на съхранение на данните не е по-дълъг от необходимия[302].

В делото *S. и Marper* ЕСПЧ заключава, че основните принципи на съответните инструменти на Съвета на Европа и законодателството и практиката на другите договарящи се страни изискват запазването на данни да бъде пропорционално по отношение на целта, за която данните са събрани, и да бъде ограничено във времето, особено в сектора на полицията[303].

Пример: В делото *S. и Marper*[304] ЕСПЧ постановява, че запазването за неограничен период от време на пръстови отпечатъци, образци от клетки и ДНК профили на двамата жалбоподатели е било непропорционално и ненужно в едно демократично общество, като

302 Общ регламент относно защитата на данните, съображение 39.

303 ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г.; вж. също например: ЕСПЧ, *M.M./Обединеното кралство*, № 24029/07, 13 ноември 2012 г.

304 ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г.

се има предвид, че наказателните производства и срещу двамата жалбоподатели са били прекратени съответно чрез оправдаване и чрез преустановяване.

Времевото ограничение за съхраняването на лични данни е приложимо само за данни, съхранявани във форма, която позволява идентифицирането на субектите на данни. Следователно законосъобразното съхраняване на данни, които вече не са необходими, би могло да бъде постигнато чрез анонимизиране на данните.

Архивирани данни в обществен интерес, за научни или исторически цели или за статистически цели може да бъдат съхранявани за по-дълги периоди, при условие че тези данни ще бъдат използвани единствено за тези цели[305]. За текущото съхраняване и използване на лични данни трябва да се прилагат подходящи технически и организационни мерки, за да се гарантират правата и свободите на субекта на данни.

В модернизираната Конвенция № 108 се допускат и изключения от принципа на ограничение на съхранението, при условие че те са предвидени в закон, зачитат същността на основните права и свободи и са необходими и пропорционални за преследването на ограничен брой легитимни цели[306]. Те включват, наред с другото, защита на националната сигурност, разследване и наказателно преследване на престъпления, изпълнение на наложените наказания, защита на субекта на данни и защита на правата и основните свободи на другите.

Пример: В делото *Digital Rights Ireland*[307] Съдът на ЕС разглежда валидността на Директивата за запазване на лични данни, чиято цел е да хармонизира разпоредбите на националното право относно запазването на лични данни, създадени или обработени от общественодостъпни електронни съобщителни услуги или мрежи

305 Общ регламент относно защитата на данните, член 5, параграф 1, буква д); модернизирана Конвенция № 108, член 5, параграф 4, буква б) и член 11, параграф 2.

306 Модернизирана Конвенция № 108, член 11, параграф 1; Обяснителен доклад към модернизираната Конвенция № 108, параграфи 91–98.

307 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

с цел борба с тежки престъпления, като организирана престъпност и тероризъм. Директивата за запазване на лични данни изисква запазването на данните за период „не по-кратък от шест месеца, без да се прави каквато и да било разлика между категориите данни, изброени в член 5 от тази директива, в зависимост от евентуалната им полза с оглед на преследваната цел или според засегнатите лица“[308]. Съдът на ЕС също така повдига въпроса за липсата на обективни критерии в Директивата за запазване на лични данни, въз основа на които да се определи точният период на запазване на данните — който би могъл да варира от минимум шест месеца до максимум две години — за да се гарантира, че е ограничен до строго необходимото[309].

3.6 Принципът на сигурност на данните

Ключови въпроси

- Сигурността и поверителността на личните данни са от ключово значение за предотвратяването на неблагоприятни последици за субекта на данни.
- Мерките за сигурност могат да бъдат от техническо и/или организационно естество.
- Псевдонимизацията е процес, чрез който личните данни могат да бъдат защитени.
- Целесъобразността на мерките за сигурност трябва да се определя за всеки отделен случай и да се преразглежда редовно.

Принципът на сигурност на данните изисква да се прилагат подходящи технически или организационни мерки при обработването на лични данни, така че данните да бъдат защитени от случаен, неразрешен или незаконен достъп, използване, промяна, разкриване, загуба, унищожаване или повреждане[310]. В ОРЗД се посочва, че при прилагането на тези мерки от администратора и обработващия лични данни следва да се вземат предвид „достиженията

308 *Пак там,* параграф 63.

309 *Пак там*, параграф 64.

310 Общ регламент относно защитата на данните, съображение 39 и член 5, параграф 1, буква е); модернизирана Конвенция № 108, член 7.

на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и [...] рисковете с различна вероятност и тежест за правата и свободите на физическите лица“[311]. В зависимост от специфичните обстоятелства на всеки отделен случай подходящите технически и организационни мерки може да включват например псевдонимизация и криптиране на личните данни и/или редовно изпитване и оценка на ефективността на мерките, за да се гарантира сигурността на обработването на данни[312].

Както е обяснено в раздел 2.1.1, псевдонимизацията на данни означава идентификаторите в личните данни, които правят възможно установяването на самоличността на субекта на данни, да бъдат заменени с псевдоним и тези идентификатори да се съхраняват отделно, като се прилагат технически и организационни мерки. Процесът на псевдонимизация не трябва да се бърка с процеса на анонимизация, при който са прекъснати всички връзки, водещи към установяване на самоличността на лицето.

Пример: Изречението „Чарлс Спенсър, роден на 3 април 1967 г., е баща в семейство с четири деца, две момчета и две момичета“ може например да бъде представено под следния псевдоним:

„Ч.С. 1967 г., е баща в семейство с четири деца, две момчета и две момичета“; или

„324 е баща в семейство с четири деца, две момчета и две момичета“; или

„YESz320l е баща в семейство с четири деца, две момчета и две момичета“.

Потребители, които имат достъп до псевдонимизираните данни, обикновено не могат да идентифицират „Чарлс Спенсър, роден на 3 април 1967 г.“ чрез „324“ или „YESz3201“. Следователно тези данни е по-вероятно да бъдат защитени от злоупотреба.

311 Общ регламент относно защитата на данните, член 32, параграф 1.

312 *Пак там*.

Първият пример обаче е по-малко сигурен. Ако изречението „Ч.С. 1967 г. е баща в семейство с четири деца, две момчета и две момичета" се използва в едно малко село, където живее Чарлс Спенсър, г-н Спенсър може лесно да бъде разпознат. Методът на псевдонимизация може да окаже влияние върху ефективността на защитата на данни.

Личните данни с криптирани или съхранявани отделно идентификатори в много случаи се използват като средство за запазване на самоличността на лицата в тайна. Това е особено полезно в случаите, когато администраторите на данни трябва да гарантират, че работят със същите субекти на данни, но не изискват или не се нуждаят от истинската им самоличност. Такъв е случаят например, когато изследовател разучава хода на болестта при пациенти, чиято самоличност е известна само на болницата, в която са лекувани и от която изследователят получава епикризите на медицинските случаи с псевдонимизирани данни. Следователно псевдонимизацията е солиден инструмент в арсенала на технологиите за подобряване на неприкосновеността на личния живот. Тя може да функционира като важен елемент при осъществяване на защита на данните още при проектирането. Това означава включване на защитата на данните в системите за обработване на данни.

В член 25 от ОРЗД, който се отнася до защитата на данните на етапа на проектирането, псевдонимизацията изрично се споменава като пример за подходяща техническа и организационна мярка, която администраторите следва да въведат, за да спазят принципите на защита на данните и да включат необходимите гаранции. По този начин администраторите ще изпълнят изискванията на регламента и ще защитят правата на субектите на данни при обработването на личните им данни.

Спазването на одобрен кодекс за поведение или одобрен механизъм за сертифициране може да помогне за доказване на спазването на изискването за сигурност на обработването[313]. В становището си относно последиците за защитата на данните от обработването на резервационните данни на пътниците Съветът на Европа дава още примери за подходящи мерки за сигурност във връзка със защитата на личните данни в системите за резервационни данни на пътниците. Те включват съхраняване на данните

313 *Пак там,* член 32, параграф 3.

в защитена физическа среда, ограничаване на достъпа чрез контрол на достъпа на няколко нива и защита на съобщаването на данни чрез засилена криптография[314].

Пример: Сайтове на социални мрежи и доставчици на електронна поща дават възможност на потребителите да добавят допълнително ниво на сигурност на данните към доставяните от тях услуги чрез въвеждане на двустепенна автентификация. Освен въвеждането на лична парола, потребителите трябва да попълнят втора регистрация, за да влязат в личния си профил. Тази втора регистрация може да бъде например въвеждането на код за сигурност, който се изпраща на мобилен номер, свързан с личния профил. По този начин проверката на два етапа осигурява по-добра защита на личната информация срещу непозволен достъп до личните профили чрез компютърно пиратство.

В Обяснителния доклад към модернизираната Конвенция № 108 са приведени допълнителни примери за подходящи гаранции, като например въвеждане на задължение за професионална тайна или приемане на квалифицирани технически мерки за сигурност, като криптиране на данните[315]. Когато въвежда специални мерки за сигурност, администраторът — или, когато е приложимо, обработващият лични данни — следва да вземе предвид няколко елемента, като например естеството и обема на обработваните лични данни, потенциалните неблагоприятни последици за субектите на данни и необходимостта от ограничен достъп до данните[316]. При прилагането на подходящи мерки за сигурност трябва да се вземат предвид текущите достижения на техническия прогрес в областта на методите за сигурност на данните и техниките за обработване на данни. Разходите по прилагането на тези мерки трябва да бъдат пропорционални на тежестта и вероятността на възможните рискове. Необходим е редовен преглед на мерките за сигурност, така че те да могат да бъдат актуализирани при необходимост[317].

314 Съвет на Европа, Комитет на Конвенция № 108, *Становище относно последиците за защитата на данните от обработването на резервационните данни на пътниците*, T-PD(2016)18rev, 19 август 2016 г., стр. 9.

315 Обяснителен доклад към модернизираната Конвенция № 108, параграф 56.

316 *Пак там*, параграф 62.

317 *Пак там,* параграф 63.

В случаите, когато се извършва нарушение на сигурността на личните данни, както модернизираната Конвенция № 108, така и ОРЗД изискват администраторът да уведоми без ненужно забавяне компетентния надзорен орган за нарушението и рисковете за правата и свободите на физическите лица[318]. Подобно задължение за уведомяване на субекта на данни съществува и когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за неговите права и свободи[319]. Уведомяването на субектите на данни за такива нарушения трябва да бъде на ясен и разбираем език[320]. Ако обработващият лични данни узнае за нарушаване на сигурността на лични данни, администраторът трябва да бъде уведомен незабавно[321]. В определени ситуации може да има изключения от задължението за уведомяване. Например не се изисква администраторът да уведомява надзорния орган, когато „не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица“[322]. Субектът на данни не е необходимо да се уведомява и когато предприетите мерки за сигурност правят данните неразбираеми за лицата, които нямат разрешение за достъп до тях, или когато взетите впоследствие мерки гарантират, че високият риск вече няма вероятност да се материализира[323]. Ако уведомяването на субектите на данни за нарушение на сигурността на личните данни изисква несъразмерно големи усилия от страна на администратора, публично съобщение или друга подобна мярка могат да гарантират „субектите на данни да бъдат в еднаква степен ефективно информирани“[324].

318 Модернизирана Конвенция № 108, член 7, параграф 2; Общ регламент относно защитата на данните, член 33, параграф 1.

319 Модернизирана Конвенция № 108, член 7, параграф 2; Общ регламент относно защитата на данните, член 34, параграф 1.

320 Общ регламент относно защитата на данните, член 34, параграф 2.

321 *Пак там*, член 33, параграф 1.

322 *Пак там*.

323 *Пак там*, член 34, параграф 3, букви а) и б).

324 *Пак там*, член 34, параграф 3, буква в).

3.7 Принципът на отчетност

Ключови въпроси

- Отчетността изисква администраторите и обработващите лични данни активно и постоянно да прилагат мерки за насърчаване и гарантиране на защитата на данните в своите дейности по обработване.
- Администраторите и обработващите лични данни носят отговорност за съответствието на своите операции по обработване с правото за защитата на данните и своите съответни задължения.
- Администраторите трябва да бъдат в състояние по всяко време да докажат пред субектите на данни, обществеността и надзорните органи, че спазват разпоредбите за защита на данните. Обработващите лични данни също трябва да спазват някои задължения, които са тясно свързани с отчетността (като например водене на регистър на извършваните операции по обработване и назначаване на длъжностно лице по защита на данните).

В ОРЗД и модернизираната Конвенция № 108 се посочва, че администраторът носи отговорност и трябва да е в състояние да докаже спазването на принципите на обработване на лични данни, описани в настоящата глава[325]. За тази цел администраторът трябва да въведе подходящи технически и организационни мерки[326]. Макар че принципът на отчетност, посочен в член 5, параграф 2 от ОРЗД, е насочен само към администраторите, от обработващите лични данни също се очаква да подлежат на отчетност, като се има предвид, че те трябва да спазват редица задължения и че тези задължения са тясно свързани с отчетността.

В правото на ЕС и на Съвета на Европа в областта на защитата на данните също така е определено, че администраторът носи отговорност и следва да може да гарантира спазването на принципите на защита на данните, разгледани в раздели 3.1–3.6[327]. Работната група по член 29 посочва, че „видът на процедурите и механизмите ще варира в зависимост от рисковете, свързани с обработването и с естеството на данните“[328].

325 *Пак там*, член 5, параграф 2; модернизирана Конвенция № 108, член 10, параграф 1.

326 Общ регламент относно защитата на данните, член 24.

327 *Пак там*, член 5, параграф 2; модернизирана Конвенция № 108, член 10, параграф 1.

328 Работна група по член 29, *Становище 3/2010 относно принципа на отчетността*, WP 173, Брюксел, 13 юли 2010 г., параграф 12.

Администраторите могат да улеснят спазването на това изискване по различни начини, които включват:

- поддържане на регистър на дейностите по обработване и предоставянето им на надзорния орган при поискване[329];
- в някои случаи определяне на длъжностно лице по защита на данните, което да участва във всички въпроси, свързани със защитата на личните данни[330];
- извършване на оценки на въздействието върху защитата на личните данни за онези видове обработване, които има вероятност да доведат до висок риск по отношение на правата и свободите на физическите лица[331];
- гарантиране на защита на данните на етапа на проектирането и по подразбиране[332];
- въвеждане на условия и процедури за упражняването на правата на субектите на данни[333];
- придържане към одобрени кодекси за поведение или механизми за сертифициране[334].

Макар и принципът на отчетност в член 5, параграф 2 от ОРЗД да не е специално насочен към обработващите лични данни, има разпоредби, свързани с отчетността, които съдържат задължения и за тях, като например воденето на регистър на извършваните дейности по обработване и назначаването на длъжностно лице по защита на данните за всяка дейност по обработването, която изисква това[335]. Обработващите лични данни също трябва да гарантират, че са въведени всички необходими мерки за осигуряване на сигурността

329 Общ регламент относно защитата на данните, член 30.

330 *Пак там*, членове 37–39.

331 *Пак там*, член 35; модернизирана Конвенция № 108, член 10, параграф 2.

332 Общ регламент относно защитата на данните, член 25. Модернизирана Конвенция № 108, член 10, параграф 2 и 3.

333 *Пак там*, член 12 и член 24.

334 *Пак там*, член 40 и член 42.

335 *Пак там*, член 5, параграф 2, член 30 и член 37.

на данните[336]. В правно обвързващия договор между администратора и обработващия лични данни трябва да бъде определено, че обработващият лични данни подпомага администратора по отношение на някои от изискванията за спазване на задълженията, като например извършването на оценка на въздействието върху защитата на данните или уведомяването на администратора за всяко нарушение на сигурността на личните данни веднага щом узнае за него[337].

През 2013 г., Организацията за икономическо сътрудничество и развитие (ОИСР) прие Насоки относно защитата на неприкосновеността на личния живот, в които подчертава, че администраторите играят важна роля за практическото приложение на защитата на данните. В насоките се съдържа принципът на отчетност, съгласно който „администраторът на данни следва да бъде отговорен за спазване на мерките, които пораждат действие по отношение на [материалните] принципи, посочени по-горе"[338].

Пример: Законодателен пример, подчертаващ принципа за отчетност, е изменението от 2009 г.[339] на Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации. В член 4, в своя изменен вид, директивата налага задължение да се гарантира „осъществяването на политика на сигурност по отношение на обработката на лични данни". По такъв начин, що се отнася до предвидените в тази директива разпоредби за сигурност, законодателят е решил, че е необходимо да се въведе изрично изискване за наличието и осъществяването на политика на сигурност.

336 *Пак там*, член 28, параграф 3, буква в).

337 *Пак там*, член 28, параграф 3, буква г).

338 ОИСР (2013 г.), Насоки, уреждащи защитата на неприкосновеността на личния живот и трансграничните потоци от лични данни, член 14.

339 Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г., стр. 11.

Съгласно становището на Работната група по член 29[340] същността на отчетността се състои в задължението на администратора да:

- въведе мерки, които при нормални обстоятелства ще гарантират, че правилата за защита на данните се спазват при извършване на операции по обработване; и

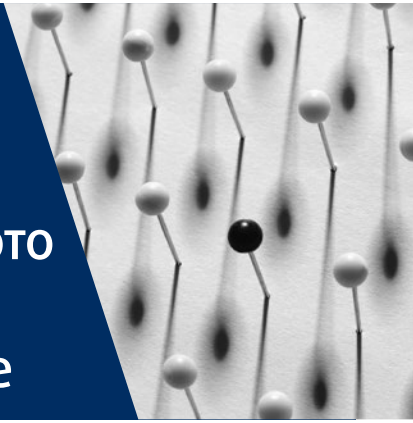
- разполага с готова документация, която доказва на субектите на данни и на надзорните органи мерките, които са взети за спазване на правилата за защита на данните.

По този начин принципът на отчетност изисква от администраторите да докажат активното спазване на правилата, а не просто да чакат субектите на данни или надзорните органи да посочват недостатъци.

340 Работна група по член 29, *Становище 3/2010 относно принципа на отчетността*, WP 173, Брюксел, 13 юли 2010 г.

4

Правила на европейското право в областта на защитата на данните



ЕС	Обхванати въпроси	СЕ
Правила за законосъобразно обработване на данните		
Общ регламент относно защитата на данните, член 6, параграф 1, буква а) Съд на ЕС, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 2011 г. Съд на ЕС, C-536/15, *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*, 2017 г.	**Съгласие**	Препоръка относно профилирането, член 3.4, буква б) и член 3.6 Модернизирана Конвенция № 108, член 5, параграф 2
Общ регламент относно защитата на данните, член 6, параграф 1, буква б)	**(Предварителни) договорни взаимоотношения**	Препоръка относно профилирането, член 3.4, буква б)
Общ регламент относно защитата на данните, член 6, параграф 1, буква в)	**Правни задължения на администратора**	Препоръка относно профилирането, член 3.4, буква а)
Общ регламент относно защитата на данните, член 6, параграф 1, буква г)	**Жизненоважни интереси на субекта на данни**	Препоръка относно профилирането, член 3.4, буква б)
Общ регламент относно защитата на данните, член 6, параграф 1, буква д) Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 2008 г.	**Обществен интерес и упражняване на официални правомощия**	Препоръка относно профилирането, член 3.4, буква б)

ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните, член 6, параграф 1, буква е) Съд на ЕС, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 г. Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 2011 г.	**Законни интереси на други лица**	Препоръка относно профилирането, член 3.4, буква б) ЕСПЧ, *Y/Турция*, № 648/10, 2015 г.
Общ регламент относно защитата на данните, член 6, параграф 4	**Изключение от принципа на ограничение на целите: по-нататъшно обработване за други цели**	Модернизирана Конвенция № 108, член 5, параграф 4, буква б)
Правила за законосъобразно обработване на чувствителни данни		
Общ регламент относно защитата на данните, член 9, параграф 1	**Обща забрана за обработване**	Модернизирана Конвенция № 108, член 6
Общ регламент относно защитата на данните, член 9, параграф 2	**Изключения от общата забрана**	Модернизирана Конвенция № 108, член 6
Правила за сигурно обработване		
Общ регламент относно защитата на данните, член 32	**Задължение да се гарантира сигурно обработване**	Модернизирана Конвенция № 108, член 7, параграф 1 ЕСПЧ, *I/Финландия*, № 20511/03, 2008 г.
Общ регламент относно защитата на данните, член 28 и член 32, параграф 1, буква б)	**Задължение за поверителност**	Модернизирана Конвенция № 108, член 7, параграф 1
Общ регламент относно защитата на данните, член 34 Директива за правото на неприкосновеност на личния живот и електронни комуникации, член 4, параграф 2	**Уведомления за нарушения на сигурността на данните**	Модернизирана Конвенция № 108, член 7, параграф 2

ЕС	Обхванати въпроси	СЕ
Правила за отчетност и насърчаване на спазването		
Общ регламент относно защитата на данните, членове 12, 13 и 14	**Прозрачността като общо понятие**	Модернизирана Конвенция № 108, член 8
Общ регламент относно защитата на данните, членове 37, 38 и 39	**Длъжностни лица по защита на данните**	Модернизирана Конвенция № 108, член 10, параграф 1
Общ регламент относно защитата на данните, член 30	**Регистри на дейностите по обработване**	
Общ регламент относно защитата на данните, членове 35 и 36	**Оценка на въздействието и предварителни консултации**	Модернизирана Конвенция № 108, член 10, параграф 2
Общ регламент относно защитата на данните, членове 33 и 34	**Уведомления за нарушения на сигурността на данните**	Модернизирана Конвенция № 108, член 7, параграф 2
Общ регламент относно защитата на данните, членове 40 и 41	**Кодекси за поведение**	
Общ регламент относно защитата на данните, членове 42 и 43	**Сертифициране**	
Защита на данните на етапа на проектирането и по подразбиране		
Общ регламент относно защитата на данните, член 25, параграф 1	**Защита на данните на етапа на проектирането**	Модернизирана Конвенция № 108, член 10, параграф 2
Общ регламент относно защитата на данните, член 25, параграф 2	**Защита на данните по подразбиране**	Модернизирана Конвенция № 108, член 10, параграф 3

Необходимо е принципите да са с общ характер. Тяхното прилагане в конкретни ситуации оставя известна свобода за тълкуване и избор на средства. Правото на **Съвета на Европа** оставя на страните по модернизираната Конвенция № 108 да пояснят тази свобода за тълкуване в националното си законодателство. Положението в **правото на ЕС** е различно: по отношение на установяването на защита на данните във вътрешния пазар беше счетено, че е необходимо да има по-подробни правила на равнище ЕС, за да се хармонизира нивото на защита на данните в националните законодателства на държавите членки. Общият регламент относно защитата на данните определя набор от подробни правила съгласно принципите, посочени в член 5 от него, които са пряко приложими в националния правен ред. Поради тази причина следващите коментари относно подробните правила за защита на данните на европейско равнище се отнасят предимно до правото на ЕС.

4.1 Правила за законосъобразно обработване

Ключови въпроси

- Лични данни могат да бъдат законосъобразно обработвани, ако е изпълнен един от следните критерии:
  - обработването се основава на съгласието на субекта на данни;
  - определени договорни взаимоотношения изискват обработването на лични данни;
  - обработването е необходимо за спазването на правно задължение на администратора;
  - жизненоважни интереси на субектите на данни или на друго лице изискват обработването на техните данни;
  - обработването е необходимо за изпълнението на задача от обществен интерес;
  - законни интереси на администраторите или на трети страни са основанието за обработването, но само ако спрямо тях нямат преимущество интересите или основните права на субектите на данни.
- Законосъобразното обработване на чувствителни лични данни подлежи на специален, по-строг режим.

4.1.1 Законосъобразни основания за обработване на данни

В глава II от Общия регламент относно защитата на данните, озаглавена „Принципи", се предвижда, че всякакво обработване на лични данни трябва да отговаря на първо място на принципите, отнасящи се до качеството на данните, посочени в член 5 от ОРЗД. Един от принципите е, че личните данни следва да бъдат „обработвани законосъобразно, добросъвестно и по прозрачен начин". На второ място, за да бъдат данните обработвани законосъобразно, обработването трябва да отговаря на някое от законосъобразните

основания, които го правят легитимно и са изброени в член 6[341] относно нечувствителните лични данни и в член 9 относно специалните категории данни (или чувствителните данни). По подобен начин глава II от модернизираната Конвенция № 108, в която се регламентират „основните принципи за защита на личните данни", предвижда, че за да бъде законосъобразно, обработването на данни следва да бъде „пропорционално по отношение на преследваната легитимна цел".

Независимо от законосъобразното основание за обработване, на което се опира администраторът, за да започне операция по обработване на лични данни, той трябва да приложи и гаранциите, които са предвидени в общия режим на законодателството за защита на данните.

Съгласие

В правото на Съвета на Европа съгласието е споменато в член 5, параграф 2 от модернизираната Конвенция № 108. То се споменава също така в съдебната практика на ЕСПЧ и в няколко препоръки на Съвета на Европа[342]. **Съгласно правото на ЕС** съгласието като основание за законосъобразно обработване на данни е твърдо установено в член 6 от ОРЗД и също така изрично е посочено в член 8 от Хартата. Характеристиките на валидното съгласие са обяснени в определението за съгласие в член 4, като условията за получаване на валидно съгласие са изброени в член 7, а специалните правила за съгласието на децата по отношение на услугите на информационното общество са установени в член 8 от ОРЗД.

Както е пояснено в раздел 2.4, съгласието трябва да е свободно изразено, информирано, конкретно и недвусмислено. Съгласието трябва да бъде изявление или ясно потвърждаващо действие, което изразява съгласие за обработване, като лицето има правото да оттегли съгласието си по всяко време.

---

341 Съд на ЕС, съединени дела C-465/00, C-138/01 и C-139/01, *Rechnungshof/Österreichischer Rundfunk и други и Christa Neukomm и Jospeh Lauermann/Österreichischer Rundfunk*, 20 май 2003 г., параграф 65; Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г., параграф 48; Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г., параграф 26.

342 Вж. например Съвет на Европа, Комитет на министрите (2010 г.), Препоръка CM/Rec(2010)13 на Комитета на министрите до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране, 23 ноември 2010 г., член 3, параграф 4, буква б).

Администраторите са длъжни да водят документация за получените съгласия, в която може да се извършват проверки.

Свободно изразено съгласие

Съгласно рамката на **Съвета на Европа**, тоест модернизираната Конвенция № 108, съгласието на субекта на данни трябва да „представлява свободно изразяване на съзнателен избор“[343]. Наличието на свободно изразено съгласие е валидно само „ако субектът на данни е в състояние да направи действителен избор и не съществува риск от измама, заплашване, принуда или съществени отрицателни последствия, ако той/тя не изрази съгласие“[344]. В това отношение **правото на ЕС** предвижда, че съгласието не следва да се разглежда като свободно дадено, „ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него“[345]. В ОРЗД се подчертава, че „когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали, *inter alia*, изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор“[346]. В Обяснителния доклад към модернизираната Конвенция № 108 се посочва, че „върху субекта на данни не може да бъде упражнявано пряко или непряко неправомерно влияние или натиск (от икономически или друг характер) и съгласието не следва да се счита за свободно изразено, ако субектът на данни няма истински избор или не е в състояние да откаже или да оттегли съгласието си, без това да му нанесе вреда“[347].

Пример: Някои общини в държава „А“ са решили да въведат карти за пребиваване с вграден чип. За местните жители не е задължително да придобиват тези електронни карти. Жителите, които не притежават такава карта, обаче нямат достъп до редица важни административни услуги, като например възможността да плащат онлайн общинските данъци, да подават жалби по електронен път, като се възползват от

343 Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

344 Вж. също Работна група по член 29 (2011 г.), *Становище 15/2011 относно понятието „съгласие“*, WP 187, Брюксел, 13 юли 2011 г., стр. 12.

345 Общ регламент относно защитата на данните, съображение 42.

346 *Пак там*, член 7, параграф 4.

347 Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

тридневния срок за получаване на отговор от органите, и дори да не чакат на опашка, да купуват с отстъпка билети за общинската концертна зала и да използват скенерите на входа.

В този случай не може да се каже, че обработването на личните данни от общината се основава на съгласие. Съгласието не е дадено свободно, тъй като най-малкото е налице непряк натиск върху жителите да придобият електронната карта и да се съгласят с обработването. Следователно въвеждането на система с електронни карти от страна на общините следва да е на друго легитимно основание, което да обосновава обработването. Например те биха могли да посочат, че обработването е необходимо за изпълнението на задача от обществен интерес, което е законно основание за обработване съгласно член 6, параграф 1, буква д) от ОРЗД[348].

Свободно изразеното съгласие би могло да бъде поставено под съмнение също така в положение на подчиненост, когато е налице значителна икономическа или друг вид неравнопоставеност между администратора, който осигурява съгласието, и субекта на данни, който дава съгласието[349]. Типичен пример за такъв дисбаланс и положение на подчиненост е обработването на лични данни от страна на работодател в контекста на трудово правоотношение. Според Работната група по член 29 „служителите почти никога не са в положение свободно да дават, отказват или оттеглят съгласието си, като се има предвид тяхната зависимост, която произтича от взаимоотношенията работодател — служител. Като се има предвид неравнопоставеността на страните, служителите могат да дадат свободно съгласие само при изключителни обстоятелства, когато няма да има никакви последици от това дали ще приемат дадено предложение, или ще го откажат“[350].

348 Работна група по член 29 (2011 г.), *Становище 15/2011 относно понятието „съгласие“*, WP 187, Брюксел, 13 юли 2011 г., стр. 16. Други примери за случаи, в които не може да се каже, че обработването се основава на съгласие, и е необходимо друго правно основание, за да бъде то законосъобразно, са посочени на стр. 14 и 17 на становището.

349 Вж. също Работна група по член 29 (2001 г.), *Становище 8/2001 относно обработването на личните данни в контекста на трудовите правоотношения*, WP 48, Брюксел, 13 септември 2001 г.; Работна група по член 29 (2005 г.), Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г., WP 114, Брюксел, 25 ноември 2005 г.; Работна група по член 29 (2017 г.), *Становище 2/2017 относно обработването на данни на работното място*, WP 249, Брюксел, 8 юни 2017 г.

350 Работна група по член 29 (2017 г.), *Становище 2/2017 относно обработването на данни на работното място*, WP 249, Брюксел, 8 юни 2017 г.

Пример: Голямо дружество планира да създаде указател, съдържащ имената на всички служители, длъжността, която те заемат в дружеството, и служебните им адреси единствено с цел подобряване на комуникацията в рамките на дружеството. Ръководителят на отдел „Човешки ресурси“ предлага в указателя да бъде добавена снимка на всеки служител с цел да се улесни разпознаването на колеги на срещи. Представители на служителите искат това да бъде направено само ако отделният служител даде съгласието си за подобно нещо.

В тази ситуация съгласието на служител следва да бъде счетено за правно основание за обработване на снимките в указателя, защото е възможно това да няма никакви последствия за служителя, независимо дали той ще се съгласи негова снимка да бъде публикувана в указателя.

Пример: Дружество „А“ планира среща между трима свои служители и директорите на дружество „Б“, за да обсъдят възможно бъдещо сътрудничество по проект. Срещата ще се проведе в помещенията на дружество „Б“, което иска от дружество „А“ да му изпрати по електронната поща имената, автобиографиите и снимките на участниците в срещата. Дружество „Б“ изтъква, че се нуждае от имената и снимките на участниците, за да могат служителите от охраната на входа на сградата да проверят дали това са правилните лица, а автобиографиите ще дадат възможност на директорите да се подготвят по-добре за срещата. В този случай не може да се каже, че предаването от страна на дружество „А“ на личните данни на неговите служители се основава на съгласие. Съгласието не може да се счита за „свободно дадено“, тъй като е възможно да има отрицателни последствия за служителите, ако откажат предложението (например те биха могли да бъдат заместени от други техни колеги не само по време на срещата, но и във взаимоотношенията с дружество „Б“ и в участието им в проекта като цяло). Следователно обработването трябва да е на друго законово основание.

Това обаче не означава, че съгласието никога не може да бъде валидно при обстоятелства, при които отказът да се даде съгласие би имал отрицателни последствия. Ако например не бъде дадено съгласие за издаване на клиентска карта за супермаркет, това води само до неполучаване на малки отстъпки

от цените на определени стоки, съгласието може да бъде валидно правно основание за обработване на личните данни на онези клиенти, които са дали съгласието си за издаване на такава карта. Не е налице подчиненост между дружество и клиент, а последствията от отказа да се даде съгласие не са толкова сериозни, че да попречат на свободния избор на субекта на данни (като се има предвид, че ценовите отстъпки са достатъчно малки, за да не повлияят на техния свободен избор).

Когато обаче продукти или услуги могат да бъдат получени само ако се разкрият известни лични данни на администратора или след това на трети страни, съгласието на субекта на данните да ги разкрие, което не е необходимо за договора, не може да се счита за свободно решение и следователно не е валидно съгласно правото за защита на данните[351]. В Общия регламент относно защитата на данните изключително строго се забранява обвързването на съгласието с предоставянето на стоки и услуги[352].

Пример: Съгласие, дадено от пътниците на авиокомпания, която предава така наречените резервационни данни на пътниците (т.е. данни относно тяхната самоличност, хранителни навици или здравословни проблеми), към имиграционните органи на конкретна чужда държава не може да бъде счетено за валидно съгласие съгласно правото за защита на данните, тъй като пътуващите лица нямат никакъв избор, ако желаят да посетят тази държава. За да бъде предаването на тези данни законосъобразно, се изисква друго правно основание, различно от съгласие: най-вероятно специален закон.

Информирано съгласие

Субектът на данни трябва да разполага с достатъчно информация, преди да упражни своя избор. Обикновено информираното съгласие включва точно и лесно разбираемо описание на въпроса, по отношение на който се изисква съгласие. Съгласно обяснението на Работната група по член 29 съгласието трябва да се основава на оценяване и разбиране на фактите и последствията, които настъпват, след като субектът на данни даде съгласие за обработването. Следователно „на заинтересованото лице трябва да бъде дадена по

351 Общ регламент относно защитата на данните, член 7, параграф 4.

352 *Пак там*.

ясен и разбираем начин точна и пълна информация по всички въпроси, които са от значение [...], като например естеството на обработваните данни, целите на обработването, възможните получатели и правата на субекта на данните“[353]. За да бъде съгласието информирано, лицата трябва също така да са запознати с последствията, ако не се съгласят с обработването.

Предвид важността на информираното съгласие, в ОРЗД и Обяснителния доклад към модернизираната Конвенция № 108 са положени усилия да се поясни това понятие. В съображенията на ОРЗД се предвижда, че информираното съгласие означава, че „субектът на данни следва да знае поне самоличността на администратора и целите на обработването, за които са предназначени“ обработваните лични данни[354].

В изключителния случай, когато съгласието се използва като дерогация, за да се осигури законово основание за международно предаване на данни, администраторът трябва да информира субекта на данни за свързаните с предаването възможни рискове поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции, за да може това съгласие да се счита за валидно[355].

В Обяснителния доклад към модернизираната Конвенция № 108 се посочва, че трябва да бъде предоставена информация за последствията от решението на субекта на данните, а именно „с какво е свързан фактът на даването на съгласие и в каква степен е дадено то“[356].

Качеството на информацията е от голямо значение. Качество на информацията означава, че тя следва да бъде адаптирана спрямо лицата, които се предвижда да я получат. Информацията трябва да се предоставя, без да се използва жаргон, на ясен и разбираем език, така че да може да бъде разбрана от обичайния потребител[357]. Информацията трябва също така да бъде леснодостъпна за субекта на данни и може да бъде предоставена устно или в писмен вид. Важни характеристики са достъпността и видимостта на

353 Работна група по член 29 (2007 г.), Работен документ относно обработването на лични здравни данни в електронните здравни досиета (ЕЗД), WP 131, Брюксел, 15 февруари 2007 г.

354 Общ регламент относно защитата на данните, съображение 42.

355 *Пак там*, член 49, параграф 1, буква а).

356 Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

357 Работна група по член 29 (2011 г.), *Становище 15/2011 относно понятието „съгласие“*, WP 187, Брюксел, 13 юли 2011 г., стр. 19.

информацията: тя трябва да бъде ясно видима и различима. В онлайн среда многопластовите информационни съобщения може да бъдат добро решение, тъй като дават възможност на субектите на данни да избират дали да прочетат кратка или по-подробна версия на информацията.

Конкретно съгласие

За да бъде съгласието валидно, то трябва също така да бъде конкретно за целта на обработването, която трябва да бъде описана ясно и с недвусмислени изрази. Това върви ръка за ръка с качеството на предоставяната информация относно целта на съгласието. В тази връзка са важни основателните очаквания на един средностатистически субект на данни. От субекта на данни може да бъде поискано още веднъж да даде съгласието си, ако предстои добавяне на операции по обработване или промяната им по начин, който не е могъл да бъде разумно предвиден при даване на първоначалното съгласие, което води до промяна на целта на обработването. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие[358].

Примери: По делото *Deutsche Telekom AG*[359] Съдът на ЕС разглежда въпроса дали доставчик на телекомуникационни услуги, който е трябвало да предаде лични данни на абонатите с цел публикуване в телефонни указатели, е имал нужда от ново съгласие от субектите на данни[360], тъй като при първоначалното даване на съгласие не са били посочени имената на получателите на услугата.

Съдът на ЕС постановява, че съгласно член 12 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации не е било необходимо ново съгласие преди предаването на данните. Тъй като субектите на данни са разполагали с възможност само да се съгласят с целта на обработването — която е публикуване на техните данни — те не са могли да избират между различните телефонни указатели, в които тези данни биха могли да бъдат публикувани.

358 Общ регламент относно защитата на данните, съображение 32.

359 Съд на ЕС, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5 май 2011 г. Вж. по-специално параграфи 53 и 54.

360 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. 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 електронни комуникации), ОВ L 201, 31.7.2002 г.

Както Съдът подчертава, „при тълкуването на член 12 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации с оглед на контекста и систематичното място на тази разпоредба се налага изводът, че съгласието по смисъла на параграф 2 от този член се отнася до целта на публикуването на личните данни в публичния указател, а не до издаването им от конкретен доставчик на указатели“[361]. В допълнение „вреди за абоната би могло да причини именно публикуването на личните данни в указател, който има особена цел“[362], а не конкретният издател.

Делото *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*[363] се отнася до молба на белгийско дружество, което предлага телефонни справочни услуги и указатели, до дружества, които предоставят телефонни номера в Нидерландия, да му дадат достъп до данните, свързани с техните абонати. Белгийското дружество се позовава на задължение, предвидено по Директивата за универсалната услуга[364]. Това задължение изисква от дружествата, които предоставят телефонни номера, да предоставят тези номера и на указателите, които ги поискат, ако абонатите са дали съгласие номерата им да бъдат публикувани. Нидерландските дружества са отказали да направят това, като са заявили, че не са длъжни да предоставят въпросните данни на предприятие, установено в друга държава членка. Те са изтъкнали, че потребителите са дали съгласието си номерата им да бъдат публикувани с разбирането, че те ще бъдат публикувани в нидерландски указател. Съдът на ЕС постановява, че Директивата за универсалната услуга обхваща всички молби от предприятия, предоставящи справочни услуги, без значение в коя държава членка са установени те. Съдът на ЕС също така постановява, че предаването на същите данни на друго предприятие, което иска да ги включи в публичен указател, без абонатът отново да е дал съгласие, не би могло да накърни самата същност на правото на защита на личните

361 Съд на ЕС, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5 май 2011 г., параграф 61.

362 *Пак там*, параграф 62.

363 Съд на ЕС, C-536/15, *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*, 15 март 2017 г.

364 Директива 2002/22/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги (Директивата за универсалната услуга), ОВ L 108, 24.4.2002 г., стр. 51, изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. (Директивата за универсалната услуга), ОВ L 337, 18.12.2009 г., стр. 11.

данни[365]. Ето защо предприятието, което предоставя телефонни номера на абонатите си, не следва да поиска съгласието на абоната, така че той да изрази това съгласие отделно в зависимост от държавата членка, към която могат да бъдат предадени засягащите го данни[366].

Недвусмислено съгласие

Всяко съгласие трябва да бъде дадено недвусмислено[367]. Това означава, че не следва да има каквото и да било основателно съмнение за това дали субектът на данни е имал желание да съобщи своето съгласие за обработване на неговите данни. Например бездействие от страна на субект на данни не указва недвусмислено съгласие.

Такъв е случаят, когато администраторите получават съгласие посредством декларации, включени в техните политики за поверителност, като например „като използвате услугата ни, вие давате съгласието си за обработване на личните ви данни". В този случай администраторите може да се наложи да гарантират, че потребителите собственоръчно и лично се съгласяват с тези политики.

Ако съгласието е дадено в писмена форма като част от договор, съгласието за обработване на личните данни трябва да бъде индивидуализирано и във всички случаи „с гаранциите следва да се обезпечи, че субектът на данни е информиран за това, че дава съгласието си, и в каква степен го дава"[368].

Изисквания за съгласието, давано от деца

ОРЗД предвижда специална защита за децата по отношение на предоставянето на услуги на информационното общество, тъй като „те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни"[369]. Следователно съгласно **правото на ЕС**, когато доставчици на услуги на информационното общество обработват лични данни на деца под 16 години въз основа на съгласие,

365 Съд на ЕС, C-536/15, *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*, 15 март 2017 г., параграф 36.

366 *Пак там*, параграфи 40—41.

367 Общ регламент относно защитата на данните, член 4, параграф 11.

368 *Пак там*, съображение 42.

369 *Пак там*, съображение 38.

това обработване е законосъобразно „само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето“[370]. Държавите членки могат да предвидят по-ниска възраст в националното си право, въпреки че тази по-ниска възраст не трябва да е под 13 години[371]. Съгласието на носещия родителска отговорност не е необходимо „в контекста на пряко предлаганите на деца услуги за превенция и консултиране“[372]. Когато обработването е насочено към дете, информацията и комуникацията следва да се предоставят с ясни и недвусмислени формулировки, които да бъдат лесноразбираеми за детето[373].

Правото на оттегляне на съгласие по всяко време

В ОРЗД е включено общо право за оттегляне на съгласие по всяко време[374]. Субектът на данни трябва да е информиран за това право, преди да даде съгласие, и може да го упражни по своя преценка. Не следва да съществува каквото и да било изискване за посочване на причини за оттеглянето, както и какъвто и да било риск от отрицателни последици, превишаващи възможните ползи, произтичащи от даденото по-рано съгласие за използване на данните. Оттеглянето на съгласие следва да бъде също толкова лесно, колкото и даването му[375]. Не може да има свободно изразено съгласие, ако субектът на данни не е в състояние да оттегли съгласието си, без това да му навреди, или ако оттеглянето на съгласието не е толкова лесно, колкото е било даването му[376].

Пример: Клиент дава съгласие за получаване на рекламно-информационни съобщения, изпращани на адрес, предоставен от този клиент на администратора на данни. Ако клиентът оттегли своето съгласие,

370 *Пак там*. член 8, параграф 1, първо тире. В член 4, параграф 25 от Общия регламент относно защитата на данните е дадено определение на понятието за услуги на информационното общество.

371 Общ регламент относно защитата на данните, член 8, параграф 1, второ тире.

372 *Пак там*, съображение 38.

373 *Пак там*, съображение 58. Вж. също модернизирана Конвенция № 108, член 15, параграф 2, буква д). Обяснителен доклад към модернизираната Конвенция № 108, параграфи 68 и 125.

374 Общ регламент относно защитата на данните, член 7, параграф 3. Обяснителен доклад към модернизираната Конвенция № 108, параграф 45.

375 Общ регламент относно защитата на данните, член 7, параграф 3.

376 Общ регламент относно защитата на данните, съображение 42; Обяснителен доклад към модернизираната Конвенция № 108, параграф 42.

администраторът трябва незабавно да спре да изпраща рекламно-информационни съобщения. Оттеглянето няма да има за своя последица каквито и да било наказания, като например плащане на такси. Оттеглянето обаче има действие за в бъдеще и няма обратно действие. Периодът, през който личните данни на клиента са били обработвани законосъобразно — поради съгласието на клиента — е легитимен. Оттеглянето предотвратява всякакво по-нататъшно обработване на тези данни, освен ако това обработване не е в съответствие с правото на изтриване на данните[377].

Обработването е необходимо за изпълнението на договор

Съгласно правото на ЕС член 6, параграф 1, буква б) от ОРЗД предвижда още едно основание за законосъобразно обработване, а именно ако обработването е „необходимо за изпълнението на договор, по който субектът на данните е страна“. Тази разпоредба обхваща и преддоговорните отношения. Например в случаите, когато една страна възнамерява да сключи договор, но все още не го е направила, вероятно защото все още трябва да бъдат приключени някои проверки. Ако едната страна трябва да обработи данни за тази цел, това обработване е законосъобразно, ако е необходимо „за предприемане на стъпки по искане на субекта на данните преди сключването на договор“[378].

Понятието за обработването на данни като „определено от закона легитимно основание“ в член 5, параграф 2 от модернизираната Конвенция № 108 обхваща и „обработването на данни с цел изпълнението на договор (или преддоговорни мерки по искане на субекта на данните), по който субектът на данните е страна“[379].

377 Общ регламент относно защитата на данните, член 17, параграф 1, буква б).

378 *Пак там*, член 6, параграф 1, буква б).

379 Обяснителен доклад към модернизираната Конвенция № 108, параграф 46; Съвет на Европа, Комитет на министрите (2010 г.), Препоръка CM/Rec(2010)13 на Комитета на министрите до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране, 23 ноември 2010 г., член 3, параграф 4, буква б).

Правни задължения на администратора

В правото на ЕС се посочва още едно основание за законосъобразност на обработването на данни, а именно, ако „обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора“ (член 6, параграф 1, буква в) от ОРЗД). Тази разпоредба се отнася до администраторите както в частния, така и в публичния сектор; правните задължения на администраторите на данни в публичния сектор може да попадат и в обхвата на член 6, параграф 1, буква д) от ОРЗД. Има много примери за ситуации, в които законът задължава администраторите от частния сектор да обработват данни за конкретни субекти на данни. Например работодателите трябва да обработват данни за своите служители по причини, свързани със социалното осигуряване и данъчното облагане, а предприятията трябва да обработват данни за своите клиенти по причини, свързани с данъчното облагане.

Правното задължение може да произтича от законодателството на Съюза или на държавата членка, което може да представлява основание за една или няколко операции по обработване. В правото следва да се определя целта на обработването, да се установяват спецификациите за определянето на администратора на лични данни, видът лични данни, които подлежат на обработване, съответните субекти на данни, образуванията, пред които могат да бъдат разкривани лични данни, ограниченията по отношение на целите, периодът на съхранение и други мерки за гарантиране на законосъобразното и добросъвестно обработване[380]. Всяко такова законодателство, което се явява основание за обработване на лични данни, трябва да е съобразено както с членове 7 и 8 от Хартата, така и с член 8 от ЕКПЧ.

Правните задължения на администратора също служат като основание за законосъобразно обработване на данни съгласно **правото на Съвета на Европа**[381]. Както е посочено по-горе, правните задължения на администратор в частния сектор са само един конкретен случай за законни интереси на други лица, както е посочено в член 8, параграф 2 от ЕКПЧ. Следователно обработването от страна на работодателите на данни за техните служители е подходящ пример и за правото на Съвета на Европа.

380 Общ регламент относно защитата на данните, съображение 45.

381 Съвет на Европа, Комитет на министрите (2010 г.), Препоръка CM/Rec(2010)13 на Комитета на министрите до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране, 23 ноември 2010 г., член 3, параграф 4, буква а).

Жизненоважни интереси на субекта на данните или на друго физическо лице

В правото на ЕС член 6, параграф 1, буква г) от ОРЗД предвижда, че обработването на лични данни е законосъобразно, ако „е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице". Това законово основание може да влезе в действие по отношение на обработването на лични данни, основано на жизненоважни интереси на други физически лица, само ако обработването „не може явно да се базира на друго правно основание"[382]. Понякога даден вид обработване може да има за основание както обществения интерес, така и жизненоважни интереси на субекта на данните или на друго лице. Такъв е случаят например, когато се наблюдават епидемии и тяхното развитие или при спешни хуманитарни ситуации.

В правото на Съвета на Европа жизненоважните интереси на субекта на данните не се посочват в член 8 от ЕКПЧ. Жизненоважните интереси на субекта на данните обаче се считат за включени в понятието за „легитимно основание" по член 5, параграф 2 от модернизираната Конвенция № 108, който третира легитимността на обработването на лични данни[383].

Обществен интерес и упражняване на официални правомощия

С оглед на множеството възможни начини за организиране на публичните дела, член 6, параграф 1, буква д) от ОРЗД предвижда, че личните данни могат да бъдат обработвани законосъобразно, ако обработването е „необходимо за изпълнение на задача от обществен интерес или при упражняване на официалните правомощия, предоставени на администратора на лични данни [...]"[384].

Пример: В делото *Huber/Bundesrepublik Deutschland*[385] г-н Huber, пребиваващ в Германия австрийски гражданин, е поискал от Федералната служба за миграцията и бежанците заличаване на свързани с него данни в Централния регистър за чужденците

382 Общ регламент относно защитата на данните, съображение 46.

383 Обяснителен доклад към модернизираната Конвенция № 108, параграф 46.

384 Вж. Общ регламент относно защитата на данните, съображение 45.

385 Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г.

(наричан по-нататък „AZR“). Регистърът, който съдържа лични данни за граждани на ЕС, които не са германски граждани, но пребивават в Германия в продължение на повече от три месеца, се използва за статистически цели, както и от правоприлагащите и съдебните органи при разследването и наказателното преследване на престъпни дейности или на такива, които представляват заплаха за обществената сигурност. Въпросът на запитващата юрисдикция е дали обработването на лични данни, извършвано в регистър като Централния регистър за чужденците, до който други публични органи също имат достъп, е съвместимо с правото на ЕС, като се има предвид, че не съществува такъв регистър за германските граждани.

Съдът на ЕС постановява, че съгласно член 7, буква д) от Директива 95/46[386] личните данни могат да бъдат обработвани законосъобразно, ако обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес или при упражняване на официални правомощия.

Според Съда на ЕС „предвид целта да се осигури еднаква степен на защита във всички държави членки понятието за необходимост, което произтича от член 7, буква д) от Директива 95/46[387], [...] не може да има различно съдържание в зависимост от държавите членки. Следователно става въпрос за самостоятелно понятие на общностното право, на което трябва да се направи тълкуване, отговарящо в пълна степен на предмета на тази директива, определен в член 1, параграф 1 от нея[388].

Съдът на ЕС отбелязва, че правото на свободно движение на гражданин на Съюза на територията на държава членка, на която не е гражданин, не е безусловно, а може да бъде придружено с ограничения и условия, предвидени от Договора за създаване на Европейската общност, както и от мерките, приети за неговото прилагане. Следователно ако използването на регистър като AZR, за да се подпомагат органите, отговарящи за прилагането на нормативната уредба относно правото

386 Предходна Директива за защита на личните данни, член 7, буква д), понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква д).

387 *Пак там*.

388 Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г., параграф 52.

на пребиваване, по принцип е законосъобразно за дадена държава членка, то този регистър трябва да съдържа само необходимата за тази цел информация. Съдът на ЕС заключава, че такава система за обработване на лични данни е в съответствие с правото на ЕС, ако тя съдържа единствено данните, които са необходими, за да се прилага тази нормативна уредба, и ако централизираният ѝ характер позволява по-ефективното прилагане на тази нормативна уредба. Националната юрисдикция трябва да провери дали в конкретния случай тези условия са изпълнени. Ако не са, при всяко положение съхранението и обработването на лични данни в рамките на регистър като AZR за статистически цели не могат да се приемат за необходими по смисъла на член 7, буква д)[389] от Директива 95/46[390].

Накрая, що се отнася до въпроса за използването на съдържащите се в регистъра данни с цел борба с престъпността, Съдът счита, че тази цел „със сигурност е да се преследват извършените престъпления и деликти без оглед на гражданството на извършителя им". Въпросният регистър не съдържа лични данни, отнасящи се до граждани на съответната държава членка, и това различно третиране представлява дискриминация, забранена от член 18 от ДФЕС. Затова Съдът на ЕС констатира, че тази разпоредба „не допуска с оглед на целта за борба с престъпността държава членка да създаде система за обработване на лични данни специално за гражданите на Съюза, които не са граждани на тази държава членка"[391].

Използването на лични данни от органи в публичната сфера също влиза в обхвата на разпоредбите на член 8 от **ЕКПЧ**, като по отношение на това използване, когато е необходимо, може да се прилага член 5, параграф 2 от модернизираната Конвенция № 108[392].

389 Предходна Директива за защита на личните данни, член 7, буква д), понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква д).

390 Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г., параграфи 54, 58—59 и 66—68.

391 *Пак там*, параграфи 78 и 81.

392 Обяснителен доклад към модернизираната Конвенция № 108, параграфи 46 и 47.

Законни интереси, преследвани от администратора или от трета страна

Съгласно **правото на ЕС** субектът на данни не е единственият със законни интереси. Член 6, параграф 1, буква е) от ОРЗД предвижда, че личните данни могат да бъдат обработвани законосъобразно, ако обработването „е необходимо за целите на легитимните интереси на администратора или на трета страна или страни [с изключение на публични органи при изпълнението на техните задачи], на които се разкриват данните, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита [...]“[393].

За установяването на законен интерес е необходима внимателна преценка във всеки конкретен случай[394]. Ако бъде установен легитимен интерес на администратора, тогава трябва да се потърси баланс между този интерес и интересите или основните права и свободи на субекта на данни[395]. При тази преценка трябва да се вземат предвид основателните очаквания на субекта на данни, за да се установи дали интересите на администратора имат преимущество пред интересите или основните права на субекта на данни[396]. Ако правата на субекта на данни имат преимущество пред законните интереси на администратора, администраторът може да предприеме мерки и да въведе гаранции, за да гарантира, че въздействието върху правата на субекта на данни е сведено до минимум (например псевдонимизация на данните), и да „обърне преимуществото“, преди да може законно да се опре на това правно основание за обработване. В Становището си относно понятието за законосъобразни интереси на администратора на данни Работната група по член 29 подчертава, че при търсенето на баланс между законните интереси на администратора и интересите на основните права на субекта на данни решаваща роля имат отчетността и прозрачността, както и правата на субектите на данни на възражение срещу обработването на данните им или срещу това данните да бъдат достъпни, променяни, заличавани или прехвърляни[397].

393 В сравнение с Директива 95/46, в Общия регламент относно защитата на данните са дадени повече примери за случаи, за които се счита, че представляват законен интерес.

394 Общ регламент относно защитата на данните, съображение 47.

395 Работна група по член 29 (2014 г.), *Становище 06/2014 относно понятието за законосъобразни интереси на администратора на данни съгласно член 7 от Директива 95/46/ЕО*, WP 217, 4 април 2014 г.

396 *Пак там.*

397 *Пак там.*

В съображенията на ОРЗД са приведени няколко примера какво представлява законен интерес на съответния администратор на данни. Например обработването на лични данни е разрешено без съгласието на субекта на данни, когато се извършва за целите на директния маркетинг или когато е „строго необходимо за целите на предотвратяването на измами“[398].

В съдебната си практика Съдът на ЕС е разширил проверката за установяване на наличието на законен интерес.

Пример: Делото *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] се отнася до вреда, причинена на тролейбус на тролейбусното дружество на град Рига поради внезапно отваряне на врата на такси от пътник в таксито. Тролейбусното дружество на град Рига (наричано по-нататък „Rīgas satiksme“) иска да съди пътника на таксито за причинената вреда. Полицията обаче предоставя само името на пътника и отказва да предостави неговия личен идентификационен номер и адреса му, като изтъква, че разкриването им би било незаконно съгласно националното законодателство за защита на данните.

Запитващата латвийска юрисдикция отправя до Съда на ЕС преюдициално запитване дали правото на ЕС в областта на защитата на данните създава задължение за разкриване на всички лични данни, необходими за подаването на граждански иск срещу лицето, за което се твърди, че е отговорно за административно нарушение[400].

Съдът на ЕС пояснява, че правото на ЕС в областта на защитата на данните включва възможността, а не задължението за разкриване на трета страна на данни, необходими за целите на преследваните от него законни интереси[401]. Съдът на ЕС определя три кумулативни условия, които трябва да бъдат изпълнени, за да бъде обработването на лични данни законосъобразно на основание „законни интереси“[402]. На първо място, третото лице, на което се разкриват данните, трябва

398 Общ регламент относно защитата на данните, съображение 47.

399 Съд на ЕС, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA ‘Rīgas satiksme’*, 4 май 2017 г.

400 *Пак там,* параграф 23.

401 *Пак там,* параграф 26.

402 *Пак там,* параграфи 28–34.

да преследва законен интерес. В конкретния случай това означава, че искането на лична информация, за да бъде предявен иск срещу определено лице за причинени от него имуществени вреди, представлява законен интерес на трета страна. На второ място, обработването на личните данни трябва да е необходимо за целите на преследваните законни интереси. В настоящия случай придобиването на лична информация, като адреса и/или личния идентификационен номер, е строго необходимо за установяването на самоличността на това лице. На трето място, основните права и свободи на субекта на данни не трябва да имат предимство пред законните интереси на администратора или на третите лица. Интересите трябва да се претеглят за всеки конкретен случай, като се вземат предвид такива елементи, като тежестта на засягане на правата на субекта на данни и дори възрастта му при определени обстоятелства. В дадения случай обаче Съдът на ЕС не счита отказа да бъдат разкрити данните за оправдан само защото субектът на данните не е навършил пълнолетие.

В решението по дело *ASNEF u FECEMD* Съдът на ЕС дава изрично отсъждане по отношение на обработването на данни на основание „законни интереси“, което по това време е залегнало в член 7, буква е) от Директивата за защита на личните данни[403].

Пример: В решението по дело *ASNEF u FECEMD*[404] Съдът на ЕС пояснява, че не е разрешено в националното законодателство да се добавят условия в допълнение към тези, посочени в член 7, буква е) от Директивата за законосъобразно обработване на данни[405]. Това се отнася за ситуация, при която в испанското законодателство за защита на данните се е съдържала разпоредба, съгласно която други частни лица са можели да предявят законен интерес за обработването на лични данни само ако информацията вече е била оповестена в публични източници.

403 Предходна Директива за защита на личните данни, член 7, буква е), понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква е).

404 Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г.

405 Предходна Директива за защита на личните данни, член 7, буква е), понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква е).

Съдът на ЕС първо отбелязва, че Директива 95/46[406] има за цел да уеднакви във всички държави членки степента на защита на правата и свободите на лицата при обработването на лични данни. Освен това сближаването на приложимите в тази област национални законодателства не трябва да води до намаляване на степента на защита, която те осигуряват. То вместо това трябва да има за цел да гарантира висока степен на защита в ЕС[407]. При това положение Съдът на ЕС постановява, че „от целта да се осигури еднаква степен на защита във всички държави членки следва, че член 7 от Директива 95/46[408] съдържа изчерпателен списък на случаите, в които обработването на лични данни може да се счита за законно". Освен това „държавите членки не могат нито да добавят нови критерии за законност на обработването на лични данни към член 7 от Директива 95/46[409], нито да предвиждат допълнителни изисквания, които изменят обхвата на някой от посочените в този член шест критерия"[410]. Съдът на ЕС допуска, че във връзка с необходимото търсене на баланс, съгласно член 7, буква е) от Директива 95/46, е възможно да се вземе предвид обстоятелството, че тежестта на засягане на основните права на лицето, до което се отнасят съответните данни, може да е различна в зависимост от това дали тези данни се съдържат или не в общодостъпни източници.

Член 7, буква е) от тази директива обаче „не допуска държава членка да изключи категорично и безусловно възможността за обработване на някои категории лични данни, без да позволи претегляне във всеки конкретен случай на съответните противоположни права и интереси".

406 Предходна Директива за защита на личните данни, понастоящем Общ регламент относно защитата на данните.

407 Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г., параграф 28. Общ регламент относно защитата на данните, съображения 8 и 10.

408 Предходна Директива за защита на личните данни, член 7, понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква е).

409 Предходна Директива за защита на личните данни, член 7, понастоящем Общ регламент относно защитата на данните, член 6.

410 *Пак там.*

> С оглед на тези съображения Съдът на ЕС заключава, че член 7, буква е) от Директива 95/46[411] трябва да се тълкува в смисъл, че „не допуска национална правна уредба, която предвижда, че за да се допусне обработване на лични данни без съгласието на съответното физическо лице, когато това е необходимо за реализирането на законни интереси на администратора или на едно или повече трети лица, на които се разкриват данните, не е достатъчно с обработването да не се нарушават основните права и свободи на това лице, а трябва и въпросните данни да се съдържат в общодостъпни източници, като по този начин изключва категорично и безусловно обработването на данни, които не се съдържат в такива източници“[412].

Съгласно член 21, параграф 1 от ОРЗД винаги когато се обработват лични данни на основание „законни интереси“, физическото лице има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни. Администраторът трябва да прекрати обработването, освен ако не докаже, че съществуват убедителни законови основания за продължаването му.

Що се отнася до **правото на Съвета на Европа**, подобни формулировки могат да бъдат намерени в модернизираната Конвенция № 108[413] и препоръките на Съвета на Европа. В Препоръката относно профилирането обработването на лични данни за целите на профилирането се признава за законно, ако е необходимо за законните интереси на други лица, „с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на субектите на данни“[414]. Освен това „защитата на правата и свободите на другите“ е посочена в член 8, параграф 2 от ЕКПЧ като едно от законните основания за ограничаване на правото на защита на личните данни.

411 Предходна Директива за защита на личните данни, член 7, буква е), понастоящем Общ регламент относно защитата на данните, член 6, параграф 1, буква е).

412 Съд на ЕС, съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г., параграфи 40, 44 и 48—49.

413 Обяснителен доклад към модернизираната Конвенция № 108, параграф 46.

414 Съвет на Европа, Комитет на министрите (2010 г.), Препоръка CM/Rec(2010)13 и обяснителен меморандум относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране, 23 ноември 2010 г., член 3.4, буква б) (Препоръка относно профилирането).

Пример: В делото *Y/Турция*[415] жалбоподателят е ХИВ позитивен. Тъй като е бил в безсъзнание при пристигането си в болницата, екипът на линейката е информирал болничния персонал, че пациентът е ХИВ позитивен. Жалбоподателят твърди пред ЕСПЧ, че разкриването на тази информация е нарушило правото му на неприкосновеност на личния живот. Като се има предвид обаче необходимостта да се защити безопасността на болничния персонал, споделянето на информацията не се счита за нарушаване на правата на жалбоподателя.

4.1.2 Обработване на специални категории данни (чувствителни данни)

Правото на Съвета на Европа оставя на националното законодателство да определи подходяща защита за използването на чувствителни данни, при условие че са изпълнени условията на член 6 от модернизираната Конвенция № 108, а именно че в закон са предвидени подходящи мерки за сигурност, които да допълват другите разпоредби на Конвенцията. **Правото на ЕС**, в член 9 от ОРЗД, съдържа подробен режим за обработването на специални категории данни (наричани също така „чувствителни данни"). Тези данни разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични и 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. Обработването на чувствителни данни по принцип е забранено[416].

Съществува обаче изчерпателен списък с изключения от тази забрана, който може да бъде намерен в член 9, параграф 2 от регламента, и тези изключения представляват законни основания за обработване на чувствителни данни. Тези изключения включват ситуации, в които:

- субектът на данни е дал своето изрично съгласие за обработването на тези данни;

415 ЕСПЧ, *Y/Турция*, № 648/10, 17 февруари 2015 г.

416 Предходна Директива за защита на личните данни, член 7, буква е), понастоящем Общ регламент относно защитата на данните, член 9, параграф 1.

- обработването се извършва в хода на законните дейности на структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, и е свързано единствено с (бившите) членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели;

- обработването е свързано с данни, които явно са направени обществено достояние от субекта на данни;

- обработването е необходимо:

  - за изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по отношение на заетостта, социалната сигурност и социалната закрила;

  - за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице (когато субектът на данните не е в състояние да даде своето съгласие);

  - с цел установяване, упражняване или защита на правни претенции или когато съдилищата действат в качеството си на правораздаващи органи;

  - за целите на превантивната или трудовата медицина: „за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза или правото на държава членка или съгласно договор с медицинско лице“;

  - за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;

  - по причини от обществен интерес в областта на общественото здраве; или

  - по причини от важен обществен интерес.

Следователно при обработването на специални категории данни наличието на договорно отношение със субекта на данните не се счита за правно основание за законосъобразно обработване на чувствителни данни, освен при договор с медицинско лице, което е обвързано от задължението за професионална тайна[417].

Изрично съгласие на субекта на данни

Съгласно **правото на ЕС** първото възможно основание за законосъобразно обработване на данни, независимо от това дали те са нечувствителни или чувствителни данни, е съгласието на субекта на данни. По отношение на чувствителните данни това съгласие трябва да бъде изрично. Правото на Съюза или на държава членка обаче може да предвижда, че забраната за обработване на специални категории данни не може да бъде отменена от съответното лице[418]. Такъв може да е случаят например, когато обработването включва необичайни рискове за субекта на данни.

Трудово право или право в областта на социалната сигурност и социалната закрила

Съгласно **правото на ЕС** забраната, посочена в член 9, параграф 1, може да бъде отменена, ако обработването е необходимо за целите на изпълнението на задълженията или упражняването на правата на администратора или на субекта на данните в областта на заетостта или социалната сигурност. Обработването обаче трябва да е разрешено от правото на ЕС или националното право, или съгласно колективна договореност в съответствие с националното право, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данни[419]. При известни условия, определени в ОРЗД и съответното национално законодателство, в досиетата на служителите на дадена организация, съхранявани от нея, може да се съдържат чувствителни лични данни. Като примери за чувствителни данни може да се посочат данните за членство в синдикални организации или информация, свързана със здравословното състояние.

417 Общ регламент относно защитата на данните, член 9, параграф 2, букви з) и и).

418 *Пак там,* член 9, параграф 2, буква а).

419 Общ регламент относно защитата на данните, член 9, параграф 2, буква б).

Жизненоважни интереси на субекта на данни или на друго лице

Съгласно **правото на ЕС**, както при нечувствителните данни, чувствителните данни може да бъдат обработвани поради основания, свързани с жизненоважните интереси на субекта на данните или на друго физическо лице[420]. Когато обработването се основава на жизненоважните интереси на друго лице, това законово основание може да влезе в действие само ако обработването „не може явно да се базира на друго правно основание"[421]. В някои случаи обработването на лични данни може да защитава както лични, така и обществени интереси, например когато то е необходимо за хуманитарни цели[422].

За да бъде обработването на чувствителни данни законно на това основание, би трябвало да е невъзможно да се поиска съгласие от субекта на данните, например поради това че той е в безсъзнание или отсъства и не може да бъде установена връзка с него. С други думи, лицето е било физически или юридически неспособно да даде своето съгласие.

Благотворителни организации или структури с нестопанска цел

Обработването на лични данни е разрешено също така в хода на законните дейности на фондации, сдружения или други структури с нестопанска цел, с политическа, философска, религиозна или синдикална цел. Обработването обаче трябва да е свързано единствено с членовете или бившите членове на съответната структура или с лица, които поддържат редовни контакти с нея[423]. Чувствителните данни не може да бъдат разкривани извън рамките на тези структури без съгласието на субектите на данните.

Данни, които явно са направени обществено достояние от субекта на данните

В член 9, параграф 2, буква д) от ОРЗД се предвижда, че обработването не е забранено, ако е свързано с данни, които явно са направени обществено достояние от субекта на данните. Макар и значението на текста „явно са направени обществено достояние от субекта на данните" да не е определено

420 *Пак там*, член 9, параграф 2, буква в).

421 *Пак там*, съображение 46.

422 *Пак там*.

423 *Пак там,* член 9, параграф 2, буква г).

в регламента, тъй като представлява изключение от забраната за обработване на чувствителни данни, то трябва да се тълкува стриктно и в смисъл, че субектът на данните трябва умишлено да е направил личните си данни обществено достояние. Следователно когато една телевизия излъчи видеоматериал, заснет от камера за видеонаблюдение, показващ, наред с другото, нараняването на пожарникар, докато се опитва да евакуира жителите на сграда, не може да се счита, че пожарникарят явно е направил данните обществено достояние. От друга страна, ако пожарникарят реши да опише произшествието и публикува видеоматериал и снимки на публична интернет страница, той ще е извършил изричен утвърдителен акт, за да направи личните данни обществено достояние. Важно е да се отбележи, че когато някой направи данните си обществено достояние, това не представлява съгласие, но се явява друг вид разрешение за обработване на специални категории данни.

Фактът, че субектът на данните е направил обществено достояние обработваните лични данни, не освобождава администраторите от техните задължения съгласно правото за защитата на данните. Например принципът на ограничение на целите продължава да е приложим за личните данни, дори ако тези данни са били направени обществено достояние[424].

Правни претенции

Обработването на специални категории данни, което „е необходимо с цел установяване, упражняване или защита на правни претенции", независимо дали това е в рамките на съдебна, административна или друга извънсъдебна процедура[425], също е разрешено по ОРЗД[426]. В този случай обработването трябва да е от значение за конкретната правна претенция и съответно за нейното упражняване или защита и може да бъде поискано от всяка от страните по спора.

Когато действат в качеството си на правораздаващи органи, съдилищата могат да обработват специални категории данни в контекста на разрешаването на съдебен спор[427]. Примери за такива специални категории данни, обра-

424 Работна група по член 29 (2013 г.), *Становище 3/2013 относно ограничаването на целта*, WP 203, Брюксел, 2 април 2013 г., стр. 14.

425 Общ регламент относно защитата на данните, преамбюл, съображение 52.

426 *Пак там*, член 9, параграф 2, буква е).

427 *Пак там*.

ботвани в такъв контекст, биха могли да бъдат например генетичните данни при установяване на родствена връзка или здравословното състояние, когато част от доказателствата се отнасят до данни за нараняването на жертва на престъпление.

Причини от важен обществен интерес

В съответствие с член 9, параграф 2, буква ж) от ОРЗД държавите членки могат да въведат допълнителни обстоятелства, при които могат да се обработват чувствителни данни, при условие че:

- обработването на данни е по причини от важен обществен интерес;
- обработването е предвидено в европейското или националното законодателство;
- европейското или националното законодателство е пропорционално, зачита правото на защита на данните и предвижда подходящи и конкретни мерки за защита на правата и интересите на субекта на данните[428].

Показателен пример са системите за електронни здравни досиета. Тези системи позволяват здравни данни, събирани от доставчиците на здравни услуги в хода на лечението на даден пациент, да се предоставят на други доставчици на здравни услуги на този пациент в голям мащаб, обикновено в национален мащаб.

Работната група по член 29 достигна до заключението, че такива системи не могат да бъдат създадени въз основа на съществуващите правни норми за обработване на данни относно пациенти[429]. Системи за електронни здравни досиета обаче е възможно да съществуват, ако се основават на „причини от важен обществен интерес"[430]. За тяхното създаване е необходимо изрично

428 *Пак там*, член 9, параграф 2, буква ж).

429 Работна група по член 29 (2007 г.), *Работен документ относно обработването на лични здравни данни в електронните здравни досиета (ЕЗД)*, WP 131, Брюксел, 15 февруари 2007 г. Вж. също Общ регламент относно защитата на данните, член 9, параграф 3.

430 Общ регламент относно защитата на данните, член 9, параграф 2, буква ж).

правно основание, което също така съдържа необходимите гаранции, за да се осигури сигурното функциониране на системата[431].

Други основания за обработване на чувствителни данни

В ОРЗД се предвижда, че чувствителни данни може да бъдат обработвани, когато това е необходимо[432]:

- за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на ЕС или правото на държава членка, или съгласно договор с медицинско лице;

- по причини от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, въз основа на правото на ЕС или правото на държава членка. В правото трябва да са предвидени подходящи и конкретни мерки за защита на правата на субекта на данните;

- за целите на архивирането, за научни или исторически изследвания или за статистически цели, на основание правото на Съюза или правото на държава членка. Правото трябва да е пропорционално на преследваната цел, да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

Допълнителни условия съгласно националното законодателство

ОРЗД позволява също така на държавите членки да въведат или да запазят допълнителни условия, включително и ограничения, по отношение на

431 Работна група по член 29 (2007 г.), *Работен документ относно обработването на лични здравни данни в електронните здравни досиета (ЕЗД),* WP 131, Брюксел, 15 февруари 2007 г.

432 Общ регламент относно защитата на данните, член 9, параграф 2, букви з), и) и й).

обработването на генетични данни, биометрични данни или данни за здравословното състояние[433].

4.2 Правила относно сигурността на обработването

Ключови въпроси

- Правилата относно сигурността на обработването задължават администратора и обработващия лични данни да прилагат подходящи технически и организационни мерки, за да се предотврати всякаква неразрешена намеса в операциите по обработване на данни.
- Необходимото ниво на сигурност на данните се определя от:
  - елементите на сигурността, достъпни на пазара за всеки отделен вид обработване;
  - разходите;
  - рисковете, които обработването на данните създава за основните права и свободи на субектите на данни.
- Гарантирането на поверителност на личните данни е част от общия принцип, признат в Общия регламент относно защитата на данните.

Както съгласно правото на ЕС, така и съгласно правото на Съвета на Европа администраторите имат общото задължение да спазват прозрачност и отчетност при обработването на лични данни, особено по отношение на нарушения на сигурността на данните, когато възникнат такива нарушения. В случай на нарушения на сигурността на личните данни администраторите трябва да уведомяват надзорните органи, освен ако няма вероятност нарушението да породи риск за правата и свободите на физическите лица. Субектите на данни също следва да бъдат информирани за нарушение на сигурността на личните данни, когато има вероятност то да породи висок риск за правата и свободите на физическите лица.

433 *Пак там*, член 9, параграф 2, буква з) и член 9, параграф 4.

4.2.1 Елементи на сигурността на данните

Съгласно съответните разпоредби на **правото на ЕС**:

> *„Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност[...].“*[434]

Тези мерки включват, наред с другото:

- псевдонимизация и криптиране на личните данни[435];
- гарантиране на поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване[436];
- своевременно възстановяване на наличността и достъпа до личните данни в случай на загуба на данни[437];
- процес на изпитване, преценяване и оценка на ефективността на мерките с оглед да се гарантира сигурността на обработването[438].

Подобна разпоредба съществува съгласно **правото на Съвета на Европа**:

> *„Всяка страна предвижда, че администраторът и, където е приложимо, обработващият лични данни вземат подходящи мерки за сигурност срещу рискове като неволен или неразрешен достъп, унищожаване, загуба, използване, промяна или разкриване на лични данни.“*[439]

434 *Пак там*, член 32, параграф 1.

435 *Пак там*, член 32, параграф 1, буква а).

436 *Пак там*, член 32, параграф 1, буква б).

437 *Пак там*, член 32, параграф 1, буква в).

438 *Пак там*, член 32, параграф 1, буква г).

439 Модернизирана Конвенция № 108, член 7, параграф 1.

Съгласно **правото на ЕС и на Съвета на Европа** при нарушение на сигурността на данните, което може да повлияе на правата и свободите на лицата, администраторът е длъжен да уведоми за него надзорния орган (вж. раздел 4.2.3).

Често има също така отраслови, национални и международни стандарти, които са били изготвени с цел сигурно обработване на данните. Европейският печат за неприкосновеност на личния живот (EuroPriSe) например е проект по програма eTEN (Трансевропейски телекомуникационни мрежи) на ЕС, в който се проучват възможностите за сертифициране на продукти, особено софтуер, като съответстващи на европейското право за защита на данните. Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) беше създадена, за да увеличи възможностите на ЕС, на държавите членки на ЕС и на деловата общност за предотвратяване, разглеждане и разрешаване на проблемите на мрежовата и информационната сигурност[440]. ENISA редовно публикува анализи на настоящите заплахи за сигурността и съвети относно начините за справяне с тях[441].

Сигурността на данните не се постига само с наличието на правилното оборудване — хардуер и софтуер. За това се изискват също така подходящи вътрешни организационни правила. Подобни вътрешни правила биха обхващали в идеалния случай следните въпроси:

- редовно предоставяне на всички служители на информация относно правилата за сигурност на данните и техните задължения съгласно правото за защита на данните, особено по отношение на техните задължения за поверителност;

- ясно разпределяне на задълженията и ясно очертаване на правомощията по въпроси, свързани с обработването на данни, особено във връзка с взимане на решения за обработване на лични данни и за предаване на данни на трети страни или на субекти на данни;

440 Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 година относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004, ОВ L 165, 18.6.2013 г.

441 Напр. ENISA, (2016 г.), Киберсигурност и устойчивост на интелигентните автомобили. Добри практики и препоръки; ENISA (2016 г.), Сигурност на мобилните плащания и цифровите портфейли.

- използване на лични данни само в съответствие с инструкциите на компетентното лице или в съответствие с установените общи правила;

- защита на достъпа до местонахожденията и до хардуера и софтуера на администратора или на обработващия лични данни, включително проверки относно разрешението за достъп;

- гарантиране, че разрешенията за достъп до лични данни са били дадени от компетентното лице и изискване на надлежна документация;

- автоматизирани протоколи относно електронния достъп до лични данни и редовни проверки на тези протоколи от вътрешната надзорна служба (като по този начин се изисква всички дейности по обработване на данни да бъдат регистрирани);

- точна документация за други форми на разкриване, различни от автоматизирания достъп до данни, за да има възможност да се докаже, че не е осъществено незаконно предаване на данни.

Важен елемент от ефективните предпазни мерки, свързани със сигурността, е и предлагането на подходящо обучение и образование по въпросите на сигурността на данните на членовете на персонала. Трябва да бъдат въведени и процедури за проверка, за да се гарантира, че съответните мерки съществуват не само на хартия, а се прилагат и функционират на практика (като например вътрешни или външни одити).

Мерките, които се използват от администратора или обработващия лични данни за подобряване на степента на сигурност, включват инструменти, като например длъжностни лица за защита на личните данни, образование на служителите по въпросите на сигурността, редовни одити, тестване на вероятни пробиви и печати за качество.

Пример: В делото *I./Финландия*[442] жалбоподателката не е била в състояние да докаже, че други служители на болницата, в която е работела, са имали незаконен достъп до нейното здравно досие. Поради това нейният иск за нарушаване на правото ѝ на защита на

442 ЕСПЧ, *I/Финландия*, № 20511/03, 17 юли 2008 г.

данните е бил отхвърлен от националните съдилища. ЕСПЧ заключава, че е налице нарушение на член 8 от ЕКПЧ, тъй като системата на болницата за вписване в здравните досиета „била такава, че не било възможно със задна дата да се изясни използването на данни за пациента, тъй като тя показвала само петте най-скорошни консултации, и че тази информация била заличавана веднага след връщането на досието в архива“. Решаващо за съда е, че въведената в болницата система за вписване на данни явно не била в съответствие с правните изисквания, съдържащи се в националното законодателство — факт, на който националните съдилища не са отдали подобаващо значение.

ЕС въведе Директивата относно сигурността на мрежите и информационните системи (Директивата за МИС)[443], която е първият правен инструмент относно киберсигурността на равнището на целия ЕС. С Директивата се цели, от една страна, да се подобри киберсигурността на национално равнище и, от друга страна, да се повиши нивото на сътрудничество в рамките на ЕС. С нея също така се налагат задължения на операторите на основни услуги (включително операторите в секторите на енергетиката, здравеопазването, банковото дело, транспорта, цифровата инфраструктура и т.н.) и на доставчиците на цифрови услуги да управляват рисковете, да гарантират сигурността на техните мрежи и информационни системи и да докладват за свързаните със сигурността инциденти.

Перспективи

През септември 2017 г. Европейската комисия предложи проект на регламент, който има за цел да реформира мандата на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), за да се вземат предвид новите правомощия и отговорности на агенцията съгласно Директивата за МИС. Целта на предложението за регламент е да развие задачите на ENISA и да засили нейната роля като „отправна точка в екосистемата на киберсигурността в ЕС“[444]. Предложението за регламент не следва да засегне принци-

443 Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, ОВ L 194, 2016 г.

444 Предложение за регламент на Европейския парламент и на Съвета относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“), COM(2017) 477, 13 септември 2017 г., стр. 6.

пите на ОРЗД, а чрез изясняване на необходимите елементи на европейските схеми за сертифициране на киберсигурността следва да подобри сигурността на личните данни. Успоредно с това през септември 2017 г. Европейската комисия предложи проект на регламент за изпълнение, в който се конкретизират елементите, които доставчиците на цифрови услуги следва да вземат предвид, за да гарантират, че техните мрежи и информационни системи са сигурни, както се изисква в член 16, параграф 8 от Директивата за МИС. Към момента на изготвяне на наръчника обсъжданията по тези две предложения все още продължаваха.

4.2.2 Поверителност

Съгласно **правото на ЕС** в ОРЗД поверителността на личните данни се разглежда като част от един общ принцип[445]. Доставчиците на обществено-достъпни електронни съобщителни услуги трябва да гарантират поверителност. Те имат също така задължението да защитят сигурността на своите услуги[446].

Пример: Служителка в застрахователно дружество получава телефонно обаждане на работното си място от лице, което казва, че е клиент, като изисква информация, отнасяща се до неговия застрахователен договор.

Задължението за опазване на поверителността на данните на клиента изисква от служителката да приложи най-малко минимални мерки за сигурност, преди да разкрие лични данни. Това например би могло да стане, като предложи да върне обаждането на телефонен номер, документиран в досието на клиента.

Съгласно член 5, параграф 1, буква е) личните данни трябва да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

445 Общ регламент относно защитата на данните, член 5, параграф 1, буква е).

446 Директива за правото на неприкосновеност на личния живот и електронни комуникации, член 5, параграф 1.

По силата на член 32 администраторът и обработващият лични данни трябва да прилагат технически и организационни мерки, за да гарантират високо ниво на сигурност. Тези мерки включват, наред с другото, псевдонимизация и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на обработването, оценка и изпитване на ефективността на мерките и способност за възстановяване на обработването в случай на физически или технически инцидент. Освен това придържането към одобрен кодекс на поведение или одобрен механизъм за сертифициране може да се използва като елемент за доказване, че е спазен принципът на цялостност и поверителност. В допълнение, съгласно член 28 от ОРЗД, в договора, който е задължителен за администратора спрямо обработващия лични данни, трябва да е предвидено, че обработващият лични данни гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност.

Задължението за поверителност не обхваща ситуации, в които данните стават известни на лице в неговото качество на частно физическо лице, а не на служител на администратор или обработващ лични данни. В този случай членове 32 и 28 от ОРЗД не са приложими, тъй като използването на лични данни от частни физически лица е напълно изключено от обхвата на регламента, където подобно използване попада в рамките на т. нар. изключение за дейности в рамките на домакинството[447]. Изключението за дейности в рамките на домакинството се отнася до използването на лични данни „от физическо лице в хода на чисто лични или домашни занимания“[448]. След решението на Съда на ЕС по делото *Bodil Lindqvist*[449] обаче това изключение трябва да се тълкува ограничително, особено във връзка с разкриването на данни. По-специално изключението за дейности в рамките на домакинството не обхваща публикуването на лични данни за неограничен брой получатели в интернет или обработването на данни, което има професионални или търговски аспекти (за повече подробности по делото вж. раздели 2.1.2, 2.2.2 и 2.3.1).

„Поверителността на съобщенията“ е друг аспект на поверителността, който е предмет на *lex specialis*. Специалните правила за гарантиране на поверителния характер на електронните съобщения съгласно Директивата за правото

447 Общ регламент относно защитата на данните, член 2, параграф 2, буква в).

448 *Пак там*.

449 Съд на ЕС, C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г.

на неприкосновеност на личния живот и електронни комуникации изискват държавите членки да забраняват на всички лица, различни от потребители, без съгласието на заинтересованите потребители да слушат, записват, съхраняват или подслушват или наблюдават по друг начин съобщенията и свързаните метаданни[450]. Националното право може да разрешава изключения от този принцип само по съображения, свързани с националната сигурност, отбраната, превенцията или разкриването на престъпления, и само ако такива мерки са необходими и пропорционални за преследваните цели[451]. Същите правила ще се прилагат съгласно бъдещия Регламент за неприкосновеността на личния живот и електронните съобщения, но все пак приложното поле на правния акт относно неприкосновеността на личния живот и електронните съобщения ще бъде разширено, за да обхваща освен общественодостъпните електронно съобщителни услуги, също така и съобщенията, направени чрез използване на високотехнологични услуги (например мобилни приложения).

Съгласно правото на Съвета на Европа задължението за поверителност е включено в понятието за сигурност на данните в член 7, параграф 1 от модернизираната Конвенция № 108, в който се разглежда сигурността на данните.

За обработващите лични данни поверителността означава, че те не може да разкриват данните на трети страни или на други получатели без разрешение. Поради съображения за поверителност от служителите на администратора или на обработващия лични данни се изисква да използват личните данни само в съответствие с инструкциите на своите компетентни висшестоящи.

Задължението за поверителност трябва да бъде включено във всички договори между администраторите и съответните обработващи лични данни. Освен това администраторите и обработващите лични данни ще трябва да вземат конкретни мерки за въвеждане на правно задължение за поверителност по отношение на своите служители, което обикновено се осъществява чрез включването на клаузи за поверителност в трудовия договор на служителя.

450 Директива за правото на неприкосновеност на личния живот и електронни комуникации, член 5, параграф 1.

451 *Пак там*, член 15, параграф 1.

Нарушаването на професионалните задължения за поверителност е наказуемо съгласно наказателното право в много държави членки на ЕС и страни по Конвенция № 108.

4.2.3 Уведомления за нарушения на сигурността на личните данни

Под нарушение на сигурността на лични данни се има предвид нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна или неразрешено разкриване или достъп до обработваните лични данни[452]. Въпреки че новите технологии, като например криптиране, вече осигуряват повече възможности за гарантиране на сигурността на обработването, нарушенията на сигурността на данните продължават да са често явление. Причините за нарушенията на сигурността на данните могат да варират от случайни грешки на хора, работещи в организацията, до външни заплахи, като хакери и организации за компютърни престъпления.

Нарушенията на сигурността на данните могат да въздействат много неблагоприятно върху правата на неприкосновеност на личния живот и на защита на данните на лицата, които в резултат на нарушението губят контрол върху личните си данни. Нарушенията могат да доведат до кражба на самоличност или измама с фалшива самоличност, финансови загуби или материални щети, нарушаване на поверителността на личните данни, защитени от професионална тайна, и накърняване на репутацията на субекта на данни. В своите Насоки относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент 2016/679 Работната група по член 29 разяснява, че нарушенията могат да доведат до три вида въздействие върху личните данни: разкриване, загуба и/или промяна[453]. В допълнение към задължението да се вземат мерки за гарантиране на сигурността на обработването, както е описано в раздел 4.2, също толкова важно е да се гарантира, че при възникване на нарушения на сигурността администраторите ще ги овладеят по подходящ и навременен начин.

452 Общ регламент относно защитата на данните, член 4, параграф 12; вж. също Работна група по член 29 (2017 г.), *Насоки относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент* 2016/679, WP 250, 3 октомври 2017 г., стр. 8.

453 Работна група по член 29 (2017 г.), *Насоки относно уведомленията за нарушения на сигурността на личните данни съгласно Регламент* 2016/679, WP 250, 3 октомври 2017 г., стр. 6.

Надзорните органи и физическите лица често не знаят, че е възникнало нарушение на сигурността на данните, и това пречи на лицата да предприемат действия, за да се защитят от неговите отрицателни последици. За да се утвърдят правата на физическите лица и да се ограничи въздействието на нарушенията на сигурността на данните, **ЕС и Съветът на Европа** налагат на администраторите изискване за уведомяване при определени обстоятелства.

Съгласно модернизираната Конвенция №108 на **Съвета на Европа** страните по нея трябва най-малкото да изискват от администраторите да уведомяват компетентния надзорен орган за нарушенията на сигурността на данните, които могат да доведат до сериозна намеса в правата на субектите на данни. Това уведомление трябва да бъде подадено „без забавяне“[454].

В **правото на ЕС** е установен подробен режим, който урежда сроковете и съдържанието на уведомленията[455]. Съответно администраторите трябва да уведомят надзорните органи за определени нарушения на сигурността на данните без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като са разбрали за нарушението. Ако не спазят 72-часовия срок, уведомлението трябва да бъде придружено от обяснение за забавянето. Администраторите са освободени от задължението за уведомяване само ако са в състояние да докажат, че няма вероятност нарушението на сигурността на данните да доведе до риск за правата и свободите на засегнатите лица.

В регламента е определена минималната информация, която трябва да бъде включена в уведомлението, за да може надзорният орган да предприеме необходимото действие[456]. Уведомлението трябва да включва най-малко описание на естеството на нарушението на сигурността на личните данни и на категориите и приблизителния брой на засегнатите субекти на данни, описание на евентуалните последици от нарушението и на предприетите от администратора мерки за справяне с нарушението и за намаляване на последиците от него. Освен това следва да се посочат името и координатите за връзка на длъжностното лице по защита на данните или друга точка за контакт, така че компетентният надзорен орган да може да получи при необходимост допълнителна информация.

454 Модернизирана Конвенция № 108, член 7, параграф 2; Обяснителен доклад към модернизираната Конвенция № 108, параграфи 64—66.

455 Общ регламент относно защитата на данните, член 33 и член 34.

456 *Пак там*, член 33, параграф 3.

Ако има вероятност нарушението да причини висок риск за правата и свободите на лицата, администраторите трябва да информират тези лица (субектите на данни) относно нарушението без ненужно забавяне[457]. Съобщението до субектите на данните, включително описанието на нарушението на сигурността на личните данни, трябва да бъде изготвено на ясен и прост език и да включва информация, подобна на тази, която се изисква за уведомленията до надзорните органи. При определени обстоятелства администраторите може да бъдат освободени от задължението да уведомят субектите на данни за тези нарушения. Изключенията се прилагат, когато администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране. Предприетите от администратора действия след нарушението, за да гарантира, че вредата спрямо правата на субектите на данни вече няма да се материализира, също могат да го освободят от задължението да уведоми субектите на данни. Накрая, ако уведомяването изисква несъразмерно големи усилия от страна на администратора, субектите на данни могат да бъдат информирани за нарушението чрез други средства, като например публично съобщение или подобни мерки[458].

Задължението за уведомяване на надзорните органи и субектите на данни относно нарушения на сигурността на данните е насочено към администраторите. Нарушения на сигурността на данните обаче могат да възникнат без значение дали обработването се извършва от администратор или от обработващ лични данни. По тази причина е важно да се гарантира, че обработващите лични данни също са задължени да докладват за нарушения на сигурността на данните. В този случай обработващите лични данни трябва да уведомят администратора за нарушенията на сигурността на данните без ненужно забавяне[459]. След това администраторът носи отговорността за уведомяване на надзорните органи и засегнатите субекти на данни в съответствие с посочените по-горе правила и срокове.

457 *Пак там*, член 34.

458 *Пак там*, член 34, параграф 3, буква в).

459 *Пак там*, член 33, параграф 2.

4.3 Правила за отчетност и насърчаване на спазването

Ключови въпроси

- За да се гарантира отчетността в хода на обработването на лични данни, администраторите и обработващите лични данни трябва да поддържат регистри на дейностите по обработване, за чието извършване отговарят, и да ги предоставят на надзорните органи при поискване.
- В Общия регламент относно защитата на данните се посочват няколко инструмента за насърчаване на спазването на разпоредбите:
  - назначаването на длъжностно лице по защита на данните в определени ситуации;
  - извършването на оценка на въздействието преди започването на дейности по обработването, които има вероятност да поставят под висок риск правата и свободите на лицата;
  - предварителна консултация със съответния надзорен орган, ако оценката на въздействието покаже, че обработването създава рискове, които не могат да бъдат ограничени;
  - кодекси за поведение за администраторите и обработващите лични данни, в които се определя как се прилагат правилата в различните обработващи данни сектори;
  - механизми за сертифициране, печати и маркировки.
- Правото на Съвета на Европа предлага подобни инструменти за насърчаване на спазването на разпоредбите в модернизираната Конвенция № 108.

Принципът на отчетност е особено важен, за да се гарантира прилагането на правилата за защита на данните в Европа. Администраторът носи отговорност и трябва да е в състояние да докаже спазването на правилата за защита на данните. Отчетността не следва да се прилага едва след като възникне нарушение. Администраторите по-скоро имат активно задължение да следват подходящи политики за управление на данните на всички етапи от обработването им. Европейското право в областта на защитата на данните изисква от администраторите да прилагат технически и организационни мерки, за да гарантират и да са в състояние да докажат, че обработването се извършва в съответствие със закона. Сред тези мерки са назначаването на длъжностни

лица по защита на данните, поддържането на регистри и документация във връзка с обработването и извършването на оценки на въздействието върху неприкосновеността на личния живот.

4.3.1 Длъжностни лица по защита на данните

Длъжностните лица по защита на данните (ДЛЗД) са лица, които предоставят съвети относно спазването на правилата за защита на данните в организациите, извършващи обработване на данни. Те са „крайъгълен камък на отчетността", тъй като подпомагат спазването на правилата, като същевременно действат като посредници между надзорните органи, субектите на данни и организациите, които са ги назначили.

Съгласно **правото на Съвета на Европа**, член 10, параграф 1 от модернизираната Конвенция № 108, администраторите и обработващите лични данни носят обща отговорност за отчетността. Това изисква администраторите и обработващите лични данни да предприемат всички подходящи мерки за спазването на правилата за защита на данните, предвидени в конвенцията, и да са в състояние да докажат, че обработването на данни под техен контрол съответства на разпоредбите на конвенцията. Макар и в конвенцията да не се уточняват конкретните мерки, които администраторите и обработващите лични данни следва да приемат, в Обяснителния доклад към модернизираната Конвенция № 108 се посочва, че назначаването на длъжностно лице по защита на данните е една от възможните мерки за доказване на спазването на правилата. На длъжностните лица по защита на данните следва да се предоставят всички необходими средства за изпълнението на техния мандат[460].

За разлика от правото на Съвета на Европа, **в ЕС** назначаването на длъжностно лице по защита на данните не винаги е по усмотрение на администраторите и обработващите лични данни, а е задължително при определени условия. В ОРЗД се признава ключовата роля на длъжностното лице по защита на данните в новата система на управление и са включени подробни разпоредби относно неговото назначаване, длъжност, задължения и задачи[461].

Съгласно ОРЗД назначаването на длъжностно лице по защита на данните е задължително в три специални случая: когато обработването се извършва

460 Обяснителен доклад към модернизираната Конвенция 108, параграф 87.

461 Общ регламент относно защитата на данните, членове 37—39.

от публичен орган или структура; когато основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни; или когато основните дейности се състоят в мащабно обработване на специални категории данни или на лични данни, свързани с присъди и нарушения[462]. Въпреки че в регламента не е дадено определение на термини като „систематично мащабно наблюдение“ и „основни дейности“, Работната група по член 29 публикува насоки относно начина, по който те следва да се тълкуват[463].

Пример: Дружествата в областта на социалните медии и интернет търсачките е вероятно да бъдат считани за администратори, чиито операции по обработване изискват редовно и систематично мащабно наблюдение на субектите на данни. Бизнес моделът на тези дружества се основава на обработването на големи количества лични данни и те реализират значителен приход от предлагането на целеви рекламни услуги и от предоставянето на възможност на дружествата да публикуват реклами на техните сайтове. Целевата реклама е начин за публикуване на реклами въз основа на демографски данни и на предишното пазаруване или поведение на потребителя. Следователно тя изисква систематично наблюдение на поведението и навиците на субектите на данни в интернет пространството.

Пример: Болниците и здравноосигурителните дружества са типични примери за администратори, чиито дейности се състоят в мащабно обработване на специални категории лични данни. Данните, разкриващи информация за здравословното състояние на дадено лице, представляват специални категории лични данни както съгласно правото на ЕС, така и съгласно правото на Съвета на Европа, поради което им се полага повишена защита. Правото на ЕС признава и генетичните и биометричните данни за специални категории данни. Ако медицинските заведения и застрахователните дружества обработват такива данни в голям мащаб, съгласно ОРЗД те са длъжни да назначат длъжностно лице по защита на данните.

462 *Пак там*, член 37, параграф 1.

463 Работна група по член 29 (2017 г.), *Насоки относно длъжностните лица по защита на данните*, WP 243, rev.01, редактирани за последен път и приети на 5 април 2017 г.

Също така член 37, параграф 4 от ОРЗД предвижда, че в случаи, различни от трите задължителни случая, посочени в член 37, параграф 1, администраторът или обработващият лични данни или сдружения и други структури, представляващи категории администратори или обработващи лични данни, могат да определят или — ако това се иска от правото на Съюза или право на държава членка — определят длъжностно лице по защита на данните.

Всички останали организации не са задължени по закон да определят длъжностно лице по защита на данните. ОРЗД обаче предвижда, че администраторите и обработващите лични данни могат да решат да определят доброволно длъжностно лице по защита на данните, като същевременно на държавите членки се дава възможността да направят това да бъде задължително за повече видове организации, отколкото е предвидено в регламента[464].

След като администраторите веднъж са назначили длъжностно лице по защита на данните, те трябва да гарантират, че то „участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни" в рамките на организацията[465]. Например длъжностните лице по защита на данните следва да участват в предоставянето на консултации относно извършването на оценки на въздействието върху защитата на данните, както и в създаването и воденето на дневници на дейностите по обработване в съответната организация. За да дадат възможност на длъжностните лица по защита на данните да изпълняват ефективно техните задачи, администраторите и обработващите лични данни трябва да им осигурят всички необходими ресурси, включително финансови средства, инфраструктура и оборудване. Допълнителните изисквания включват предоставяне на достатъчно време на длъжностните лица по защита на данните за изпълнение на техните функции и непрекъснато обучение, за да им се даде възможност да развиват експертния си опит и да са в крак с всички промени в законодателството за защита на данните[466].

ОРЗД предвижда няколко основни гаранции, за да се осигури независимост на длъжностните лица по защита на данните в техните действия. Администраторите и обработващите лични данни трябва да гарантират, че при

464 Общ регламент относно защитата на данните, член 37, параграфи 3 и 4.

465 *Пак там*, член 38, параграф 1.

466 Работна група по член 29 (2017 г.), *Насоки относно длъжностните лица по защита на данните*, WP 243, rev.01, редактирани за последен път и приети на 5 април 2017 г., параграф 3.1.

изпълнение на задачите им, свързани с обработване на данни, длъжностните лица по защита на данните не получават никакви указания от дружеството, включително от лицата на най-висшето ръководно ниво. Освен това те не трябва да бъдат освобождавани от длъжност, нито санкционирани по какъвто и да било начин за изпълнението на техните задачи[467]. Да разгледаме например случай, в който длъжностното лице по защита на данните препоръчва на администратора или на обработващия лични данни да извърши оценка на въздействието върху защитата на данните, защото счита, че обработването има вероятност да породи висок риск за субектите на данни. Дружеството не е съгласно със съвета на длъжностното лице по защита на данните, не го счита за основателен и поради това решава да не извършва оценка на въздействието. Дружеството може да пренебрегне съвета, но не може да освободи от длъжност или да санкционира длъжностното лице по защита на данните за това, че го е дало.

На последно място, задачите и задълженията на длъжностните лица по защита на данните са подробно определени в член 39 от ОРЗД. Те включват изисквания към длъжностното лице да информира и съветва дружествата и служителите, които извършват обработването, за техните задължения по силата на законодателството и да наблюдава спазването на европейските и националните правила за защита на данните чрез извършване на одити и обучение на персонала, участващ в операциите по обработване. Длъжностните лица по защита на данните трябва също така да си сътрудничат с надзорния орган и да му служат като точка за контакт по въпроси, свързани с обработването на лични данни, като например нарушения на сигурността на данните.

Що се отнася до личните данни, обработвани от институциите и структурите на ЕС, Регламент № 45/2001 предвижда, че всяка институция и структура на Съюза трябва да назначи длъжностно лице по защита на данните. На длъжностните лица по защита на данните е възложено да гарантират, че разпоредбите на регламента се прилагат правилно в рамките на институциите и структурите на ЕС и че както субектите на данни, така и администраторите на лични данни са информирани за техните права и задължения[468]. Те също така са задължени да отговарят на запитванията на ЕНОЗД и да си сътрудничат с него

467 Общ регламент относно защитата на данните, член 38, параграфи 2 и 3.

468 Вж. член 24, параграф 1 от Регламент (ЕО) № 45/2001 относно пълния списък със задачи на длъжностните лица по защита на данните.

при необходимост. Подобно на ОРЗД, Регламент № 45/2001 съдържа разпоредби относно независимостта на длъжностните лица по защита на данните при изпълнението на техните задачи, както и относно необходимостта да им бъдат предоставени необходимите ресурси и персонал[469]. Длъжностните лица по защита на данните трябва да бъдат уведомени, преди съответната институция или структура на ЕС (или техен отдел) да извърши каквито и да било операции по обработване, като са длъжни да водят регистър на всички операции по обработване, за които са уведомени[470].

4.3.2 Регистри на дейностите по обработване

Дружествата често са длъжни по закон да документират и записват дейностите си, за да могат да докажат, че спазват правилата, и да може да им се търси отговорност. Важен пример за това са данъчното законодателство и одитите, които изискват от всички дружества да поддържат подробна документация и отчетност. Въвеждането на подобни изисквания в други области на правото, по-специално в правото в областта на защитата на данните, също е важно, тъй като отчетността е важен начин да се улесни спазването на правилата за защита на данните. Затова в **правото на ЕС** се предвижда, че администраторите или техните представители трябва да поддържат регистър на дейностите по обработване, за чието извършване отговарят[471]. Целта на това задължение е да се гарантира, че при необходимост надзорните органи ще разполагат с необходимата документация, за да могат да потвърдят законосъобразността на обработването.

Информацията, която трябва да бъде документирана, включва:

- името и координатите за връзка на администратора и на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;
- целите на обработването;
- описание на категориите субекти на данни и на категориите лични данни, свързани с обработването;

469 Регламент (ЕО) № 45/2001, член 24, параграфи 6 и 7.

470 *Пак там*, членове 25 и 26.

471 Общ регламент относно защитата на данните, член 30.

- информация относно категориите получатели, пред които са или ще бъдат разкрити личните данни;

- информация дали е било или ще бъде извършено предаване на лични данни на трети държави или международни организации;

- когато е възможно, предвидените срокове за заличаване на различните категории лични данни, както и преглед на приетите технически мерки за гарантиране на сигурността на обработването[472].

Задължението за водене на регистър на дейностите по обработване съгласно ОРЗД засяга не само администраторите, но и обработващите лични данни. Това е важна промяна, тъй като преди приемането на регламента договорът, сключван между администратора и обработващия лични данни, уреждаше предимно задълженията на обработващия лични данни. Понастоящем тяхното задължение за водене на регистър е пряко предвидено по закон.

В ОРЗД се предвижда изключение от това задължение. Изискването за поддържане на регистър не се прилага по отношение на предприятие или дружество (администратор или обработващ лични данни) с по-малко от 250 служители. За да е приложимо изключението обаче, трябва да бъдат изпълнени изискванията дружеството да не извършва обработване, което има вероятност да породи риск за правата и свободите на субектите на данни, обработването да е спорадично и да не включва специални категории данни по член 9, параграф 1 или лични данни, свързани с присъди и нарушения по член 10.

Поддържането на регистър на дейностите по обработване дава възможност на администраторите и обработващите лични данни да докажат, че спазват регламента. То също така следва да дава възможност на надзорните органи да упражняват контрол върху законосъобразността на обработването. Когато надзорен орган поиска достъп до този регистър, администраторите и обработващите лични данни са длъжни да съдействат и да го предоставят.

472 *Пак там*, член 30, параграф 1.

4.3.3 Оценка на въздействието върху защитата на данните и предварителни консултации

Операциите по обработване създават някои присъщи рискове за правата на лицата. Личните данни могат да бъдат загубени, разкрити на неупълномощени страни или обработени незаконно. Естествено, рисковете се различават в зависимост от естеството и обхвата на обработването. Мащабните операции, които включват обработване на чувствителни данни например, носят много по-висок риск за субектите на данни в сравнение с възможните рискове, когато малко дружество обработва адресите и личните телефонни номера на своите служители.

Тъй като се появяват нови технологии и обработването става все по-сложно, администраторите трябва да преодолеят тези рискове, като проучват възможното въздействие, което ще окаже планираното обработване, преди да започнат операциите по него. Това дава възможност на дружествата правилно да установят, преодолеят и ограничат рисковете предварително, като значително намалят вероятността за отрицателно въздействие върху лицата в резултат на обработването.

Извършването на оценки на въздействието върху защитата на данните е предвидено **както в правото на Съвета на Европа, така и в правото на ЕС**. В правната рамка на Съвета на Европа член 10, параграф 2 от модернизираната Конвенция № 108 изисква страните по нея да гарантират, че администраторите и обработващите лични данни „проучват вероятното въздействие на планираното обработване на данни върху правата и основните свободи на субектите на данни, преди да започнат това обработване“ и след оценката проектират обработването по такъв начин, че да предотвратят или сведат до минимум рисковете, свързани с него.

В правото на ЕС се налага сходно, по-детайлно задължение на администраторите, което попада в обхвата на ОРЗД. В член 35 се предвижда, че трябва да се извърши оценка на въздействието, когато има вероятност обработването да доведе до висок риск за правата и свободите на лицата. В регламента не е определено как трябва да се оценява вероятността от настъпване на риска, а по-скоро се посочва какви биха могли да бъдат тези рискове[473]. Той съдържа списък на операциите по обработване, за които се счита, че създават висок

473 Общ регламент относно защитата на данните, съображение 75.

риск и за които е особено необходимо да се извърши предварителна оценка на въздействието, а именно в случаите, когато:

- личните данни се обработват с цел вземане на решения относно физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица (профилиране);

- се извършва мащабно обработване на чувствителни данни или лични данни, свързани с присъди и нарушения;

- обработването включва широкомащабно, систематично наблюдение на публично достъпни зони.

Надзорните органи трябва да приемат и публикуват списък на видовете операции по обработване, за които се изисква оценка на въздействието. Те може също така да съставят списък на операциите по обработване, освободени от това задължение[474].

Когато се изисква оценка на въздействието, администраторите трябва да оценят необходимостта и пропорционалността на обработването и възможните рискове за правата на лицата. Оценката на въздействието трябва да съдържа и планираните мерки за сигурност с цел преодоляване на установените рискове. За съставянето на списъците надзорните органи на държавите членки трябва да сътрудничат помежду си и с Европейския комитет по защита на данните. Това ще гарантира последователен подход в целия ЕС по отношение на тези операции, които изискват оценка на въздействието, и еднакви изисквания към администраторите, независимо от местоположението им.

Ако след оценката на риска изглежда, че обработването ще доведе до висок риск за правата на лицата и не са въведени мерки за ограничаване на риска, администраторът трябва да се консултира със съответния надзорен орган преди започване на операциите по обработване[475].

474 *Пак там*, член 35, параграфи 4 и 5.

475 *Пак там*, член 36, параграф 1; Работна група по член 29 (2017 г.), *Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент 2016/679*, WP 248 rev.01, Брюксел, 4 октомври 2017 г.

Работната група по член 29 е издала насоки относно оценката на въздействието върху защитата на данните и начина на определяне дали съществува вероятност обработването да породи висок риск[476]. Тя е разработила девет критерия, за да помогне да се определи дали в конкретен случай се изисква оценка на въздействието върху защитата на данни[477]: 1) оценка или точкуване; 2) автоматизирано вземане на решения с правни последици или подобни сериозни последици; 3) систематично наблюдение; 4) чувствителни данни; 5) мащабно обработване на данни; 6) търсене на съвпадение или съчетаване на набори от данни; 7) данни относно уязвими субекти на данни; 8) иновативно използване или прилагане на нови технологични или организационни решения; 9) операциите по обработването сами по себе си „възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор“. Работната група по член 29 е въвела практическото правило, че операциите по обработване, които отговарят на по-малко от два критерия, представляват по-нисък риск и за тях не се изисква оценка на въздействието върху защитата на данните, докато за тези, които отговарят на два и повече критерия, се изисква такава оценка. В случаите, когато не е ясно дали се изисква ОВЗД, Работната група по член 29 препоръчва все пак да се извърши такава оценка, тъй като тя представлява „полезен инструмент, който помага на администраторите да спазват законодателството в областта на защитата на данните“[478]. Когато се въвежда нова технология на обработване на лични данни, е важно да се извърши оценка на въздействието върху защитата на данните[479].

4.3.4 Кодекси за поведение

Кодексите за поведение са предназначени да бъдат използвани в редица промишлени сектори, за да се очертае и уточни прилагането на ОРЗД в конкретния сектор. За администраторите и обработващите лични данни създаването на такива кодекси може значително да подобри спазването и да засили прилагането на правилата на ЕС за защита на данните. Експертният опит на членовете от сектора ще благоприятства намирането на решения, които са

476 Работна група по член 29 (2017 г.), *Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679*, WP 248 rev.01, Брюксел, 4 октомври 2017 г.

477 *Пак там*, стр. 9—11.

478 *Пак там*, стр. 9.

479 *Пак там*.

практически осъществими и следователно биха могли да бъдат прилагани. Като признава значението на тези кодекси за ефективното прилагане на законодателството за защита на данните, ОРЗД призовава държавите членки, надзорните органи, Комисията и Европейския комитет по защита на данните да насърчават изготвянето на кодекси за поведение, които имат за цел да допринесат за правилното прилагане на регламента в целия ЕС[480]. Кодексите биха могли да уточняват прилагането на регламента в конкретни сектори, включително по въпроси като събирането на лични данни, информацията, която трябва да бъде предоставена на субектите на данни и на обществеността, и упражняването на правата на субектите на данни.

За да се гарантира, че кодексите за поведение съответстват на установените в ОРЗД правила, те трябва да бъдат представени на компетентния надзорен орган, преди да бъдат приети. След това надзорният орган дава становище дали представения проект на кодекс благоприятства спазването на регламента и ако установи, че кодексът осигурява подходящи гаранции, го одобрява[481]. Надзорните органи трябва да публикуват одобрените кодекси за поведение, както и критериите, въз основа на които са ги одобрили. Ако проект на кодекс за поведение има отношение към дейности по обработване в няколко държави членки, компетентният надзорен орган, преди одобряването на проекта на кодекс, негово изменение или допълнение, представя кодекса на Европейския комитет по защита на данните, който дава становище относно съответствието на кодекса с ОРЗД. Комисията може чрез актове за изпълнение да реши дали одобреният кодекс за поведение, който ѝ е представен, е общовалиден в рамките на Съюза.

Придържането към кодекс за поведение предоставя важни предимства както на субектите на данни, така и на администраторите и обработващите лични данни. Тези кодекси предоставят подробни насоки, които адаптират правните изисквания към конкретни сектори и подпомагат прозрачността на дейностите по обработване. Придържането към кодексите от страна на администраторите и обработващите лични данни може също така да бъде използвано като доказателство за това, че те спазват законодателството на ЕС, и като средство за утвърждаване на публичния им образ като организации, които отдават предимство и се ангажират със защитата на данните в техните действия. Одобрените кодекси за поведение, заедно със задължителни и изпълними

480 Общ регламент относно защитата на данните, член 40, параграф 1.

481 *Пак там*, член 40, параграф 5.

ангажименти, могат да се използват като подходящи гаранции за прехвърлянето на данни към трети държави. За да се гарантира, че организациите, които се придържат към кодексите за поведение, наистина ги спазват, може да бъде назначен специален орган (акредитиран от съответния надзорен орган), който да наблюдава и гарантира спазването им. За да изпълнява ефективно задачите си, органът трябва да е независим, да има доказан експертен опит по въпросите, които са уредени в кодекса за поведение, и да има прозрачни процедури и структури, които да му позволяват да разглежда жалби относно нарушаването на кодекса[482].

Съгласно **правото на Съвета на Европа** в модернизираната Конвенция № 108 се предвижда, че нивото на защита на данните, гарантирано от националното законодателство, може реално да бъде повишено чрез доброволни регулаторни мерки, като например кодекси за добра практика или кодекси за професионално поведение. Те обаче са само доброволни мерки по модернизираната Конвенция № 108: няма никакво правно задължение за въвеждането на такива мерки, въпреки че е препоръчително, а такива мерки сами по себе си не са достатъчни, за да се гарантира пълно спазване на конвенцията[483].

4.3.5 Сертифициране

Други средства освен кодексите за поведение, чрез които администраторите и обработващите лични данни могат да докажат спазването на ОРЗД, са механизмите за сертифициране и печатите и маркировките за защита на данните. За тази цел в регламента се предвижда система за доброволно сертифициране, чрез която определени структури или надзорни органи могат да издават сертификати. Администраторите и обработващите лични данни, които са избрали да се придържат към механизъм за сертифициране, могат да спечелят повече видимост и доверие, тъй като сертификатите, печатите и маркировките дават възможност на субектите на данни бързо да оценят нивото на защита на обработваните данни от организацията. Важно е да се отбележи, че фактът, че администраторът или обработващият лични данни притежават такъв сертификат, не намалява техните задължения и отговорности да спазват всички изисквания на регламента.

482 *Пак там*, член 41, параграфи 1 и 2.

483 Обяснителен доклад към модернизираната Конвенция 108, параграф 33.

4.4 Защита на данните на етапа на проектирането и по подразбиране

Защита на данните на етапа на проектирането

В **правото на ЕС** се изисква администраторите да въведат мерки за ефективно прилагане на принципите за защита на данните и да интегрират необходимите гаранции, за да се спазят изискванията на регламента и да се защитят правата на субектите на данни[484]. Тези мерки следва да се прилагат както по време на обработването, така и при определянето на средствата за обработване. При прилагането на тези мерки администраторът трябва да вземе предвид достиженията на техническия прогрес, разходите за прилагане, естеството, обхвата и целите на обработването на личните данни, както и рисковете и тяхната тежест за правата и свободите на субектите на данни[485].

Съгласно **правото на Съвета на Европа** администраторите и обработващите лични данни трябва да оценят вероятния ефект на обработването върху правата и свободите на субектите на данни, преди да го започнат. Освен това администраторите и обработващите лични данни са длъжни да проектират обработването на данни по такъв начин, че да предотвратят или да сведат до минимум риска от намеса в тези права и свободи и да въведат технически и организационни мерки, съобразени с последиците върху правото на защита на личните данни на всички етапи от обработването[486].

Защита на данните по подразбиране

Съгласно **правото на ЕС** администраторът трябва да въведе подходящи мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за целите на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването,

484 Общ регламент относно защитата на данните, член 25, параграф 1.

485 Вж. Работна група по член 29 (2017 г.), *Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679*, WP 248 rev.01, 4 октомври 2017 г. Вж. също ENISA (2015 г.), Защита на неприкосновеността на личния живот и на данните още на етапа на проектирането – от политиката до инженерството, 12 януари 2015 г.

486 Модернизирана Конвенция № 108, член 10, параграфи 2 и 3, Обяснителен доклад към модернизираната Конвенция № 108, параграф 89.

периода на съхраняването им и тяхната достъпност[487]. Тази мярка трябва да гарантира например, че не всички служители на администратора имат достъп до личните данни на субектите. ЕНОЗД е разработил допълнителни насоки в *Инструментариума за оценяване на необходимостта от мерки, които ограничават основното право на защита на личните данни* (*Necessity Toolkit*)[488].

Съгласно **правото на Съвета на Европа** администраторите и обработващите лични данни трябва да прилагат технически и организационни мерки, за да се вземат предвид последиците от правото на защита на данните и да въведат технически и организационни мерки, съобразени с последиците върху правото на защита на личните данни на всички етапи от обработването[489].

През 2016 г. ENISA публикува доклад за съществуващите инструменти и услуги в областта на зачитането на неприкосновеността на личния живот[490]. Наред с другото в тази оценка се представя списък с критериите и параметрите, които са показатели за добри или лоши практики. Докато някои от критериите са пряко свързани с разпоредбите на ОРЗД — като например използването на псевдонимизация и на одобрени механизми за сертифициране, други осигуряват новаторски инициативи за гарантиране на неприкосновеността на личния живот на етапа на проектирането и по подразбиране. Например критерият за използваемост, макар и да не е пряко свързан с неприкосновеността на личния живот, може да я подобри, тъй като може да даде възможност за по-широко въвеждане на инструменти или услуги в областта на зачитането на неприкосновеността на личния живот. Всъщност инструментите, чието практическо приложение е трудно, може да бъдат приети много слабо от широката общественост, дори и да предлагат много силни гаранции за неприкосновеността на личния живот. Освен това критерият за зрялост и стабилност на инструмента за неприкосновеност на личния живот — тоест начинът, по който той се развива във времето и отговаря на съществуващите или на новите предизвикателства, свързани с неприкосновеността на личния живот — е от особена важност. Сред другите технологии за подобряване на

487 Общ регламент относно защитата на данните, член 25, параграф 2.

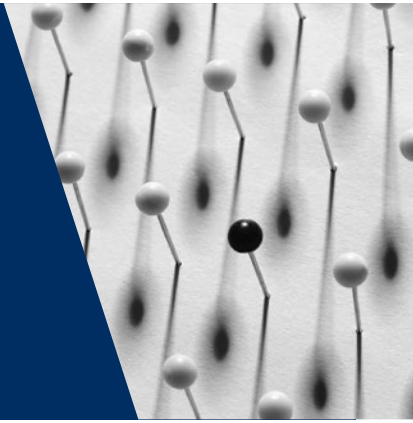
488 Европейски надзорен орган по защита на данните (ЕНОЗД) (2017 г.), *Necessity Toolkit*, Брюксел, 11 април 2017 г.

489 Модернизирана Конвенция № 108, член 10, параграф 3, Обяснителен доклад към модернизираната Конвенция № 108, параграф 89.

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 декември 2016 г.

неприкосновеността на личния живот, например в контекста на сигурността на съобщенията, са цялостно криптиране (комуникация, при която комуникиращите си лица са единствените, които могат да четат съобщенията); криптиране клиент-сървър (криптиране на комуникационния канал, установен между клиента и сървъра); автентификация (проверка на самоличността на комуникиращите си страни); и анонимна комуникация (самоличността на комуникиращите си страни не може да бъде установена от трета страна).

5 Независим надзор



ЕС	Обхванати въпроси	СЕ
Хартата, член 8, параграф 3 Договор за функционирането на Европейския съюз, член 16, параграф 2 Общ регламент относно защитата на данните, членове 51—59 Съд на ЕС, C-518/07, *Европейска комисия/Федерална република Германия* [голям състав], 2010 г. Съд на ЕС, C-614/10, *Европейска комисия/Република Австрия* [голям състав], 2012 г. Съд на ЕС, C-288/12, *Европейска комисия/Унгария* [голям състав], 2014 г. Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 2015 г.	**Надзорни органи**	Модернизирана Конвенция № 108, член 15
Общ регламент относно защитата на данните, членове 60—67	**Сътрудничество между надзорните органи**	Модернизирана Конвенция № 108, членове 16—21
Общ регламент относно защитата на данните, членове 68—76	**Европейски комитет по защита на данните**	

Ключови въпроси

- Независимият надзор е съществен елемент от европейското право в областта на защитата на данните и е залегнал в член 8, параграф 3 от Хартата.
- За да се гарантира ефективна защита на данните, националното законодателство трябва да предвижда създаването на независими надзорни органи.
- Надзорните органи трябва да действат напълно независимо, което трябва да бъде гарантирано от учредителния акт и да намира отражение в специфичната организационна структура на надзорния орган.
- Надзорните органи имат конкретни правомощия и задачи. Те включват, наред с другото:
  - да наблюдават и насърчават защитата на данните на национално равнище;
  - да съветват субектите на данни и администраторите, както и правителството и обществеността като цяло;
  - да изслушват жалбите и да помагат на субектите на данни при твърдения за нарушения на правата, свързани със защитата на данните;
  - да упражняват надзор над администраторите и обработващите лични данни;
- Надзорните органи имат също и правомощия да се намесват при необходимост, като:
  - отправят предупреждение, строга забележка и дори глобяват администраторите и обработващите лични данни;
  - разпореждат коригиране, блокиране или заличаване на данни;
  - налагат забрана за обработване или административна глоба;
  - да сезират съда по конкретни случаи.
- Тъй като обработването на лични данни често включва администратори, обработващи лични данни и субекти на данни, разположени в различни държави, надзорните органи трябва да си сътрудничат по трансграничните въпроси, за се гарантира ефективната защита на физическите лица в Европа.

- В рамките на ЕС Общият регламент относно защитата на данните установява механизъм „обслужване на едно гише“ за случаите на трансгранично обработване. Някои дружества извършват дейности по трансгранично обработване, защото обработването на лични данни се извършва в контекста на дейностите на място на установяване в повече от една държава членка или обработването, което се осъществява в контекста на дейностите на едно-единствено място на установяване в Съюза, засяга съществено субекти на данни в повече от една държава членка. Съгласно установения механизъм такива дружества ще трябва да работят само с един национален надзорен орган за защита на данните.

- Наличието на механизъм за сътрудничество и съгласуваност ще осигури възможност за координиран подход между всички надзорни органи, замесени в съответния случай. Водещият надзорен орган — този на основното или на единственото място на установяване — дава мнението си и представя проекторешенията си на другите засегнати надзорни органи.

- Подобно на настоящата Работна група по член 29, надзорният орган на всяка държава членка и Европейският надзорен орган по защита на данните (ЕНОЗД) ще бъдат част от Европейския комитет по защита на данните.

- Задачите на Европейския комитет по защита на данните включват например наблюдение на правилното прилагане на регламента, консултиране на Комисията по свързани въпроси и издаване на становища, насоки или най-добри практики по множество теми.

- Основната разлика е, че Европейския комитет по защита на данните издава не само становища, както е съгласно Директива 95/46/ЕО. Той приема и решения със задължителен характер относно случаите, когато надзорен орган е повдигнал относимо и обосновано възражение в случаите на обслужване на едно гише, когато има противоречиви виждания за това кой от надзорните органи е водещият и, последно, когато компетентният надзорен орган не е поискал становището на ЕКЗД или не се е съобразил с него. Целта е да се осигури последователно прилагане на регламента във всички държави членки.

Независимият надзор е съществен елемент от европейското право в областта на защитата на данните. Както в правото на ЕС, така и в правото на Съвета на Европа наличието на независими надзорни органи се счита за крайно необходимо за ефективната защита на правата и свободите на физическите лица, що се отнася до обработването на личните им данни. Тъй като обработването на данни вече е неотменима част от съвременния живот и става все по-трудноразбираемо за физическите лица, тези органи са стражите на цифровата ера. В ЕС наличието на независими надзорни органи се счита за един от най-важните елементи на правото на защита на личните данни, което е залегнало в първичното законодателство на ЕС. В член 8, параграф 3 от Хартата на основните права на ЕС и в член 16, параграф 2 от ДФЕС защитата на личните

данни се признава за основно право и се утвърждава, че спазването на правилата за защита на данните трябва да бъде предмет на контрол от независим орган.

Значението на независимия надзор за правото в областта на защитата на данните се признава и в съдебната практика.

Пример: По делото *Schrems*[491] Съдът на ЕС разглежда въпроса дали изпращането на лични данни към Съединените щати (САЩ) съгласно първото Споразумение относно неприкосновеността на личните данни между ЕС и САЩ е в съответствие с правото на ЕС в областта на защитата на данните предвид разкритията на Едуард Сноудън относно провеждането на масово наблюдение от страна на Агенцията за национална сигурност на САЩ. Личните данни са били предавани към САЩ въз основа на решение на Европейската комисия, прието през 2000 г., което допуска предаването на лични данни от ЕС на американски организации, които сами са се сертифицирали по схемата за „сфера на неприкосновеност на личния живот", въз основа на това, че схемата гарантира достатъчна степен на защита на личните данни. Когато от ирландския надзорен орган е било поискано да проведе разследване по жалбата на жалбоподателя относно законосъобразността на предаването на данни след разкритията на Сноудън, той отхвърля жалбата на основание, че наличието на решение на Комисията относно адекватността на режима за защита на данните в САЩ, което е отразено в „принципите за сфера на неприкосновеност на личния живот" (Решението относно „сферата на неприкосновеност на личния живот"), възпрепятства по-нататъшното разследване на жалбата.

Съдът на ЕС обаче постановява, че наличието на решение на Комисията, което позволява предаване на данни към трети страни, които гарантират достатъчна степен на защита, не отнема, нито намалява правомощията на националните надзорни органи. Съдът на ЕС отбелязва, че правомощията на тези органи да наблюдават и осигуряват спазването на правилата на ЕС за защита на данните произтичат от първичното право на ЕС, по-специално от член 8, параграф 3 от Хартата и от член 16,

491 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

параграф 2 от ДФЕС. „Учредяването на независими надзорни органи е [...] съществен елемент от осигуряването на защита на лицата при обработването на лични данни.“[492]

Поради това Съдът на ЕС решава, че дори когато предаването на лични данни е предмет на решение на Комисията относно адекватното ниво на защита, при подадена жалба до национален надзорен орган, този орган трябва да я разгледа с цялата дължима грижа. Надзорният орган може да отхвърли жалбата, ако счете, че тя е неоснователна. Съдът на ЕС подчертава, че в такъв случай правото на ефективна съдебна защита изисква физическите лица да могат да оспорят такова решение пред националните юрисдикции, които могат да отправят преюдициално запитване до Съда на ЕС относно валидността на решението на Комисията. Когато надзорният орган счете жалбата за основателна, той трябва да има право да предприеме действия по съдебен ред и да сезира националните юрисдикции. Националните юрисдикции могат да отнесат делото до Съда на ЕС като единствения орган, който има правомощието да се произнесе дали е валидно решението на Комисията относно адекватното ниво на защита[493].

След това Съдът на ЕС разглежда валидността на Решението относно „сферата на неприкосновеност на личния живот“, за да установи дали системата за предаване на данни е в съответствие с правилата на ЕС за защита на данните. Съдът установява, че член 3 от Решението относно „сферата на неприкосновеност на личния живот“ ограничава правомощията на националните надзорни органи (предоставени им съгласно Директивата за защита на личните данни) да предприемат действия за предотвратяване на предаването на данни в случай на недостатъчно ниво на защита на личните данни в САЩ. С оглед на значението на независимите надзорни органи за гарантиране на спазването на законодателството за защита на данните Съдът на ЕС постановява, че съгласно Директивата за защита на личните данни, тълкувана във връзка с Хартата, Комисията не е имала право да ограничава по този начин правомощията на независимите надзорни

492 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г., параграф 41.

493 *Пак там*, параграфи 53–66.

органи. Ограничаването на правомощията на надзорните органи е една от причините, поради които Съдът на ЕС обявява Решението относно „сферата на неприкосновеност на личния живот“ за невалидно.

Поради това европейското законодателство изисква въвеждането на независим надзор като важен механизъм за гарантиране на ефективна защита на личните данни. Независимите надзорни органи са първата точка за контакт за субектите на данни в случай на нарушаване на неприкосновеността на личния им живот[494]. Съгласно правото на ЕС и правото на Съвета на Европа създаването на надзорни органи е задължително. И двете правни рамки определят задачите и правомощията на тези органи по начин, подобен на съдържащия се в ОРЗД. Следователно надзорните органи следва по принцип да функционират по един и същ начин съгласно правото на ЕС и това на Съвета на Европа[495].

5.1 Независимост

В **правото на ЕС** и в **правото на Съвета на Европа** се изисква всеки надзорен орган да действа напълно независимо при изпълнението на задачите си и при упражняването на правомощията си[496]. Независимостта на надзорния орган и на неговите членове и персонал от преки и непреки външни влияния е от основно значение, за да се гарантира пълната му обективност при вземане на решения по въпроси относно защитата на данните. Освен че законът за създаване на надзорен орган трябва да съдържа разпоредби, които изрично да гарантират неговата независимост, организационната структура на институцията също трябва да показва неговата самостоятелност. През 2010 г. Съдът на ЕС за първи път разглежда степента, до която се изисква надзорните органи да бъдат независими[497]. Подчертаните примери показват определението на Съда на ЕС за „пълна независимост“.

494 Общ регламент относно защитата на данните, член 13, параграф 2, буква г).

495 *Пак там*, член 51; модернизирана Конвенция № 108, член 15.

496 Общ регламент относно защитата на данните, член 52, параграф 1; модернизирана Конвенция № 108, член 15, параграф 5.

497 FRA (2010 г.), *„Fundamental rights: challenges and achievements in 2010.“*, Годишен доклад за 2010 г., стр. 59; FRA (2010 г.), *„Data protection in the European Union: the role of National Data Protection Authorities “*, май 2010 г.

Пример: В делото *Европейска комисия/Федерална република Германия*[498] Европейската комисия отправя искане към Съда на ЕС да обяви, че Германия е транспонирала неправилно изискването за „пълна независимост" на надзорните органи, отговорни да гарантират защитата на данните, и по този начин не е изпълнила задълженията си по силата на член 28, параграф 1 от Директивата за защита на личните данни. Според Комисията фактът, че Германия е поставила надзорните органи, които следят обработването на личните данни в различните федерални провинции (*Länder*), под държавен надзор, за да гарантира спазването на законодателството за защита на данните, нарушава изискването за независимост.

Съдът на ЕС подчертава, че думите „с пълна независимост" трябва да се тълкуват въз основа на реалната формулировка на тази разпоредба и в съответствие с целите и механизмите на правото на ЕС в областта на защитата на данните[499]. Съдът на ЕС подчертава, че надзорните органи са „пазители" на правата, свързани с обработването на личните данни. Следователно тяхното създаване в държавите членки се счита за „съществен елемент от защитата на лицата при обработването на лични данни"[500]. Съдът на ЕС заключава, че „при упражняване на техните функции надзорните органи трябва да действат обективно и безпристрастно. За целта те трябва да бъдат предпазени от всяко външно влияние, включително от прякото или косвено влияние от страна на публични органи"[501].

Съдът на ЕС също така приема, че значението на термина „пълна независимост" следва да се тълкува с оглед на независимостта на ЕНОЗД, както е определена в Регламента относно защитата на данните при обработването им от институции на ЕС. В този регламент понятието за независимост изисква ЕНОЗД да не търси и да не получава инструкции от никого.

498 Съд на ЕС, C-518/07, *Европейска комисия/Федерална република Германия* [голям състав], 9 март 2010 г., параграф 27.

499 *Пак там*, параграфи 17 и 29.

500 *Пак там*, параграф 23.

501 *Пак там*, параграф 25.

Съответно Съдът на ЕС постановява, че поради упражнявания от публичните органи надзор, надзорните органи в Германия не са напълно независими по смисъла на правото на ЕС в областта на защитата на данните.

Пример: В делото *Европейска комисия/Република Австрия*[502] Съдът на ЕС посочва наличието на сходни проблеми, свързани с независимостта на някои членове и сътрудници на австрийския орган по защита на данните (Комисията за защита на данните, DSK). Съдът на ЕС заключава, че фактът, че Федералното канцлерство подсигурява персонала на надзорния орган, подкопава изискването за независимост, установено в правото на ЕС в областта на защитата на данните. Съдът също така постановява, че изискването надзорният орган да информира Канцлерството по всяко време относно работата си отрича съществуването на неговата пълна независимост.

Пример: В делото *Европейска комисия/Унгария*[503] са забранени сходни национални практики, които засягат независимостта на персонала. Съдът на ЕС посочва, че „изискването [...] да се гарантира, че всеки надзорен орган упражнява възложените му функции при пълна независимост, включва задължение за съответната държава членка да се съобразява с продължителността на мандата на този орган до изтичането на първоначално предвидения му краен срок“. Съдът също така приема, че „с предсрочното прекратяване на мандата на надзорния орган за защита на личните данни Унгария не е изпълнила задълженията си, произтичащи от Директива 95/46/ЕО [...]“.

Понятието и критериите за „пълна независимост“ понастоящем са изрично предвидени в ОРЗД, който включва принципите, установени чрез описаните решения на Съда на ЕС. Съгласно регламента пълната независимост при изпълнението на задачите и упражняването на правомощията изисква[504]:

502 Съд на ЕС, C-614/10, *Европейска комисия/Република Австрия* [голям състав], 16 октомври 2012 г., параграфи 59 и 63.

503 Съд на ЕС, C-288/12, *Европейска комисия/Унгария* [голям състав], 8 април 2014 г., параграфи 50 и 67.

504 Общ регламент относно защитата на данните, член 52.

- членовете на всеки надзорен орган да остават независими от външно влияние, било то пряко или непряко, и да не приемат инструкции от когото и да било;

- членовете на надзорния орган да се въздържат от всякакви несъвместими със задълженията им действия, за да се предотвратят конфликти на интереси;

- държавите членки да предоставят на всеки надзорен орган необходимите човешки, технически и финансови ресурси и инфраструктура за ефективното изпълнение на неговите задачи;

- държавите членки да гарантират, че всеки надзорен орган избира свой собствен персонал;

- финансовият контрол, на който подлежи всеки надзорен орган в съответствие с националното законодателство, да не засяга неговата независимост. Надзорните органи трябва да имат отделни и публични годишни бюджети, които да им позволяват да работят нормално.

Независимостта на надзорните органи се счита за съществено изискване и съгласно правото на Съвета на Европа. В модернизираната Конвенция № 108 се изисква надзорните органи „да действат напълно независимо и безпристрастно при изпълнението на задачите си и упражняването на правомощията си“, без да търсят или да получават указания[505]. По този начин в конвенцията се признава, че тези органи не могат ефективно да защитят правата и свободите на физическите лица, свързани с обработването на данни, ако не изпълняват функциите си напълно независимо. В Обяснителния доклад към модернизираната Конвенция № 108 се определят редица елементи, които допринасят за гарантирането на тази независимост. Тези елементи включват възможността надзорните органи да наемат свой собствен персонал и да приемат решения, без да бъдат обект на външно влияние, както и фактори, отнасящи се до срока на упражняването на техните функции и условията, при които те могат да ги прекратят[506].

505 Модернизирана Конвенция № 108, член 15, параграф 5.

506 Обяснителен доклад към модернизираната Конвенция № 108.

5.2 Компетентност и правомощия

В рамките на правото на ЕС в ОРЗД са определени компетентностите и организационната структура на надзорните органи, като се предвижда, че те трябва да са компетентни и да имат правомощията да изпълняват задачите, които се изискват съгласно регламента.

Надзорният орган е основната структура в националното право, която гарантира спазването на законодателството на ЕС в областта на защитата на данните. Освен да извършват наблюдение, надзорните органи имат обширен списък от задачи и правомощия, които включват проактивни и превантивни надзорни дейности. За да изпълняват тези задачи, надзорните органи трябва да имат подходящи правомощия за разследване, корективни правомощия и правомощия да дават становища, както те са изброени в членове 57 и 58 от ОРЗД, като например[507]:

- да дават становища на администраторите и субектите на данни по всички въпроси, свързани със защитата на данните;
- да дават разрешение за стандартните договорни клаузи, задължителните фирмени правила или административните договорености;
- да разследват операциите по обработване и да се намесват по подходящ начин;
- да изискват да им бъде предоставена всяка информация, която е от значение за упражняването на надзор на дейностите на администратора;
- да предупреждават или да отправят официално предупреждение до администратора, както и да му разпореждат да съобщава на субекта на данните за нарушение на сигурността на личните данни;
- да разпореждат коригирането, блокирането, изтриването или унищожаването на данни;

507 Общ регламент относно защитата на данните, член 58. Вж. също Конвенция № 108, Допълнителен протокол, член 1.

- да налагат временна или постоянна забрана на обработването на данни или да налагат административно наказание „глоба“ или „имуществена санкция“;

- да сезират съда по конкретни случаи.

За да може да изпълнява задълженията си, надзорният орган трябва да има достъп до всички лични данни и до цялата информация, необходима за провеждане на разследване, както и до помещенията, в които администраторът съхранява съответната информация. Според Съда на ЕС правомощията на надзорния орган трябва да се тълкуват широко, за да се гарантира пълна ефективност на защитата на данните за субектите на данни в ЕС.

Пример: В делото *Schrems* Съдът на ЕС разглежда въпроса дали изпращането на лични данни към САЩ съгласно първото Споразумение относно неприкосновеността на личните данни между ЕС и САЩ е в съответствие с правото на ЕС в областта на защитата на данните предвид разкритията на Едуард Сноудън. В мотивите на Съда на ЕС се посочва, че националните надзорни органи, действащи в качеството си на независими наблюдатели на извършваното от администраторите обработване на данни, могат да предотвратят прехвърлянето на лични данни към трета държава въпреки съществуването на решение относно адекватното ниво на защита, ако е налице основателно доказателство, че адекватното ниво на защита вече не е гарантирано в третата държава[508].

Всеки надзорен орган разполага с правомощия по разследване и с правомощия за намеса в рамките на неговата територия. Тъй като обаче дейностите на администраторите и обработващите лични данни често са трансгранични и обработването на данни засяга субекти на данни, разположени в няколко държави членки, възниква въпросът за разделянето на компетентностите между различните надзорни органи. Съдът на ЕС е имал възможността да разгледа този въпрос в делото *Weltimmo*.

508 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г., параграфи 26–36 и 40–41.

Пример: В делото *Weltimmo*[509] Съдът на ЕС е сезиран относно компетентността на националните надзорни органи да разглеждат въпроси, засягащи организации, които не са под тяхната юрисдикция. Weltimmo е дружество, регистрирано в Словакия, което е оператор на уебсайт за обяви за недвижими имоти на територията на Унгария. Подалите обяви лица подават жалби пред унгарския надзорен орган за нарушение на унгарското законодателство за защита на данните и органът налага имуществена санкция на Weltimmo. Дружеството оспорва имуществената санкция пред националните съдилища и делото е отнесено до Съда на ЕС, за да установи дали Директивата на ЕС за защита на данните позволява на надзорните органи на дадена държава членка да прилагат националното си законодателство за защита на данните по отношение на дружество, регистрирано в друга държава членка.

Съдът на ЕС е дал тълкуване на член 4, параграф 1, буква а) от Директивата за защита на личните данни в смисъл, че той 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“. Съдът на ЕС отбелязва, че въз основа на предоставената му информация Weltimmo осъществява ефективна и действителна дейност в Унгария, тъй като дружеството има представител в Унгария, който е включен в регистъра на словашките дружества с адрес в Унгария, както и банкова сметка и пощенска кутия в Унгария, и също така е осъществявало дейности в Унгария на унгарски език. Тази информация сочи съществуването на постоянен обект и прави дейността на Weltimmo обект на унгарското право за защита на данните и на юрисдикцията на унгарския надзорен орган. Съдът на ЕС обаче оставя на националния съд да провери информацията и да реши дали Weltimmo в действителност има обект в Унгария.

509 Съд на ЕС, C-230/14, *Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 октомври 2015 г.

Ако запитващата юрисдикция установи, че Weltimmo има обект в Унгария, унгарският надзорен орган ще има правомощието да наложи имуществена санкция. Все пак ако националният съд реши обратното, т.е. че Weltimmo няма обект в Унгария, приложимото право следователно ще бъде това на държавата членка, в която дружеството е регистрирано. В този случай, тъй като правомощията на надзорните органи трябва да бъдат упражнявани в съответствие с териториалния суверенитет на другите държави членки, унгарският орган няма да е в състояние да наложи имуществени санкции. Тъй като Директивата за защита на личните данни включва задължение за сътрудничество за надзорните органи, унгарският орган все пак е можел да поиска от словашкия си партньор да разгледа въпроса, да установи нарушение на словашкото законодателство и да наложи санкциите, които са предвидени в словашкото законодателство.

С приемането на ОРЗД вече са въведени подробни правила относно компетентността на надзорните органи в трансгранични случаи. Регламентът създава „механизъм за обслужване на едно гише" и включва разпоредби, с които се налага задължение за сътрудничество на различните надзорни органи. За да бъде ефективно сътрудничеството в трансграничните случаи, в ОРЗД се изисква надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни да действа като водещ надзорен орган[510]. Водещият надзорен орган отговаря за трансграничните случаи и администраторът или обработващият лични данни комуникират единствено с него, а той координира сътрудничеството с другите надзорни органи с оглед на постигането на консенсус. Сътрудничеството включва обмен на информация, предоставяне на взаимопомощ при извършването на наблюдение и разследвания и приемане на задължителни решения[511].

В правото на Съвета на Европа компетентностите и правомощията на надзорните органи са посочени в член 15 от модернизираната Конвенция № 108. Тези правомощия отговарят на предоставените на надзорните органи по правото на ЕС, като включват правомощия за разследване и намеса, правомощия за издаване на решения и налагане на административни санкции относно нарушения на разпоредбите на конвенцията, както и правомощия за

510 Общ регламент относно защитата на данните, член 56, параграф 1.

511 *Пак там,* член 60.

предприемане на действия по съдебен ред. Независимите надзорни органи също така са компетентни да разглеждат искания и жалби, подадени от субектите на данни, да повишават обществената осведоменост относно законодателството за защита на данните и да предоставят становища на вземащите решения на национално равнище по всички законодателни или административни мерки, които предвиждат обработване на лични данни.

5.3 Сътрудничество

С ОРЗД се установява обща рамка за сътрудничество между надзорните органи и се предвиждат по-конкретни правила относно това сътрудничество при трансгранични дейности по обработване на лични данни.

Съгласно ОРЗД надзорните органи си предоставят взаимопомощ и си споделят значима информация, за да изпълняват и прилагат регламента по съгласуван начин[512]. Това включва провеждането на консултации, проверки и разследвания от надзорния орган, до който е отправено искането. Надзорните органи могат да провеждат съвместни операции, включително съвместни разследвания и съвместни мерки за изпълнение, в които участва персоналът на всички надзорни органи[513].

Администраторите и обработващите лични данни в ЕС все повече работят на транснационално ниво. Това изисква тясно сътрудничество между компетентните надзорни органи в държавите членки, за да се гарантира, че обработването на лични данни отговаря на изискванията на ОРЗД. Съгласно въведения с регламента механизъм за „обслужване на едно гише“, ако администратор или обработващ лични данни е установен в няколко държави членки или е установен на едно-единствено място, но операциите по обработването засягат съществено субекти на данни в повече от една държава членка, надзорният орган на основното (или на единственото) място на установяване е водещият орган за трансграничните дейности на администратора или обработващия лични данни. Водещите органи имат правомощието да предприемат правоприлагащи действия срещу администратора или обработващия лични данни. Механизмът за „обслужване на едно гише“ има за цел да подобри хармонизацията и еднаквото прилагане на правото на ЕС в областта на защитата на данните в различните държави членки. Той е от полза и за

512 *Пак там*, член 61, параграфи 1—3 и член 62, параграф 1.

513 *Пак там*, член 62, параграф 1.

предприятията, тъй като те трябва да взаимодействат само с водещия орган, вместо с няколко надзорни органа. Това подобрява правната сигурност за предприятията и на практика би следвало да означава, че решенията се вземат по-бързо и че предприятията не се сблъскват с различни надзорни органи, които им налагат противоречиви изисквания.

Определянето на водещ орган е свързано с определянето на основното място на установяване на дадено предприятие в ЕС. Понятието „основно място на установяване“ е определено в ОРЗД. Освен това Работната група по член 29 е издала насоки за определянето на водещия надзорен орган на администратора или на обработващия лични данни, които включват критериите за определяне на основното място на установяване[514].

За да се гарантира високо ниво на защита на данните в целия ЕС, водещият надзорен орган не действа самостоятелно. Той трябва да си сътрудничи с другите засегнати надзорни органи с оглед на приемането на решения относно обработването на лични данни от администраторите и обработващите лични данни, като се стреми към постигането на консенсус и гарантирането на последователност. Сътрудничеството между съответните надзорни органи включва обмен на информация, предоставяне на взаимопомощ, провеждане на съвместни разследвания и дейности по наблюдение[515]. Когато си предоставят взаимопомощ, надзорните органи трябва да обработват точно исканията за информация, отправени от други надзорни органи, и да упражняват мерки за надзор, като например предоставяне на предварителни разрешения или провеждане на предварителни консултации с администратора на данни относно неговите дейности по обработване, извършване на проверки и разследвания. На надзорните органи в друга държава членка трябва да се предоставя взаимопомощ при поискване, без неоснователно забавяне и до един месец след получаване на искането[516].

Когато администраторът има място на установяване в няколко държави членки, надзорните органи могат да провеждат съвместни операции,

514 Работна група по член 29 (2016 г.), *Насоки за определяне на водещ надзорен орган на администратор или обработващ лични данни*, WP 244, Брюксел, 13 декември 2016 г., редактирани на 5 април 2017 г.

515 Общ регламент относно защитата на данните, член 60, параграфи 1—3.

516 *Пак там*, член 61, параграфи 1 и 2.

включително разследвания и мерки за изпълнение, в които участват членове или персонал на надзорни органи от други държави членки[517].

Сътрудничеството между различните надзорни органи е важно изискване и съгласно правото на Съвета на Европа. В модернизираната Конвенция № 108 се предвижда, че надзорните органи трябва да си сътрудничат до необходимата степен за изпълнение на техните задачи[518]. Това следва да бъде изпълнено например, като си предоставят взаимно всякаква значима и полезна информация и като координират разследванията си и провеждат съвместни действия[519].

5.4 Европейски комитет по защита на данните

Значението на независимите надзорни органи и основните правомощия, които те имат съгласно европейското право в областта на защитата на данните, са описани по-горе в настоящата глава. Европейският комитет по защита на данните (ЕКЗД) е друг важен участник, който да гарантира, че правилата за защита на данните се прилагат ефективно и последователно в целия ЕС.

ОРЗД определя ЕКЗД като орган на ЕС, който притежава правосубектност[520]. Той е правоприемник на Работната група по член 29[521], създадена с Директивата за защита на личните данни с цел да консултира Комисията относно всяка мярка на ЕС, която засяга правата на физическите лица във връзка с обработването на лични данни и неприкосновеността на личния живот, да насърчава еднаквото прилагане на директивата и да предоставя експертно становище на Комисията по въпроси, свързани със защитата на данните.

517 *Пак там*, член 62, параграф 1.

518 Модернизирана Конвенция № 108, член 16 и член 17.

519 *Пак там*, член 17.

520 Общ регламент относно защитата на данните, член 68.

521 Съгласно Директива 95/46/ЕО Работната група по член 29 трябваше да консултира Комисията относно всяка мярка на ЕС, която засяга правата на физическите лица във връзка с обработването на лични данни и неприкосновеността на личния живот, да насърчава еднаквото прилагане на директивата и да предоставя експертно становище на Комисията по въпроси, свързани със защитата на данните. Работната група по член 29 е съставена от представители на надзорните органи на държавите членки на ЕС, както и на Комисията и на ЕНОЗД.

Работната група по член 29 е съставена от представители на надзорните органи на държавите членки на ЕС и представители на Комисията и на ЕНОЗД.

Подобно на Работната група, ЕКЗД е съставен от ръководителите на надзорните органи на всяка държава членка и ЕНОЗД или от техни представители[522]. ЕНОЗД се ползва с равни права на глас, с изключение на случаите, свързани с разрешаване на спорове, където има право на глас само във връзка с решения относно принципите и правилата, приложими за институциите на ЕС, които съответстват по същество на предвидените в ОРЗД. Комисията има право да участва в дейностите и заседанията на ЕКЗД, но няма право на глас[523]. Комитетът избира с обикновено мнозинство председател (на когото е възложено да го представлява) и двама заместник-председатели измежду своите членове, за срок от пет години. Освен това ЕКЗД има на разположение и секретариат, който се осигурява от ЕНОЗД, за да може Комитетът да има аналитична, административна и логистична подкрепа[524].

Задачите на ЕКЗД са определени в членове 64, 65 и 70 от ОРЗД и включват обширни задължения, които могат да бъдат разделени на три вида основни дейности:

- **Съгласуваност:** ЕКЗД може да приема решения със задължителен характер в три случая: когато надзорен орган е повдигнал относимо и обосновано възражение в случаите на обслужване на едно гише, когато има противоречиви виждания за това кой от надзорните органи е водещият и, последно, когато компетентният надзорен орган не е поискал или не се е съобразил със становището на ЕКЗД[525]. Главната отговорност на ЕКЗД е да гарантира, че ОРЗД се прилага съгласувано в целия ЕС, като Комитетът играе ключова роля в механизма за съгласуваност, описано в раздел 5.5.

- **Консултации:** Задачите на ЕКЗД включват да консултира Комисията по всеки въпрос, свързан със защитата на личните данни в Съюза, като измененията на ОРЗД, преразглежданията на законодателството на ЕС, които засягат обработването на данни и могат да противоречат на правилата на ЕС за защита на данните, или издаването на решения на Комисията

522 Общ регламент относно защитата на данните, член 68, параграф 3.

523 *Пак там*, член 68, параграфи 4 и 5.

524 *Пак там*, членове 73 и 75.

525 *Пак там*, член 65.

относно адекватното ниво на защита, които позволяват предаване на лични данни на трети държави или на международни организации.

- **Насоки:** Комитетът също така издава насоки, препоръки и най-добри практики, за да насърчи съгласуваното прилагане на регламента, и подпомага сътрудничеството и обмена на знания между надзорните органи. Освен това той трябва да насърчава сдруженията на администратори или обработващи лични данни да изготвят кодекси за поведение и да създадат механизми за сертифициране, както и печати за защита на данните.

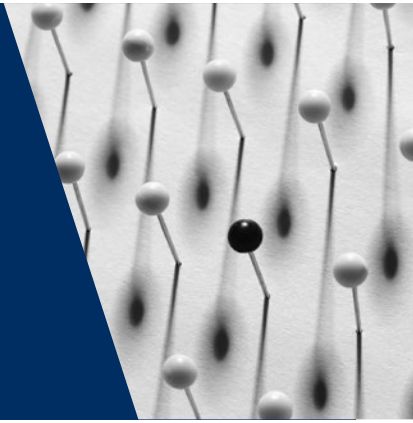
Решенията на ЕКЗД може да бъдат обжалвани пред Съда на ЕС.

5.5 Механизмът за съгласуваност по ОРЗД

За да се гарантира последователното прилагане на регламента във всички държави членки, с ОРЗД се създава механизъм за съгласуваност, чрез който надзорните органи си сътрудничат помежду си и, ако е целесъобразно, с Комисията. Механизмът за съгласуваност се използва в два случая. Първият случай засяга становищата на ЕКЗД, когато компетентен надзорен орган възнамерява да приеме мерки, например списък на операциите по обработване, за които се изисква оценка на въздействието върху защитата на данните (ОВЗД), или да определя стандартни договорни клаузи. Вторият случай засяга задължителните решения на ЕКЗД за надзорните органи в случаите на обслужване на едно гише и когато надзорен орган не се е съобразил със становището на ЕКЗД или не е поискал такова становище.

6

Правата на субектите на данни и тяхното прилагане



ЕС	Обхванати въпроси	СЕ
Право на информация		
Общ регламент относно защитата на данните, член 12 Съд на ЕС, C-473/12, *Institut professionnel des agents immobiliers (IPI)/Englebert*, 2013 г. Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 2015 г.	**Прозрачност на информацията**	Модернизирана Конвенция № 108, член 8
Общ регламент относно защитата на данните, член 13, параграфи 1 и 2 и член 14, параграфи 1 и 2	**Съдържание на информацията**	Модернизизрана Конвенция № 108, член 8, параграф 1
Общ регламент относно защитата на данните, член 13, параграф 1 и член 14, параграф 3	**Момент на предоставяне на информацията**	Модернизирана Конвенция № 108, член 9, параграф 1, буква б)
Общ регламент относно защитата на данните, член 12, параграфи 1, 5 и 7	**Средства за предоставяне на информацията**	Модернизирана Конвенция № 108, член 9, параграф 1, буква б)
Общ регламент относно защитата на данните, член 13, параграф 2, буква г) и член 14, параграф 2, буква д), членове 77, 78 и 79	**Право на подаване на жалба**	Модернизирана Конвенция № 108, член 9, параграф 1, буква е)

ЕС	Обхванати въпроси	СЕ
Право на достъп		
Общ регламент относно защитата на данните, член 15, параграф 1 Съд на ЕС, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 2009 г.	**Право на достъп на дадено лице до собствените му данни**	Модернизирана Конвенция № 108, член 9, параграф 1, буква б) ЕСПЧ, *Leander/Швеция*, № 9248/81, 1987 г.
Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister vor Immigratie, Integratie en Asiel/M u S*, 2014 г. Съд на ЕС, C-434/16, *Peter Nowak/Data Protection Commissioner*, 2017 г.		
Право на коригиране		
Общ регламент относно защитата на данните, член 16	**Коригиране на неточни лични данни**	Модернизирана Конвенция № 108, член 9, параграф 1, буква д) ЕСПЧ, *Cemalettin Canli/Турция*, № 22427/04, 2008 г. ЕСПЧ, *Ciubotaru/Молдова*, № 27138/04, 2010 г.
Право на изтриване		
Общ регламент относно защитата на данните, член 17, параграф 1	**Изтриване на лични данни**	Модернизирана Конвенция № 108, член 9, параграф 1, буква д) ЕСПЧ, *Segerstedt-Wiberg и други/Швеция*, № 62332/00, 2006 г.
Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 2014 г. Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017 г.	**Право „да бъдеш забравен“**	

ЕС	Обхванати въпроси	СЕ
Право на ограничаване на обработването		
Общ регламент относно защитата на данните, член 18, параграф 1	Право на ограничаване на използването на лични данни	
Общ регламент относно защитата на данните, член 19	Задължение за уведомяване	
Право на преносимост на данните		
Общ регламент относно защитата на данните, член 20	Право на преносимост на данните	
Право на възражение		
Общ регламент относно защитата на данните, член 21, параграф 1 Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 2017 г.	Право на възражение, свързано с конкретното положение на субекта на данни	Препоръка относно профилирането, член 5.3 Модернизирана Конвенция № 108, член 9, параграф 1, буква г)
Общ регламент относно защитата на данните, член 21, параграф 2	Право на възражение срещу използване на данните за целите на маркетинга	Препоръка относно директния маркетинг, член 4.1
Общ регламент относно защитата на данните, член 21, параграф 5	Право на възражение чрез автоматизирани средства	
Права, свързани с автоматизираното вземане на решения и профилирането		
Общ регламент относно защитата на данните, член 22	Права, свързани с автоматизираното вземане на решения и профилирането	Модернизирана Конвенция № 108, член 9, параграф 1, буква а)
Общ регламент относно защитата на данните, член 21	Право на възражение срещу автоматизираното вземане на решения	
Общ регламент относно защитата на данните, член 13, параграф 2, буква е)	Право на съдържателно обяснение	Модернизирана Конвенция № 108, член 9, параграф 1, буква в)

ЕС	Обхванати въпроси	СЕ
Средства за правна защита, отговорности, санкции и компенсация		
Хартата, член 47 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 2015 г. Общ регламент относно защитата на данните, членове 77—84	**За нарушения на националното законодателство за защита на данните**	ЕКПЧ, член 13 (само за държави членки на Съвета на Европа) Модернизирана Конвенция № 108, член 9, параграф 1, буква е), членове 12, 15, 16—21 ЕСПЧ, *K.U./Финландия*, № 2872/02, 2008 г. ЕСПЧ, *Biriuk/Литва*, № 23373/03, 2008 г.
Регламент относно защитата на данните при обработването им от институции на ЕС, членове 34 и 49 Съд на ЕС, C-28/08 P, *Европейска комисия/The Bavarian Lager Co. Ltd.* [голям състав], 2010 г.	**За нарушения на правото на ЕС от страна на институции или органи на ЕС**	

Ефективността на правните норми като цяло, и по-конкретно на правата на субектите на данни зависи до голяма степен от наличието на подходящи механизми за прилагането им. В цифровата ера обработването на данни стана повсеместно и все по-трудно разбираемо за физическите лица. За да се ограничи липсата на равновесие в правомощията между субектите на данни и администраторите, на физическите лица са предоставени определени права да упражняват по-голям контрол върху обработването на тяхната лична информация. Правото на достъп на дадено лице до неговите собствени данни и правото на коригиране на тези данни са залегнали в член 8, параграф 2 от Хартата на основните права на ЕС — документ, който представлява първично право на ЕС и е от изключителна ценност в правния ред на ЕС. Вторичното право на ЕС, и по-конкретно Общият регламент относно защитата на данните, създава съгласувана правна рамка, която оправомощава субектите на данни, като им предоставя определени права спрямо администраторите на данни. В допълнение към правата на достъп и коригиране, в ОРЗД се признават редица други права, като правото на изтриване („право да бъдеш забравен“), правото на възражение или на ограничаване на обработването на лични данни, както и права, свързани с автоматизираното вземане на решения и профилирането. Подобни гаранции с цел осигуряване на ефективното упражняване на контрол от страна на субектите на данни върху данните им са

включени и в модернизираната Конвенция № 108. В член 9 са изброени правата, които физическите лица следва да могат да упражняват по отношение на обработването на техните лични данни. Страните по конвенцията трябва да гарантират, че тези права са на разположение на всеки субект на данни в рамките на тяхната юрисдикция и са придружени от ефективни правни и практически средства, които дават възможност на субектите на данни да ги упражняват.

В допълнение към предоставянето на права на физическите лица, също толкова важно е да бъдат създадени механизми, които да позволяват на субектите на данни да подават жалби срещу нарушенията на техните права, да търсят отговорност от администраторите и да претендират за обезщетение. Правото на ефективни правни средства за защита, гарантирано от ЕКПЧ и Хартата, изисква средствата за правна защита да бъдат направени достъпни за всяко лице.

6.1 Правата на субектите на данни

Ключови въпроси

- Всеки субект на данни има право на информация относно всяко обработване на негови лични данни от страна на администратора, с няколко ограничени изключения.
- Субектите на данни имат право:
  - да получат достъп до собствените си данни и да получат определена информация относно обработването;
  - данните им да бъдат коригирани от администратора, който обработва данните им, ако тези данни са неточни;
  - да изискат от администратора изтриване на своите данни, ако той ги обработва незаконно;
  - временно да ограничават обработването;
  - данните им да бъдат прехвърлени на друг администратор при определени условия.
- В допълнение, субектите на данни имат правото да предявяват възражения срещу обработването:

  - на основания, свързани с конкретното им положение;
  - относно използването на техните данни за целите на директен маркетинг.
- Субектите на данни имат право да не бъдат обект на решения, основаващи се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия или ги засяга в значителна степен. Субектите на данни имат също така право:
  - да изискат човешка намеса от страна на администратора;
  - да изразят гледната си точка и да оспорят решение, което се основава на автоматизирано обработване.

6.1.1 Право на информация

Съгласно **правото на Съвета на Европа,** както и съгласно **правото на ЕС** администраторите, които осъществяват операции по обработване на данни, са длъжни да информират субектите на данни за планираното обработване в момента на събиране на личните данни. Това задължение не зависи от наличието на искане от страна на съответния субект на данни, а трябва да се изпълнява проактивно от администратора, независимо от това дали субектът на данни проявява интерес към информацията.

Съгласно правото на Съвета на Европа, в съответствие с член 8 от модернизираната Конвенция № 108, страните по нея трябва да предвидят задължение за администраторите да уведомяват субектите на данни относно самоличността и обичайното си местопребиваване, правното основание и целта на обработването, категориите обработвани лични данни, получателите на техните лични данни (ако има такива) и как те могат да упражняват правата си съгласно член 9, които включват правата на достъп, коригиране и правна защита. На субектите на данни следва да бъде предоставена и всяка друга допълнителна информация, считана за необходима за гарантирането на добросъвестно и прозрачно обработване на личните данни. В обяснителния доклад към модернизираната Конвенция № 108 се пояснява, че информацията, представена на субектите на данни, „следва да бъде леснодостъпна, четима, разбираема и пригодена към съответните субекти на данни“[526].

526 Обяснителен доклад към модернизираната Конвенция № 108, параграф 68.

Съгласно правото на ЕС принципът на прозрачност изисква всяко обработване на лични данни да бъде прозрачно, като цяло, за физическите лица. Физическите лица имат правото да знаят как и какви лични данни се събират, използват или обработват по друг начин, както и да бъдат информирани за рисковете, гаранциите и правата си във връзка с обработването[527]. Ето защо в член 12 от ОРЗД се създава широко и всеобхватно задължение за администраторите да осигуряват прозрачна информация и/или да съобщават как субектите на данни могат да упражняват правата си[528]. Информацията трябва да бъде кратка, прозрачна, разбираема и леснодостъпна, на ясен и прост език. Тя трябва да се предоставя писмено, включително в електронен вид, когато е целесъобразно, и дори може да бъде предоставена устно по искане на субекта на данни и ако самоличността му е безспорно установена. Информацията следва да бъде предоставена без прекалено забавяне или разходи[529].

Член 13 и член 14 от ОРЗД третират правото на субектите на данни да бъдат информирани както в случаите, когато личните данни се събират пряко от тях, така и в случаите, когато данните не са получени от тях.

Обхватът на правото на информация и неговите ограничения съгласно правото на ЕС са пояснени в съдебната практика на Съда на ЕС.

Пример: В делото *Institut professionnel des agents immobiliers (IPI)/ Englebert*[530] от Съда на ЕС беше поискано да даде тълкуване на член 13, параграф 1 от Директива 95/46. Този член дава на държавите членки свободата да приемат законодателни мерки за ограничаване на обхвата на правото на субектите на данни да бъдат информирани, ако това е необходимо за защитата, наред с другото, на правата и свободите на други лица и за предотвратяването и разследването на престъпления или нарушения на етичните кодекси при регламентираните професии. IPI е професионална организация на агентите на недвижими имоти в Белгия, на която е възложена функцията да следи за упражняването на професията агент на недвижими имоти в съответствие с изискванията.

527 Общ регламент относно защитата на данните, съображение 39.

528 *Пак там*, членове 13 и 14; модернизирана Конвенция № 108, член 8, параграф 1, буква б).

529 Общ регламент относно защитата на данните, член 12, параграф 5; модернизирана Конвенция № 108, член 9, параграф 1, буква б).

530 Съд на ЕС, C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert и други*, 7 ноември 2013 г.

Организацията отправя искане до националния съд да постанови, че ответниците са нарушили професионалните правила, и да им разпореди да прекратят различни дейности, свързани с недвижими имоти. IPI основава искането си на доказателства, събрани от частни детективи, чиито услуги той е използвал.

Националният съд е имал съмнения относно стойността на събраните от детективите доказателства, с оглед на възможността те да са били събрани, без да са спазени изискванията на белгийското законодателство относно защитата на данните, и по-конкретно задължението съответното физическо лице да бъде информирано за обработването на личните му данни преди събирането на тази информация. Съдът на ЕС отбелязва, че според член 13, параграф 1 държавите членки „могат", но не са задължени да предвидят в националното си право изключения от задължението съответните физически лица да бъдат информирани за обработването на личните им данни. Тъй като член 13, параграф 1 включва предотвратяването, разследването, разкриването и преследването на углавни престъпления или нарушения на етичните кодекси при регламентираните професии като основания, на които държавите членки могат да ограничават правата на физическите лица, дейността на организация като IPI и на частните детективи, действащи от нейно име, може да се позовава на тази разпоредба. Ако обаче дадена държава членка не е предвидила такова изключение, субектите на данни трябва да бъдат информирани.

Пример: В делото *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*[531] Съдът на ЕС изяснява дали правото на ЕС не допуска един публичен административен орган да предава лични данни на друг публичен административен орган за последващо обработване, без субектите на данни да са уведомени за това предаване и за обработването. В този случай Националната агенция за управление на данъците не е информирала жалбоподателите, че е предала техните данни на Националната здравноосигурителна каса преди самото предаване.

531 Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 1 октомври 2015 г.

Съдът на ЕС посочва, че изискването съгласно правото на ЕС субектите на данни да бъдат уведомявани за обработването на личните им данни „е още по-важно, доколкото то е условие за упражняване на правото на тези лица на достъп до обработваните данни и на поправка на същите, [...] и на правото на възражение срещу обработването на посочените данни". Принципът на добросъвестно обработване изисква субектите на данни да бъдат информирани за предаването на техни данни на друг публичен орган за по-нататъшно обработване от него. Съгласно член 13, параграф 1 от Директива 95/46 държавите членки могат да ограничат правото на информация, ако това бъде счетено за необходимо, за да се защитят важни икономически интереси на държавата, включително данъчни въпроси. Тези ограничения обаче трябва да се извършват чрез законодателни мерки. Тъй като определянето на информацията, която подлежи на предаване, и редът и условията за предаване на тази информация не са уредени със закон, а само с протокол между двата публични органа, условията за дерогация съгласно правото на ЕС не са били изпълнени. Жалбоподателите е следвало да бъдат уведомени предварително за предаването на техни данни към Националната здравноосигурителна каса и за последващото обработване на тези данни.

Съдържание на информацията

Съгласно член 8, параграф 1 от модернизираната Конвенция № 108 администраторът е длъжен да предостави на субекта на данни всяка информация, която гарантира добросъвестно и прозрачно обработване на личните данни, включително:

- самоличността и обичайното местопребиваване или място на стопанска дейност на администратора;
- правното основание и целите на планираното обработване;
- категориите обработвани лични данни;
- получателите или категориите получатели на личните данни, ако има такива;
- начините, по които субектите на данни могат да упражнят правата си.

Съгласно ОРЗД, когато личните данни се събират от субекта на данните, в момента на получаване на личните данни администраторът е задължен да предостави на субекта на данните посочената по-долу информация[532]:

- данните, които идентифицират администратора, и координатите за връзка с него, включително данните на длъжностното лице по защита на данните, ако има такова;
- целите и правното основание за обработването, т.е. договор или правно задължение;
- законния интерес на администратора на данни, ако това е основанието за обработването;
- възможните получатели или категории получатели на личните данни;
- дали личните данни ще бъдат предадени на трета държава или на международна организация и дали това предаване се основава на решение относно адекватното ниво на защита или на подходящи гаранции;
- срока, за който ще се съхраняват личните данни, а ако установяването му е невъзможно, критериите, използвани за определяне на този срок;
- правата на субектите на данни във връзка с обработването, като правото на достъп, коригиране, изтриване, както и правото на ограничаване на обработването или на възражение срещу него;
- дали предоставянето на лични данни е законово или договорно изискване, дали субектът на данните е задължен да предостави личните си данни, както и последствията, в случай че тези данни не бъдат предоставени;
- съществуването на автоматизирано вземане на решения, включително профилиране;
- правото на жалба до надзорен орган;

532 Общ регламент относно защитата на данните, член 13, параграф 1.

- съществуването на право на оттегляне на съгласието.

В случаите на автоматизирано вземане на решения, включително профилиране, субектите на данни трябва да получат съответната информация относно използваната логика при профилирането, неговото значение и предвидените последствия за тях от обработването.

В случаите, когато личните данни не са получени пряко от субекта на данните, администраторът на данни трябва да уведоми физическото лице относно произхода на личните данни. Във всички случаи администраторът трябва, наред с другото, да уведоми субектите на данни относно съществуването на автоматизирано вземане на решения, включително профилиране[533]. Накрая, ако администраторът възнамерява да обработва лични данни за цел, различна от първоначално обявената пред субекта на данни, принципите на ограничение на целите и прозрачност изискват той да уведоми субекта на данни за тази нова цел. Администраторите трябва да предоставят информация преди всякакво по-нататъшно обработване на данните. С други думи, в случаите, когато субектът на данни е дал съгласие за обработването на личните му данни, администраторът трябва да получи отново съгласие от него, ако целта на обработването на личните данни се промени или ако бъдат добавени допълнителни цели.

Момент на предоставяне на информацията

В ОРЗД се прави разграничение между два сценария и два момента, в които администраторът на данни трябва да предостави информация на субекта на данните.

- Когато личните данни са получени пряко от субекта на данните, администраторът трябва да уведоми субекта на данните относно всички свързани с него данни и права съгласно ОРЗД в момента на получаване на данните[534].

533 Общ регламент относно защитата на данните, член 13, параграф 2 и член 14, параграф 2, буква е).

534 *Пак там,* член 13, параграфи 1 и 2, встъпителният текст, където в Общия регламент за защита на данните се посочва, че информацията за задължението се предоставя в „момента на получаване на личните данни".

Ако администраторът възнамерява да обработва личните данни по-нататък за различна цел, той следва да предостави цялата необходима информация, преди да извърши обработването.

- Когато личните данни не са получени пряко от субекта на данните, администраторът е длъжен да предостави на субекта на данни информация за обработването „в разумен срок след получаването на личните данни, но най-късно в срок до един месец" или преди данните да бъдат разкрити на трета страна[535].

В Обяснителния доклад към модернизираната Конвенция № 108 се предвижда, че ако субектите на данни не е възможно да бъдат информирани при започване на обработването, това може да бъде направено на по-късен етап, например когато администраторът влезе във връзка със субекта на данни по някаква причина[536].

Различни начини за предоставяне на информация

Както съгласно правото на Съвета на Европа, така и съгласно правото на ЕС информацията, която администраторът трябва да предостави на субектите на данни, трябва да бъде кратка, прозрачна, разбираема и леснодостъпна. Тя трябва да бъде предоставена писмено или по друг начин, включително с електронни средства, като се използва ясен, прост и лесно разбираем език. При предоставянето на информация администраторът може да използва стандартизирани икони, за да я представи по лесно видим и разбираем начин[537]. Например може да се използва икона, представляваща ключалка, за да се покаже, че данните са събрани по сигурен начин и/или са криптирани. Субектите на данни могат да изискат информацията да им бъде предоставена устно. Информацията трябва да бъде безплатна, освен ако исканията на субекта на данни не са явно неоснователни или прекомерни (т.е. повтарящи се)[538]. Лесният достъп до предоставената информация е от първостепенно значение

535 *Пак там*, член 13, параграф 3 и член 14, параграф 3; вж. също препратката към „разумни интервали от време и без прекалено забавяне" в модернизираната Конвенция № 108, член 8, параграф 1, буква б).

536 Обяснителен доклад към модернизираната Конвенция № 108, параграф 70.

537 Чрез делегирани актове Европейската комисия допълнително ще развие информацията, която да бъде представена под формата на икони, и процедурите за предоставяне на стандартизирани икони; вж. Общия регламент относно защитата на данните, член 12, параграф 8.

538 Общ регламент относно защитата на данните, член 12, параграфи 1, 5 и 7 и модернизирана Конвенция № 108, член 9, параграф 1, буква б).

за способността на субекта на данни да упражни правата си, предвидени в правото на ЕС в областта на защитата на данните.

Принципът на добросъвестно обработване на данните изисква информацията да бъде лесно разбираема от съответните субекти на данни. Трябва да се използва език, който е подходящ за съответните адресати. Нивото и видът на използвания език би трябвало да бъдат различни в зависимост от това дали групата, за която е предназначена, са например възрастни хора или деца, широката общественост или университетски експерти. Въпросът за начините за балансиране на този аспект на разбираемото информиране е разгледан в становището на Работната група по член 29 относно по-хармонизирани разпоредби за информацията. В него се подкрепя идеята за т. нар. „многостепенни" съобщения[539], позволяващи на съответния субект на данни да реши какво ниво на информираност предпочита. Този начин на представяне на информацията обаче не освобождава администратора от задълженията му съгласно член 13 и член 14 от ОРЗД. Администраторът пак трябва да предоставя цялата информация на субекта на данните.

Един от най-ефективните начини за предоставяне на информация е наличието на подходящи клаузи относно информацията, качени на началната страница на администратора, като например политика за поверителност на уебсайта. Има обаче значителна част от населението, която не използва интернет, и информационната политика на дружеството или на публичния орган трябва да предвиди това.

Едно съобщение за поверителност на уебстраницата относно обработването на лични данни би могло да изглежда по следния начин:

Кои сме ние?

Администратор на данните е дружеството Bed and Breakfast C&U, установено в [адрес: xxx], тел.: xxx; факс: xxx; електронна поща: ; данни за контакт на длъжностното лице по защита на данните: [xxx].

Информационното съобщение относно личните данни е част от реда и условията, които уреждат нашите хотелски услуги.

539 Работна група по член 29 (2004 г.), *Становище 10/2004 относно по-хармонизирани разпоредби за информацията*, WP 100, Брюксел, 25 ноември 2004 г.

Какви данни събираме от вас?

Ние събираме от вас следните лични данни: вашето име, пощенски адрес, телефонен номер, електронна поща, информация за престоя, номер на кредитна и дебитна карта и IP адреси или имена на домейни на компютрите, които използвате, за да се свържете с нашия уебсайт.

Защо събираме вашите данни?

Ние обработваме вашите данни въз основа на вашето съгласие и за целите на изпълнението на резервациите, сключването и изпълнението на договорите във връзка с услугите, които ви предлагаме, и спазването на изискванията на закона, например Закона за местните такси, който изисква да събираме лични данни, за да гарантираме плащане на градския данък за хотелски услуги.

Как обработваме вашите данни?

Вашите данни ще бъдат запазени за срок от три месеца. Вашите данни не са предмет на процедури за автоматизирано вземане на решения.

Нашето дружество Bed and Breakfast C&U следва стриктно процедурите за сигурност, за да гарантира, че вашата лична информация няма да бъде повредена, унищожена или разкрита на трета страна без ваше разрешение, и за да предотврати неразрешен достъп. Компютрите, на които се съхранява информацията, се намират в защитена среда с ограничен физически достъп. Ние използваме сигурни защитни системи и други мерки, за да ограничим електронния достъп. Ако данните трябва да бъдат предадени на трета страна, ние изискваме от нея да е въвела сходни мерки за защита на вашите лични данни.

Цялата информация, която събираме или записваме, е ограничена до нашите служби. Достъп до личните данни имат само лицата, които се нуждаят от информацията, за да изпълнят задълженията си по настоящия договор. Ако се нуждаем от информация, за да установим самоличността ви, ще ви изпратим изрично запитване. Преди да ви разкрием дадена информация, може да поискаме от вас да изпълните

нашите проверки за сигурност. Можете да актуализирате личната информация, която ни давате, по всяко време, като се свържете директно с нас.

Какви са вашите права?

Вие имате право на достъп до вашите данни, да получавате копие на вашите данни, да изискате тяхното изтриване или коригиране или тяхното прехвърляне на друг администратор.

Можете да отправяте исканията си към нас на . Трябва да отговорим на искането ви в срок от един месец, но ако то е твърде сложно или получаваме твърде много други искания, срокът може да бъде удължен с още два месеца, за което ще ви информираме.

Достъп до личните ви данни

Вие имате право на достъп до вашите данни, при поискване да бъдете уведомени за причините за обработването на данните, да изискате тяхното изтриване или коригиране; имате също така право да не бъдете обект на чисто автоматизирани решения, без да се вземе предвид мнението ви. Можете да отправяте исканията си към нас на . Вие също така имате право на възражение срещу обработването, да оттеглите съгласието си и да подадете жалба до националния надзорен орган, ако считате, че това обработване на данни е в нарушение на закона, както и да претендирате обезщетение за вреди, възникнали в резултат на незаконно обработване.

Право на подаване на жалба

ОРЗД изисква администраторите да информират субектите на данни относно механизмите за прилагане по националното право и правото на ЕС в случай на нарушение на сигурността на личните данни. Администраторът трябва да уведоми субектите на данни за правото им да подадат жалба за нарушение на сигурността на личните данни до надзорния орган и при необходимост до националния съд[540]. Правото на Съвета на Европа също предвижда правото

540 Общ регламент относно защитата на данните, член 13, параграф 2, буква г) и член 14, параграф 2, буква д); модернизирана Конвенция № 108, член 8, параграф 1, буква е).

на субектите на данни да бъдат информирани относно средствата за упражняване на техните права, включително правото на обезщетение, заложено в чл. 9, параграф 1, буква е).

Изключения от задължението за информиране

В ОРЗД се предвижда изключение от задължението за информиране. Съгласно член 13, параграф 4 и член 14, параграф 5 от ОРЗД задължението за информиране на субектите на данни не се прилага, ако субектът на данни вече разполага с цялата съответна информация[541]. Освен това, когато личните данни не са получени от субекта на данни, задължението за информиране не се прилага, ако предоставянето на информация е невъзможно или изисква несъразмерно големи усилия, по-конкретно когато личните данни се обработват за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели[542].

Освен това съгласно ОРЗД държавите членки се ползват от свобода на преценка да наложат ограничения върху предвидени в регламента задължения и права на физическите лица, ако това е необходима и пропорционална мярка в едно демократично общество, например за да се гарантират националната и обществената сигурност, отбраната, за защита на съдебни разследвания и производства или за защита на икономически и финансови интереси, както и на частни интереси, които са по-основателни от интересите, свързани със защитата на данните[543].

Всички изключения или ограничения трябва да са необходими в едно демократично общество и да са пропорционални на преследваната цел. В много извънредни случаи, например поради медицински показания, защитата на физическото лице сама по себе си може да налага ограничение по отношение на прозрачността; това е свързано по-специално с ограничаване на правото на достъп на всеки субект на данни[544]. Като минимално ниво на защита обаче националното право трябва да е съобразено със същността на основните права и свободи, защитени от законодателството на ЕС[545]. Това изисква нацио-

541 *Пак там*, член 13, параграф 4 и член 14, параграф 5, буква а).

542 *Пак там,* член 14, параграф 5, букви б–д).

543 Общ регламент относно защитата на данните, член 23, параграф 1.

544 Общ регламент относно защитата на данните, член 15.

545 Общ регламент относно защитата на данните, член 23, параграф 1.

налното право да съдържа специални разпоредби, които изясняват целта на обработването, категориите включени лични данни, гаранциите и другите процедурни изисквания[546].

Когато данните са събрани за целите на научни или исторически изследвания, за статистически цели или за целите на архивирането в обществен интерес, Съюзът или държавите членки могат да предвидят дерогации от задължението за информиране, ако има вероятност това задължение да направи невъзможно или сериозно да затрудни постигането на конкретните цели[547].

Подобни ограничения съществуват и в правото на Съвета на Европа, където правата, гарантирани на субектите на данни съгласно чл. 9 от модернизираната Конвенция № 108, могат да бъдат обект на възможни органичения при строго определени условия, разписани в член 11 от модернизираната Конвенция № 108. Освен това, в съответствие с член 8, параграф 2 от модернизираната Конвенция № 108, задължението за прозрачност на обработката от страна на администраторите не се прилага, когато физическите лица вече разполагат с информацията.

Правото на достъп на дадено лице до собствените му данни

Съгласно правото на Съвета на Европа правото на достъп на дадено лице до собствените му данни е изрично признато в член 9 от модернизираната Конвенция № 108. Този член предвижда, че всяко лице има правото да получи при поискване информация относно обработването на лични данни, свързани с него, която да му бъде съобщена по разбираем начин. Правото на достъп е признато не само в разпоредбите на модернизираната Конвенция № 108, а и в съдебната практика на ЕСПЧ. ЕСПЧ многократно е постановявал, че лицата имат право на достъп до информация за личните им данни и че това право произтича от необходимостта да се зачита личният живот[548]. Правото на достъп до лични данни, съхранявани от публични или частни организации, обаче може да бъде ограничено при определени обстоятелства[549].

546 *Пак там*, член 23, параграф 2.

547 *Пак там*, член 89, параграфи 2 и 3.

548 ЕСПЧ, *Gaskin/Обединеното кралство*, № 10454/83; 7 юли 1989 г.; ЕСПЧ, *Odièvre/Франция* [голям състав], № 42326/98, 13 февруари 2003 г.; ЕСПЧ, *K.H. и други/Словакия*, № 32881/04, 28 април 2009 г.; ЕСПЧ, *Godelli/Италия*, № 33783/09, 25 септември 2012 г.

549 ЕСПЧ, *Leander/Швеция*, № 9248/81, 26 март 1987 г.

Съгласно законодателството на ЕС правото на достъп на дадено лице до собствените му данни е изрично признато в член 15 от ОРЗД, като е посочено и като елемент от основното право на защита на личните данни в член 8, параграф 2 от Хартата на основните права на ЕС[550]. Правото на дадено лице да получи достъп до собствените му лични данни е основен елемент от европейското право в областта на защитата на данните[551].

В ОРЗД се предвижда, че всеки субект на данни има правото на достъп до личните му данни и на определена информация относно обработването, която администраторите трябва да предоставят[552]. По-специално всеки субект на данни има право да получи (от администратора) потвърждение за това, дали отнасящи се до него данни се обработват, както и информация най-малкото за следното:

- целите на обработването;
- съответните категории данни;
- получателите или категориите получатели, пред които се разкриват данните;
- предвидения срок, за който ще се съхраняват данните, а ако това е невъзможно, критериите, използвани за определянето на този срок;
- съществуването на право на коригиране или изтриване на лични данни или ограничаване на обработването на лични данни;
- правото на жалба до надзорния орган;
- когато данните, които са в процес на обработване, не са събрани от субекта на данните, всякаква налична информация за техния източник;

550 Вж. също Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister vor Immigratie, Integratie en Asiel/M и S.*, 17 юли 2014 г.; Съд на ЕС, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Европейски орган за безопасност на храните (ЕОБХ), Европейска комисия*, 16 юли 2015 г.

551 Съд на ЕС, съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister vor Immigratie, Integratie en Asiel/M и S*, 17 юли 2014 г.

552 Общ регламент относно защитата на данните, член 15, параграф 1.

- в случаите на автоматизирани решения — логиката на всяко автоматизирано обработване на данни.

Администраторът на данни трябва да предостави на субекта на данни копие от личните данни, които са в процес на обработване. Всяка информация, която се съобщава на субекта на данни, трябва да бъде предоставена в разбираема форма, което означава, че администраторът трябва да се увери, че субектът на данни е в състояние да разбере предоставяната информация. Например включването на технически съкращения, кодирани понятия или акроними в отговор на искане за достъп обикновено не е достатъчно, освен ако не е обяснено значението на тези термини. Когато се извършва автоматизирано вземане на решения, включително профилиране, е необходимо да бъде разяснена използваната при автоматизираното вземане на решение логика, включително критериите, които са били взети предвид при оценяването на субекта на данните. Подобни изисквания съществуват в **правото на Съвета на Европа**[553].

Пример: Достъпът на субекта на данните до неговите лични данни му помага да определи дали те са точни. Затова е от съществено значение субектът на данни да бъде информиран в разбираема форма не само за действителните лични данни, които се обработват, но също и за категориите, по които се обработват тези лични данни, като име, IP адрес, координати на местонахождението, номер на кредитна карта и др.

Когато данните не са събрани от субекта на данните, в отговор на искане за достъп трябва да бъде предоставена информация за източника на данни, доколкото тази информация е налична. Тази разпоредба трябва да се разбира в контекста на принципите на добросъвестност, прозрачност и отчетност. Администраторът не може да унищожава информация за източника на данни, за да бъде освободен от задължението да го разкрие, освен ако нейното заличаване не е щяло да бъде извършено въпреки полученото искане за достъп, като администраторът все пак трябва да спазва общите изисквания за „отчетност".

553 Вж. модернизираната Конвенция № 108, член 8, параграф 1, буква в).

Както е посочено в съдебната практика на Съда на ЕС, правото на достъп до личните данни не може да бъде неправомерно ограничавано от времеви рамки. Освен това на субектите на данни трябва да бъде предоставяна разумна възможност за получаване на информация относно операции по обработване на данни, които са се случили в миналото.

Пример: В делото *Rijkeboer*[554] от Съда на ЕС беше поискано да определи дали правото на дадено лице на достъп до информация относно получателите или категориите получатели на личните данни и относно съдържанието на данните може да бъде ограничено до една година, предхождаща искането му за достъп.

За да определи дали в законодателството на ЕС се разрешава такова времево ограничение, Съдът на ЕС реши да тълкува член 12 с оглед на целите на директивата. Съдът на ЕС първо посочва, че правото на достъп е необходимо, за да позволи на субекта на данни да упражнява правото да накара администратора да поправи, изтрие или блокира неговите данни или да го накара да уведоми третите лица, на които са разкрити данните, за поправките, изтриването или блокирането. Ефективно право на достъп е необходимо и за да се позволи на съответния субект на данни да упражни правото си на възражение срещу обработването на неговите лични данни или правото си на подаване на жалба и претендиране на обезщетение за вреди[555].

За да се гарантира полезният ефект на правата, предоставени на субектите на данни, Съдът на ЕС постановява, че „това право трябва задължително да се отнася за минал момент. Всъщност, ако случаят не е такъв, заинтересованото лице не би могло ефикасно да упражни правото си да иска поправка, изтриване или блокиране на данните, за които предполага, че са непълни или неточни, както и да предяви съдебен иск и да получи обезщетение за претърпените вреди“.

554 Съд на ЕС, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 7 май 2009 г.

555 Общ регламент относно защитата на данните, член 15, параграф 1, букви в) и е), член 16, член 17, параграф 2, член 21 и глава VIII.

6.1.2 Право на коригиране

Съгласно правото на ЕС и **правото на Съвета на Европа** субектите на данни имат право на коригиране на личните им данни. Точността на личните данни е от съществено значение, за да се гарантира високо ниво на защита на данните за субектите на данни[556].

Пример: В делото *Ciubotaru/Молдова*[557] жалбоподателят не е могъл да промени своя, регистриран в официалните регистри, етнически произход от молдовски на румънски с аргумента, че не е успял да обоснове искането си. ЕСПЧ счита, че е приемливо държавите да изискват обективни доказателства при регистрацията на етническата идентичност на отделните лица. Ако такова искане се основава на чисто субективни и необосновани причини, органите биха могли да го отхвърлят. Въпреки това претенцията на жалбоподателя е била основана на нещо повече от субективното възприятие за собствената му етническа принадлежност, като той е бил в състояние да предостави обективно проверими връзки с румънската етническа група, като език, име, светоусещане и т.н. Въпреки това, съгласно националното законодателство, жалбоподателят е бил задължен да предостави доказателство за принадлежността на родителите си към румънската етническа група. Предвид историческата реалност в Молдова подобно искане е създало непреодолима пречка пред регистрацията на етническа идентичност, различна от онази, която съветските власти са посочили по отношение на родителите му. Възпрепятствайки разглеждането на искането на жалбоподателя в светлината на обективно проверими доказателства, държавата не е изпълнила своето позитивно задължение да осигури на жалбоподателя ефективно зачитане на неприкосновеността на личния му живот. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

В някои случаи е достатъчно субектът на данните просто да поиска коригиране, например на начина на изписване на името, промяна на адрес или на телефонен номер. Съгласно **правото на ЕС** и **правото на Съвета на Европа** неточните лични данни трябва да бъдат коригирани без неоснователно или

556 *Пак там*, член 16 и съображение 65; модернизирана Конвенция № 108, член 9, параграф 1, буква д).

557 ЕСПЧ, *Ciubotaru/Молдова*, № 27138/04, 27 април 2010 г., параграфи 51 и 59.

прекалено забавяне[558]. Ако обаче подобни искания са свързани с въпроси от значим правен характер, като например правната самоличност на субекта на данни или точното местожителство с оглед връчването на правни документи, исканията за коригиране може да се окажат недостатъчни и администраторът може да има право да поиска твърдението за неточност на данните да бъде доказано. Подобни искания не трябва да налагат непосилна тежест на доказване на субектите на данни и по този начин да ги възпират да искат коригиране на свързаните с тях данни. ЕСПЧ е установил нарушение на член 8 от ЕКПЧ в няколко случая, при които жалбоподателят не е имал възможност да оспори точността на информация, пазена в секретни архиви[559].

Пример: По делото *Cemalettin Canli/Турция*[560] Европейският съд по правата на човека констатира нарушение на член 8 от ЕКПЧ, свързано с неточно изготвени полицейски доклади в рамките на наказателно производство.

Жалбоподателят е бил обект два пъти на наказателно производство заради предполагаемо участие в незаконни организации, но не е бил осъждан. При нов арест на жалбоподателя по обвинение в друго престъпление полицията е внесла в наказателния съд доклад, озаглавен *„информационен формуляр за допълнителни престъпления“*, в който жалбоподателят е представен като член на две незаконни организации. Искането на жалбоподателя да получи доклада и полицейското досие не е удовлетворено. ЕСПЧ приема, че информацията в полицейския доклад попада в обхвата на член 8 от ЕКПЧ, тъй като публичната информация също би могла да попадне в обхвата на понятието „личен живот“, когато тя е обект на системно събиране и съхранение от страна на органите. В допълнение на това полицейският доклад е бил неточен и неговото изготвяне и внасяне в наказателния съд не е било извършено в съответствие с националното право. Съдът заключава, че е налице нарушение на член 8.

558 Общ регламент относно защитата на данните, член 16; модернизирана Конвенция № 108, член 9, параграф 1.

559 ЕСПЧ, *Rotaru/Румъния* [голям състав], № 28341/95, 4 май 2000 г.

560 ЕСПЧ, *Cemalettin Canli/Турция*, № 22427/04, 18 ноември 2008 г., параграфи 33 и 42—43; ЕСПЧ, *Dalea/Франция*, № 964/07, 2 февруари 2010 г.

В хода на граждански спорове или производства пред публичен орган, когато се решава дали дадени данни са точни или не, субектът на данни може да изиска в досието с неговите данни да бъде добавен коментар или бележка, в които да се посочва, че точността им се оспорва и че предстои вземането на официално решение[561]. През този период администраторът на данни не трябва да представя данните като точни или като неподлежащи на изменение, по-специално пред трети страни.

6.1.3 Право на изтриване (право „да бъдеш забравен“)

Предоставянето на субектите на данни на право на изтриване на собствените им данни е особено важно за ефективното прилагане на принципите за защита на данните и най-вече на принципа на свеждане на данните до минимум (личните данни трябва да бъдат ограничени до необходимото за целите, за които се обработват). Ето защо правото на изтриване се среща в правните инструменти както на Съвета на Европа, така и на ЕС[562].

Пример: В делото *Segerstedt-Wiberg и други/Швеция*[563] жалбоподателите са били обвързани с някои либерални и комунистически политически партии. Те подозират, че свързана с тях информация е била включена в тайни полицейски доклади и искат тя да бъде изтрита. ЕСПЧ приема, че съхраняването на спорните данни е правно обосновано и преследва легитимна цел. По отношение на някои от жалбоподателите обаче ЕСПЧ констатира, че продължаващото съхранение на данните представлява непропорционална намеса в личния живот. Например в случая с един от жалбоподателите органите са запазили информация, че през 1969 г. за него се е твърдяло, че е оказал насилствена съпротива при проверка от страна на полицията по време на демонстрации. ЕСПЧ счита, че тази информация не би могла да представлява интерес с оглед на националната сигурност, особено предвид нейната давност. Съдът констатира, че този случай представлява нарушение на член 8 от ЕКПЧ по отношение на четирима от петимата жалбоподатели, тъй

561 Общ регламент относно защитата на данните, член 18 и съображение 67.

562 *Пак там*, член 17.

563 ЕСПЧ, *Segerstedt-Wiberg и други/Швеция*, № 62332/00, 6 юни 2006 г., параграфи 89 и 90; вж. също например ЕСПЧ, *М.К./Франция*, № 19522/09, 18 април 2013 г.

като предвид изтеклото време от момента на действията, които се твърди, че са извършили, продължаващото съхранение на данните им е необосновано.

Пример: В делото *Brunet/Франция*[564] жалбоподателите възразяват срещу съхранението на тяхна лична информация в полицейска база данни, която съдържа информация за осъдени лица, обвиняеми и жертви. Макар че наказателното производство срещу жалбоподателя е било прекратено, базата данни е съдържала информация за него. ЕСПЧ постановява, че е налице нарушение на член 8 от ЕКПЧ. За да достигне до заключение, Съдът приема, че на практика жалбоподателят не е имал никаква възможност да заличи личните си данни от базата данни. ЕСПЧ също така разглежда естеството на включената в базата данни информация и констатира, че тя представлява намеса в правото на неприкосновеност на личния живот на жалбоподателя, тъй като съдържа подробности за неговата самоличност и личност. Освен това Съдът установява, че периодът на съхранение за личните данни в базата данни, който е 20 години, е прекомерно дълъг, особено след като жалбоподателят така и не е получил никаква присъда.

В модернизираната Конвенция № 108 изрично се признава, че всяко лице има право на изтриване на неточни, неверни или незаконосъбразно обработени данни[565].

В правото на ЕС член 17 от ОРЗД поражда действие по отношение на исканията на субектите на данни за изтриване или заличаване на данните им. Правото на дадено лице на изтриване на личните му данни без ненужно забавяне се прилага, когато:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните, и няма друго правно основание за обработването;

564 ЕСПЧ, *Brunet/Франция*, № 21010/10, 18 септември 2014 г.

565 Модернизирана Конвенция № 108, член 9, параграф 1, буква д).

- субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;

- личните данни са били обработвани незаконосъобразно;

- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

- личните данни са били събрани във връзка с предлагането на услуги на информационното общество на деца по член 8 от ОРЗД[566].

Тежестта, свързана с доказването на законосъобразността на обработването на данните, се носи от администраторите, тъй като те отговарят за законосъобразността на обработването[567]. Съгласно принципа на отчетност администраторът трябва във всеки момент да може да докаже, че е налице стабилно правно основание за обработването на данните, като в противен случай обработването трябва да бъде прекратено[568]. В ОРЗД са определени изключения от правото „да бъдеш забравен", включително когато обработването на лични данни е необходимо:

- за упражняване на правото на свобода на изразяването и правото на информация;

- за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора;

- по причини от обществен интерес в областта на общественото здраве;

- за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;

566 Общ регламент относно защитата на данните, член 17, параграф 1.

567 *Пак там*.

568 *Пак там*, член 5, параграф 2.

- за установяването, упражняването или защитата на правни претенции[569].

Съдът на ЕС е потвърдил значението на правото на изтриване, за да се гарантира високо ниво на защита на данните.

Пример: В делото *Google Spain*[570] Съдът на ЕС разглежда въпроса дали Google е длъжно да заличи остаряла информация относно финансови затруднения на жалбоподателя от списъка на резултатите от търсенето. Наред с другото, дружеството Google оспорва отговорността си с твърдението, че само осигурява хипервръзка към уебстраницата на издателя, която хоства информацията, в случая вестник, който съобщава за несъстоятелността на жалбоподателя[571]. Според дружеството Google искането да се заличи остаряла информация от уебстраница следва да се отправи към хоста на уебстраницата, а не към Google, което просто осигурява връзка към оригиналната страница. Съдът на ЕС заключава, че когато търси информация и уебстраници в мрежата и индексира съдържанието с цел осигуряване на резултати от търсенето, Google се превръща в администратор на данни, към който са приложими отговорностите и задълженията по правото на ЕС.

Съдът на ЕС пояснява, че интернет търсачките и резултатите от търсенето, предоставящи лични данни, могат да изградят подробен профил на съответното лице[572]. Търсачките придават всеобщ характер на информацията, съдържаща се в подобен списък на резултатите. Предвид потенциалната тежест на това вмешателство, то не може да се обоснове единствено с икономическия интерес на лицето, което управлява интернет търсачка, при това обработване на данни. Трябва да

569 *Пак там*, член 17, параграф 3.

570 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграфи 55—58.

571 Дружеството Google оспорва и приложимостта на правилата на ЕС за защита на данните поради факта, че Google Inc. е установено в САЩ и обработването на лични данни, предмет на делото, също е било извършено в САЩ. Във връзка с иска се изтъква и втори аргумент за неприложимостта на правото на ЕС в областта на защитата на данните, че интернет търсачките не могат да бъдат считани за „администратори" по отношение на данните, показвани в техните резултати, тъй като те не са запознати с тях, нито пък упражняват контрол върху тях. Съдът на ЕС отхвърля и двата аргумента, като постановява, че Директива 95/46/ЕО е приложима в този случай, и продължава с разглеждането на обхвата на правата, които тя гарантира, по-конкретно на правото на изтриване на личните данни.

572 *Пак там*, параграфи 36, 38, 80—81 и 97.

се потърси справедливо равновесие по специално между легитимния интерес на потребителите на интернет за достъп до информация и основните права на субектите на данни съгласно членове 7 и 8 от Хартата на основните права на ЕС. Във все по-цифровизиращото се общество изискването личните данни да бъдат точни и да не надхвърлят необходимото (т.е. при предоставянето на информация на обществеността) е от основно значение за гарантирането на високо ниво на защита на данните на лицата. Лицето, което управлява търсачката в качеството си на „администратор, трябва да гарантира в рамките на своята отговорност, компетентност и възможности, че посоченото обработване на данни отговаря на изискванията" на правото на ЕС, за да могат предвидените в нея гаранции да разгърнат цялостното си действие[573]. Това означава, че правото на заличаване на лични данни, когато обработването им е остаряло или вече не е необходимо, обхваща и администраторите на данни, които само копират информацията[574].

При разглеждането на въпроса дали Google е трябвало да премахне връзките, свързани с жалбоподателя, Съдът на ЕС постановява, че при определени условия физическите лица имат право да изискат изтриване на лични данни. Към това право може да се прибегне, когато информацията, отнасяща се до лицето, не е точна, не е адекватна, не е релевантна или е прекомерна по отношение на целите на обработването на данни. Съдът на ЕС признава, че това право не е абсолютно; то трябва да бъде балансирано с други права и интереси, по-специално с интересите на широката общественост да има достъп до определена информация. Всяко искане за изтриване трябва да се преценява поотделно, за да се потърси баланс между основните права на защита на личните данни и на неприкосновеност на личния живот на субекта на данни, от една страна, и законните интереси на всички интернет потребители, включително издателите, от друга страна. Съдът на ЕС дава насоки относно факторите, които трябва да се вземат предвид при търсенето на баланс. Особено важен фактор е естеството

573 *Пак там*, параграфи 81—83.

574 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграф 88. Вж. също Работна група за защита на личните данни по член 29 (2014 г.), *Насоки относно изпълнението на решението на Съда на ЕС по дело Google Spain и Google Inc/Agencia Española de Protección de Datos (AEPD) и Mario Costeja González, C-131/12*, WP 225, Брюксел, 26 ноември 2014 г. и Препоръка CM/Rec(2012)3 на Комитета на министрите до държавите членки относно защитата на човешките права при осъществяване на услуги на търсене в мрежата (search engines), 4 април 2012 г.

на въпросната информация. Ако информацията е свързана с личния живот на лицето и няма обществен интерес към нейната наличност, тогава защитата на данните и неприкосновеността на личния живот биха имали предимство пред правото на широката общественост да има достъп до тази информация. И обратно, ако субектът на данни е обществена личност или информацията е от такъв характер, че достъпът на широката общественост до нея да е оправдан, тогава имащият предимство интерес на широката общественост за достъп до информацията може да обоснове намесата в основните права на защита на личните данни и неприкосновеност на личния живот на субекта на данни.

След решението Работната група по член 29 прие насоки за прилагане на решението на Съда на ЕС[575]. Насоките включват списък от общи критерии, които да бъдат използвани от надзорните органи при разглеждането на жалби, свързани с искания за заличаване на данни от страна на физически лица, с обяснение какво означава правото на изтриване, и от които тези органи да се ръководят при търсенето на баланс между правата. В насоките отново се посочва, че оценка трябва да се извършва за всеки отделен случай. Тъй като правото „да бъдеш забравен" не е абсолютно, резултатът от такова искане може да се различава в зависимост от конкретния случай. Това се вижда и в съдебната практика на Съда на ЕС след делото Google.

Пример: По делото *Camera di Commercio di Lecce/Manni*[576] Съдът на ЕС трябваше да прецени дали физическо лице има право на изтриване на личните му данни, публикувани в публичен дружествен регистър, след като неговото дружество е престанало да съществува. Г-н Manni е поискал от Търговската палата на Лече да заличи негови лични данни от нейния регистър, след като разбрал, че негови потенциални клиенти ще направят справка в регистъра и ще видят, че е бил управител на дружество, което е било обявено в несъстоятелност преди повече от десет години. Жалбоподателят счита, че тази информация ще отблъсне потенциалните му клиенти.

575 Работна група по член 29 (2014 г.), *Насоки относно изпълнението на решението на Съда на ЕС по дело Google Spain u Google Inc/Agencia Española de Protección de Datos (AEPD) u Mario Costeja González, C-131/12*, WP 225, Брюксел, 26 ноември 2014 г.

576 Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 март 2017 г.

При търсенето на баланс между правото на г-н Manni на защита на личните му данни и интереса на широката общественост за достъп до информацията Съдът на ЕС първо разглежда целта на публичния регистър. Съдът посочва факта, че оповестяването е предвидено в закон, и по-специално в директива на ЕС, която цели да направи информацията за дружествата по-леснодостъпна за трети страни. Следователно трети страни следва да имат достъп и да могат да преглеждат основните документи на дадено дружество и друга информация във връзка с него, „особено данни за лицата, упълномощени да задължават дружеството". Целта на оповестяването е и да се гарантира правната сигурност с цел засилване на търговията между държавите членки, като се гарантира, че трети страни имат достъп до цялата информация, свързана с дружествата в целия ЕС.

По-нататък Съдът на ЕС отбелязва, че дори след изминаването на определено време и дори след прекратяването на дадено дружество често продължават да съществуват права и правоотношения, свързани с това дружество. Споровете, свързани с прекратяването, могат да бъдат продължителни и още много години след като е престанало да съществува дадено дружество могат да възникват въпроси относно дружеството, неговите управители и ликвидатори. Съдът на ЕС постановява, че предвид широкия набор от възможни сценарии и разликите в давностните срокове, предвидени във всяка държава членка, „понастоящем изглежда невъзможно да се определи единен срок, считано от прекратяването на дадено дружество, след изтичането на който повече няма да е необходимо вписването на посочените данни в регистъра и оповестяването им". Поради легитимната цел на оповестяването и трудностите при определяне на срок, след изтичането на който личните данни могат да бъдат изтрити от регистъра, без да се навреди на интересите на трети страни, Съдът на ЕС констатира, че правилата на ЕС за защита на данните не гарантират право на изтриване на лични данни за лицата в положението на г-н Manni.

Когато администраторът е направил личните данни обществено достояние и е задължен да изтрие информацията, той е длъжен и трябва да предприеме „разумни" стъпки, за да уведоми другите администратори, които обработват същите данни, относно искането на субекта на данни за изтриването

им. В своите действия администраторът трябва да отчита наличните технологии и разходите по изпълнението[577].

6.1.4 Право на ограничаване на обработването

Член 18 от ОРЗД оправомощава субектите на данни да накарат администратора временно да ограничи обработването на личните им данни. Субектите на данни могат да поискат от администратора да ограничи обработването, когато:

- точността на личните данни се оспорва;
- обработването е неправомерно и субектът на данните изисква използването на личните данни да бъде ограничено, вместо те да бъдат изтрити;
- данните трябва да бъдат съхранени за упражняването или защитата на правни претенции;
- предстои вземането на решение дали законните интереси на администратора на данни имат преимущество пред интересите на субекта на данните[578].

Методите, с които администраторът може да ограничи обработването на лични данни, могат да включват например временно преместване на избраните данни в друга система за обработване, прекратяване на достъпа на ползвателите до тях или временно премахване на личните данни[579]. Администраторът трябва да информира субекта на данни преди отмяната на ограничаването на обработването[580].

577 Общ регламент относно защитата на данните, член 17, параграф 2 и съображение 66.

578 *Пак там*, член 18, параграф 1.

579 *Пак там*, съображение 67.

580 *Пак там*, член 18, параграф 3.

Задължение за уведомяване относно коригирането или изтриването на лични данни или ограничаването на обработването им

Администраторът трябва да съобщава за всяко коригиране или изтриване на лични данни или всяко ограничаване на обработването на всеки получател, на когото администраторът е разкрил личните данни, освен ако това е невъзможно или изисква несъразмерно големи усилия[581]. Ако субектът на данните поиска информация за тези получатели, администраторът трябва да му я предостави[582].

6.1.5 Право на преносимост на данните

Съгласно ОРЗД субектите на данни имат право на преносимост на данните, когато личните данни, които са предоставили на администратор, се обработват чрез автоматизирани средства въз основа на съгласието им или когато обработването на лични данни е необходимо за изпълнението на договор и се извършва по автоматизиран начин. Това означава, че правото на преносимост на данните не се прилага, когато обработването на лични данни се базира на правно основание, различно от съгласие или договор[583].

Ако правото на преносимост на данните е приложимо, субектите на данни имат право да получат пряко прехвърляне на личните им данни от един администратор към друг, ако това е технически осъществимо[584]. За да се улесни това, администраторът следва да разработи оперативно съвместими формати, които позволяват преносимост на данните за субектите на данни[585]. В ОРЗД се посочва, че тези формати трябва да бъдат структурирани, широко използвани и пригодени за машинно четене, за да се улесни оперативната съвместимост[586]. Оперативната съвместимост може да бъде определена в широк смисъл като способността на информационните системи да обменят данни и да дават възможност за споделяне на информация[587]. Тъй като целта

581 *Пак там,* член 19.

582 *Пак там.*

583 *Пак там,* съображение 68 и член 20, параграф 1.

584 *Пак там*, член 20, параграф 2.

585 *Пак там,* съображение 68 и член 20, параграф 1.

586 *Пак там*, съображение 68.

587 Европейска комисия, Съобщение „По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността“, COM(2016) 205 окончателен, 2 април 2016 г.

на използваните формати е да се постигне оперативна съвместимост, ОРЗД не включва определени препоръки относно конкретния формат, който трябва да бъде осигурен: форматите в отделните сектори може да се различават[588].

Съгласно насоките на Работната група по член 29 правото на преносимост на данните „подкрепя избора на потребителя, контрола от негова страна и оправомощаването му“ с цел да се даде на субектите на данни контрол върху собствените им лични данни[589]. В насоките се пояснява основните елементи на преносимостта на данните, които включват:

- правото на субектите на данни да получават собствените си лични данни, обработвани от администратора, в структуриран, широко използван, пригоден за машинно четене и оперативно съвместим формат;

- правото на прехвърляне на личните данни от един администратор на лични данни към друг без възпрепятстване, ако това е технически осъществимо;

- режима на администриране — когато даден администратор отговаря на искане за преносимост на данни, той действа по указания на субекта на данни, което означава, че не носи отговорност за съответствието на получаващия администратор с правото в областта на защитата на данните, като се има предвид, че субектът на данни решава на кого да бъдат прехвърлени те;

- правото на преносимост на данните се упражнява, без да се засяга никое друго право, какъвто е случаят с всички други права съгласно ОРЗД.

6.1.6 Право на възражение

Субектите на данни могат да се позоват на правото си на възражение срещу обработването на лични данни на основания, свързани с тяхното конкретно положение, както и срещу обработването на данни за целите на директния маркетинг. Правото на възражение може да бъде упражнено чрез автоматизирани средства.

588 Работна група по член 29 (2016 г.), *Насоки относно правото на преносимост на данните*, WP 242, 13 декември 2016 г., преразгледани на 5 април 2017 г., стр. 13.

589 *Пак там.*

Право на възражение на основания, свързани с конкретното положение на субектите на данни

Субектите на данни нямат общо право на възражение срещу обработването на техните данни[590]. В член 21, параграф 1 от ОРЗД на субектите на данни се дава право на възражение на основания, свързани с тяхното конкретно положение, когато правното основание за обработването е изпълнението от страна на администратора на задача от обществен интерес или когато обработването се основава на законните интереси на администратора[591]. Правото на възражение се прилага към дейностите на профилиране. Подобно право е признато в модернизираната Конвенция № 108[592].

Правото на възражение на основания, свързани с конкретното положение на субекта на данни, цели да се намери правилният баланс между правата на субекта на данни, свързани със защитата на данните му, и законните права на други лица да обработват данните на субекта на данни. Съдът на ЕС обаче пояснява, че правата на субекта на данни „като общо правило" имат предимство пред икономическите интереси на администратора на данни, в зависимост от „естеството на въпросната информация и от чувствителността ѝ по отношение на личния живот на съответното лице, както и от интереса на обществеността да разполага с тази информация"[593]. Съгласно ОРЗД тежестта на доказване е вменена на администраторите, които трябва да представят неопровержими основания за продължаване на обработването[594]. По подобен начин в Обяснителния доклад към модернизираната Конвенция № 108 се пояснява, че законните интереси за обработването на данни (които може да имат предимство пред правото на възражение на субекта на данните) трябва да се доказват във всеки случай поотделно[595].

590 Вж. също ЕСПЧ, *M.S./Швеция*, № 20837/92, 27 август 1997 г. (в което медицински данни са били съобщени без предоставянето на съгласие или възможност за възражение); ЕСПЧ, *Leander/Швеция*, № 9248/81, 26 март 1987 г.; ЕСПЧ, *Mosley/Обединеното кралство*, № 48009/08, 10 май 2011 г.

591 Общ регламент относно защитата на данните, съображение 69; член 6, параграф 1, букви д) и е).

592 Модернизирана Конвенция № 108, член 9, параграф 1, буква г); Препоръка относно профилирането, член 5, параграф 3.

593 Съд на ЕС, C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г., параграф 81.

594 Вж. също модернизираната Конвенция № 108, член 98, параграф 1, буква г), където се посочва, че субектът на данни може да възрази срещу обработването на негови лични данни, „освен ако администраторът не докаже, че съществуват законни основания за обработването, които имат предимство пред интересите или правата и основните свободи на субекта на данните".

595 Обяснителен доклад към модернизираната Конвенция № 108, параграф 78.

Пример: По делото *Manni*[596] Съдът на ЕС постановява, че поради законната цел на оповестяването на лични данни в дружествения регистър, по-специално необходимостта да се защитят интересите на трети страни и да се гарантира правната сигурност, по принцип г-н Manni няма право на изтриване на личните му данни от дружествения регистър. Съдът обаче признава съществуването на право на възражение срещу обработването, като посочва, че „не може да се изключи, че е възможно да съществуват особени случаи, при които неопровержими законови основания, свързани с конкретното положение на съответното лице, обосновават по изключение достъпа до вписаните в регистъра лични данни, отнасящи се до него, да бъде ограничен — след изтичането на достатъчно дълъг срок [...] — до третите лица, които могат да докажат особен интерес от консултирането им".

Съдът на ЕС счита, че националните съдилища трябва да преценяват всеки конкретен случай с оглед на всички свързани с лицето обстоятелства и като вземат предвид евентуалното наличие на законови основания, които биха могли да обосноват по изключение ограничаването на достъпа на трети страни до данните, съдържащи се в дружествените регистри. Съдът обаче пояснява, че в случая на г-н Manni само по себе си твърдението, че оповестяването на личните му данни в регистъра е отблъснало неговите клиенти, не може да бъде считано за такова неопровержимо законово основание. Потенциалните клиенти на г-н Manni имат законен интерес от достъпа до информацията относно несъстоятелността на предишното му дружество.

Резултатът от успешно възражение се състои в това, че администраторът не може повече да обработва въпросните данни. Операциите по обработването на данните на физическото лице, извършени преди възражението, обаче продължават да бъдат законни.

Право на възражение срещу обработване на данните за целите на директен маркетинг

В член 21, параграф 2 от ОРЗД се предвижда специално право на възражение срещу използването на личните данни за целите на директен маркетинг, като

596 Съд на ЕС, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 март 2017 г., параграфи 47 и 60.

се дава допълнително разяснение на член 13 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Такова право е предвидено и в модернизираната Конвенция № 108, както и в Препоръката на Съвета на Европа относно директния маркетинг[597]. В Обяснителния доклад към модернизираната Конвенция № 108 се пояснява, че възраженията срещу обработването на лични данни за целите на директен маркетинг следва да доведат до безусловно изтриване или премахване на въпросните лични данни[598].

Субектът на данни има правото да направи възражение срещу използването на личните му данни за целите на директен маркетинг безплатно и по всяко време. Субектите на данни трябва да бъдат уведомени за това право по ясен начин, отделно от всяка друга информация.

Право на възражение чрез автоматизирани средства

Когато лична информация се използва и обработва за услуги на информационното общество, субектът на данни може да упражни правото си на възражение срещу обработването на личните му данни чрез автоматизирани средства.

Под услуги на информационното общество се разбира каквато и да е услуга, нормално предоставяна срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба от получателя на услугите[599].

Администраторите на данни, които предлагат услуги на информационното общество, трябва да разполагат с подходящи технически средства и процедури, за да гарантират, че правото на възражение чрез автоматизирани средства може да бъде ефективно упражнено[600]. Например това може да включва блокиране на „бисквитки“ на уебстраници или изключване на функцията за проследяване при търсене в интернет.

597 Съвет на Европа, Комитет на министрите (1985 г.), Препоръка Rec(85)20 до държавите членки относно защитата на лични данни, използвани за целите на директен маркетинг, 25 октомври 1985 г., член 4, параграф 1.

598 Обяснителен доклад към модернизираната Конвенция № 108, параграф 79.

599 Директива 98/34/ЕО, изменена с Директива 98/48/ЕО относно определяне на процедура за предоставяне на информация в областта на техническите стандарти и правила, член 1, параграф 2.

600 Общ регламент относно защитата на данните, член 21, параграф 5.

Право на възражение срещу обработване на данни за целите на научни или исторически изследвания или статистически цели

Съгласно правото на ЕС научноизследователската дейност следва да се тълкува в по-широк смисъл и да включва например технологичното развитие и демонстрационни дейности, фундаменталните научни изследвания, приложните научни изследвания и частно финансираните научни изследвания[601]. Историческите изследвания включват и изследвания за генеалогични цели, като се има предвид, че регламентът не следва да се прилага за починали лица[602]. Статистически цели означава всяка операция по събиране и обработване на лични данни, необходими за статистически изследвания или за изготвяне на статистически резултати[603]. Законното основание за правото на възражение срещу обработване на лични данни за целите на научни изследвания отново е конкретното положение на субекта на данни[604]. Единственото изключение е, когато обработването е необходимо за изпълнението на задача от обществен интерес. Правото на изтриване обаче не се прилага, когато обработването е необходимо (независимо дали са налице причини от обществен интерес) за целите на научни или исторически изследвания или за статистически цели[605].

В ОРЗД се търси баланс между изискванията на научните, статистическите или историческите изследвания и правата на субектите на данни със специални гаранции и дерогации в член 89. Ето защо в правото на Съюза или в правото на държава членка може да бъдат предвидени дерогации от правото на възражение, доколкото има вероятност това право да направи невъзможно или сериозно да затрудни постигането на целите на изследванията и посочените дерогации са необходими за постигането на тези цели.

Съгласно **правото на Съвета на Европа** член 9, параграф 2 от модернизираната Конвенция № 108 установява, че по отношение на обработването на данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, в закон могат да бъдат предвидени ограничения на правата на субектите на данни, включително на правото на

601 *Пак там*, съображение 159.

602 *Пак там*, съображение 160.

603 *Пак там,* съображение 162.

604 *Пак там,* член 21, параграф 6.

605 *Пак там*, член 17, параграф 3, буква г).

възражение, когато не съществува очевиден риск от нарушаване на правата и основните свободи на субектите на данни.

В Обяснителния доклад (параграф 41) обаче също така се признава, че субектите на данни следва да имат възможност да дадат съгласието си само за определени области на научни изследвания или части от научноизследователски проекти, доколкото преследваната цел позволява това, и да възразят, ако считат, че обработването представлява прекомерна намеса в техните права и свободи без законово основание.

С други думи, такова обработване следва по принцип да се счита за съвместимо, при условие че съществуват и други гаранции и че по принцип операциите изключват всякакво използване на получената информация за вземане на решения или предприемане на мерки, които засягат конкретно лице.

6.1.7 Автоматизирано вземане на индивидуални решения, включително профилиране

Автоматизирани решения са решения, взети въз основа на лични данни, обработени само с автоматизирани средства, без никаква човешка намеса. **Съгласно правото на ЕС** субектът на данни не трябва да бъде обект на автоматизирани решения, които пораждат правни последствия или по подобен начин го засягат в значителна степен. Ако съществува вероятност такива решения да имат значително въздействие върху живота на лицата, като те касаят, например, тяхната кредитоспособност, наемането им на работа по електронен път, резултатите от работата им или анализите на поведението или надеждността им, е необходима специална защита с цел избягване на отрицателни последици. Автоматизираното вземане на решения включва „профилиране", което се състои от всякакви форми на автоматизирано оценяване на „личните аспекти във връзка с дадено физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите от работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията му"[606].

606 *Пак там,* съображение 71, член 4, параграф 4 и член 22.

Пример: За да направят бърза оценка на кредитоспособността на бъдещ клиент, агенциите за кредитна информация събират определени данни, като например как клиентът е обслужвал кредитите си и сметките си за комунални и други услуги, подробности за предходните адреси на клиента, както и информация от общодостъпни източници, като избирателни списъци, публични регистри (включително съдебни решения) или данни за обявяването му в неплатежоспособност и несъстоятелност. Тези лични данни впоследствие се вкарват в алгоритъм за оценка, който изчислява общата стойност, отговаряща на кредитоспособността на потенциалния клиент.

Според Работната група по член 29 правото на лицето да не бъде обект на решения, основани единствено на автоматизирано обработване, което може да породи правни последствия за субекта на данни или по подобен начин го засяга в значителна степен, се равнява на обща забрана и не изисква от субекта на данни активно да оспорва такова решение[607].

Въпреки това според ОРЗД автоматизираното вземане на решения, което поражда правни последствия за лицето или по подобен начин го засяга в значителна степен, може да бъде приемливо, ако е необходимо за сключването или изпълнението на договор между администратора на данни и субекта на данни, или ако субектът на данни е дал изричното си съгласие. Автоматизираното вземане на решения е приемливо и ако е разрешено от закона, и ако правата, свободите и законните интереси на субекта на данни са подходящо защитени[608].

ОРЗД също така предвижда, че задълженията на администратора относно информацията, която трябва да бъде предоставена при събирането на личните данни, включват и уведомяване на субектите на данни за съществуването на автоматизирано вземане на решения, включително профилиране[609]. Правото на достъп до личните данни, обработвани от администратора, остава незасегнато[610]. Уведомлението следва не просто да посочва факта, че ще

607 Работна група по член 29, *Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679*, WP 251, 3 октомври 2017 г., стр. 15.

608 Общ регламент относно защитата на данните, член 22, параграф 2.

609 *Пак там*, член 12.

610 *Пак там*, член 15.

бъде извършено профилиране, а да съдържа и съществена информация относно използваната логика при профилирането и предвидените последствия от това обработване за лицата[611]. Например здравноосигурително дружество, което използва автоматизирано вземане на решения относно заявленията, следва да предостави на субектите на данни обща информация как работи алгоритъмът и какви коефициенти използва той, за да изчисли застрахователните им премии. По подобен начин при упражняването на правото си на достъп субектите на данни могат да поискат информация от администратора за съществуването на автоматизирано вземане на решения, както и съществена информация относно използваната логика[612].

Информацията, предоставена на субектите на данни, е предназначена да осигури прозрачност и да им даде възможност да предоставят информирано съгласие, ако случаят е такъв, или да изискат човешка намеса. Администраторът на данни е длъжен да предприеме подходящи мерки, за да гарантира правата, свободите и законните интереси на субектите на данни. Това включва най-малко правото на човешка намеса от страна на администратора и възможността субектът на данните да изрази гледната си точка и да оспори решение, което се основава на автоматизирано обработване на личните му данни[613].

Работната група по член 29 е предоставила допълнителни насоки относно използването на автоматизирано вземане на решения съгласно ОРЗД[614].

Съгласно правото на Съвета на Европа лицата имат право да не бъдат обект на решение, което ги засяга в значителна степен и се основава единствено на автоматизирано обработване, без да се вземат предвид техните гледни точки[615]. Изискването да се вземат предвид гледните точки на субектите на данни, когато решенията се основават единствено на автоматизирано обработване, означава, че те имат право да оспорват такива решения и следва да могат да оспорват евентуални неточности в използваните от администратора

611 *Пак там*, член 13, параграф 2, буква е).

612 *Пак там*, член 15, параграф 1, буква з).

613 *Пак там*, член 22, параграф 3.

614 Работна група по член 29 (2017 г.), *Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679*, WP 251, 3 октомври 2017 г.

615 Модернизирана Конвенция № 108, член 9, параграф 1, буква а).

лични данни и релевантността на прилагания към тях профил[616]. Лицата обаче не могат да упражняват това право, ако автоматизираното решение е разрешено в закон, който е приложим спрямо администратора и в който се предвиждат и подходящи мерки за защита на правата, свободите и законните интереси на субектите на данни. Освен това субектите на данни имат право да бъдат уведомени за причините за извършваното обработване[617]. В Обяснителния доклад към модернизираната Конвенция № 108 се дава като пример изготвянето на оценката при кандидатстване за кредит. Лицата следва да имат право да знаят не само дали самото решение е положително или отрицателно, но също и *логиката*, залегнала при обработването на личните им данни, която е довела до това решение. „Разбирането на тези елементи допринася за ефективното упражняване на други съществени предпазни мерки, като правото на възражение и правото на подаване на жалба пред компетентен орган“[618].

Препоръката относно профилирането, макар и да не е правно обвързваща, определя условията за събирането и обработването на лични данни в контекста на профилирането[619]. Тя включва разпоредби относно необходимостта да се гарантира, че обработването на данни в контекста на профилирането следва да бъде добросъвестно, законосъобразно, пропорционално и за конкретни и легитимни цели. Тя също така съдържа разпоредби относно информацията, която администраторите следва да предоставят на субектите на данни. В препоръката е изтъкнат и принципът на качество на данните, който изисква администраторите да предприемат мерки да коригират факторите, които водят до неточности в личните данни, да ограничат рисковете или грешките, които профилирането може да предизвика, и периодично да оценяват качеството на използваните данни и алгоритми.

616 Обяснителен доклад към модернизираната Конвенция № 108, параграф 75.

617 Модернизирана Конвенция № 108, член 9, параграф 1, буква в).

618 Обяснителен доклад към модернизираната Конвенция № 108, параграф 77.

619 Съвет на Европа, Препоръка CM/Rec(2010)13 на Комитета на министрите до държавите членки относно защитата на лицата при автоматизираната обработка на лични данни в контекста на профилиране, член 5, параграф 5.

6.2 Средства за правна защита, отговорност за причинени вреди, санкции и обезщетения

Ключови въпроси

- Съгласно модернизираната Конвенция № 108 в националното законодателство на страните по нея трябва да се определят подходящи средства за правна защита и санкции срещу нарушенията на правото на защита на данните.
- В ЕС ОРЗД предвижда средства за правна защита за субектите на данни в случаите на нарушение на техните права, както и санкции за администраторите и обработващите лични данни, които не спазват разпоредбите на регламента. В регламента се предвижда също и право на обезщетение и отговорност за причинени вреди.
  - Субектите на данни имат право да подадат жалба до надзорен орган за предполагаеми нарушения на регламента, както и право на ефективна съдебна защита и на получаване на обезщетение.
  - При упражняването на правото си на ефективна съдебна защита физическите лица може да бъдат представлявани от организации с нестопанска цел, които действат в областта на защитата на личните данни.
  - Администраторът или обработващият лични данни е отговорен за всяка материална и нематериална вреда в резултат на нарушението.
  - Надзорните органи имат правомощието да налагат административни наказания „глоба“ или „имуществена санкция“ за нарушение на регламента в размер до 20 000 000 EUR или, в случай на предприятие — до 4 % от общия му годишен световен оборот, която от двете суми е по-висока.
- При определени условия физическите лица могат да подават оплаквания, свързани с нарушения на законодателството за защита на данните, пред ЕСПЧ в качеството му на последна инстанция.
- Всяко физическо или юридическо лице има правото да подава жалба срещу всяко от решенията на Европейския комитет по защита на данните пред Съда на ЕС при условията, предвидени в Договорите.

Приемането на правни инструменти не е достатъчно, за да се гарантира защита на личните данни в Европа. За да станат ефективни европейските правила за защита на данните, е необходимо да се установят механизми, които дават възможност на лицата да противодействат на нарушенията на техните

права и да търсят обезщетение за всяка претърпяна вреда. Също така е важно надзорните органи да имат правомощието да налагат санкции, които са ефективни, възпиращи и пропорционални на въпросното нарушение.

Правата по силата на законодателството за защита на данните могат да се упражняват от лицето, чиито права са изложени на риск; това трябва да е самият субект на данните. Все пак и други лица, които изпълняват необходимите изисквания по силата на националното законодателство, също може да представляват субектите на данни при упражняването на техните права. Съгласно редица национални законодателства децата и хората с интелектуални затруднения трябва да бъдат представлявани от своите настойници[620]. Съгласно правото на ЕС в областта на защитата на данните сдружение, чиято законна цел е да насърчава правата, свързани със защитата на данните, може да представлява субектите на данни пред надзорен орган или пред съда[621].

6.2.1 Право на подаване на жалба до надзорен орган

Както според **правото на Съвета на Европа**, така и според **правото на ЕС** лицата имат правото да подават искания и жалби до компетентния надзорен орган, ако считат, че обработването на личните им данни не се извършва в съответствие със закона.

В модернизираната Конвенция № 108 се признава правото на субектите на данни да се възползват от помощта на надзорен орган при упражняването на правата им по силата на конвенцията независимо от тяхното гражданство или местопребиваване[622]. Искане за помощ може да бъде отхвърлено само при извънредни обстоятелства, като субектите на данни не следва да покриват разходите и таксите, свързани с помощта[623].

Подобни разпоредби може да бъдат намерени и в правната система на ЕС. ОРЗД изисква надзорните органи да приемат мерки за улесняване на

620 FRA (2015 г.), Наръчник по европейско право в областта на правата на детето, Люксембург, Служба за публикации; FRA (2013 г.), Legal capacity of persons with intellectual disabilities and persons with mental health problems, Люксембург, Служба за публикации.

621 Общ регламент относно защитата на данните, член 80.

622 Модернизирана Конвенция № 108, член 18.

623 *Пак там*, членове 16—17.

подаването на жалбите, като например създаване на електронен формуляр за подаване на жалби[624]. Субектът на данни може да подаде жалба до надзорен орган в държавата членка на обичайно местопребиваване, място на работа или място на предполагаемото нарушение[625]. Жалбите трябва да бъдат разследвани, а надзорният орган трябва да информира засегнатото лице за резултата от производствата по неговия иск[626].

За възможни нарушения от страна на институции или органи на ЕС може да бъде уведомен Европейският надзорен орган по защита на данните[627]. При липса на отговор от ЕНОЗД в срок от шест месеца жалбата се счита за отхвърлена. Решенията на ЕНОЗД може да бъдат обжалвани пред Съда на ЕС по силата на Регламент (ЕО) № 45/2001, който задължава институциите и органите на ЕС да спазват правилата за защита на данните.

Трябва да съществува възможност за обжалване на решенията на национален надзорен орган пред съда. Това се отнася както за субектите на данни, така и за администраторите и обработващите лични данни, които са страна по производства пред надзорен орган.

Пример: През септември 2017 г. испанският орган за защита на данните налага глоба на Facebook за нарушаване на няколко разпоредби за защита на данните. Надзорният орган осъжда социалната мрежа за събирането, съхраняването и обработването на лични данни, включително специални категории лични данни, за рекламни цели и без съгласието на субектите на данни. Решението е взето въз основа на разследване, проведено по собствена инициатива на надзорния орган.

624 Общ регламент относно защитата на данните, член 57, параграф 2.

625 *Пак там*, член 77, параграф 1.

626 *Пак там*, член 77, параграф 2.

627 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

6.2.2 Право на ефективна съдебна защита

В допълнение към правото на жалба пред надзорния орган, физическите лица трябва да имат право на ефективна съдебна защита и на сезиране на съда. Правото на правна защита е добре установено в европейската правна традиция и е признато за основно право както съгласно член 47 от Хартата на основните права на ЕС, така и съгласно член 13 от ЕКПЧ[628].

В правото на ЕС предоставянето на ефективни правни средства за защита на субектите на данни в случай на нарушение на техните права е от важно значение, което е ясно както от разпоредбите на ОРЗД — които установяват правото на ефективна съдебна защита срещу надзорни органи, администратори и обработващи лични данни — така и от съдебната практика на Съда на ЕС.

Пример: В делото *Schrems*[629] Съдът на ЕС обявява решението относно адекватното ниво на защита на „сферата на неприкосновеност на личния живот" за невалидно. Това решение е позволило международно предаване на данни от ЕС към организации в САЩ, които сами са се сертифицирали по схемата за „сфера на неприкосновеност на личния живот". Съдът на ЕС счита, че схемата за „сфера на неприкосновеност на личния живот" има няколко недостатъка, които засягат основните права на гражданите на ЕС на защита на неприкосновеността на личния живот, на защита на личните данни и на ефективни правни средства за защита.

Що се отнася до нарушението на правата на неприкосновеност на личния живот и на защита на личните данни, Съдът на ЕС подчертава, че законодателството на САЩ разрешава на определени публични органи да имат достъп до прехвърляните лични данни от държавите членки към САЩ и да ги обработват по начин, който е несъвместим с първоначалната цел на прехвърлянето им и който надхвърля строго необходимото и пропорционалното за защитата на националната сигурност. По отношение на правото на ефективни средства за правна защита Съдът отбелязва, че субектите на данни не разполагат със средства за защита по административен или съдебен път, чрез които

628 Вж. например ЕСПЧ, *Karabeyoğlu/Турция*, № C-30083/10, 7 юни 2016 г.; ЕСПЧ, *Mustafa Sezgin Tanrıkulu/Турция*, № 27473/06, 18 юли 2017 г.

629 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

да получат достъп до засягащите ги данни и при необходимост данните да бъдат поправени или заличени. Съдът на ЕС заключава, че правна уредба, в която не се предвижда никаква възможност лицето да използва средства за правна защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни, „не зачита съществената съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата". Той подчертава, че наличието на средства за съдебна защита, които да гарантират спазването на правните норми, е неделимо свързано със съществуването на правовата държава.

Физическите лица, администраторите или обработващите лични данни, които искат да оспорят решение със задължителен характер на надзорен орган, могат да сезират съда[630]. Терминът „решение" следва да се тълкува в широк смисъл, като обхващащо упражняването на правомощията за разследване, даване на разрешение и корективните правомощия на надзорния орган или неговите решения за оставяне без разглеждане или отхвърляне на жалби. Предмет на съдебно производство обаче не може да бъдат мерки, които не са със задължителен характер, като становища или консултации, предоставени от надзорния орган[631]. Съдебните производства трябва да бъдат образувани пред съдилищата на държавата членка, в която е установен съответният надзорен орган[632].

В случаите, когато администратор или обработващ лични данни наруши правата на субектите на данни, те имат право да подадат жалба пред съда[633]. При производствата срещу администратор или обработващ лични данни е особено важно лицата да разполагат с избор къде да заведат дело. Те могат да изберат да направят това или в държавата членка, в която администраторът или обработващият лични данни е установен, или в държавата членка по обичайно местопребиваване на съответните субекти на данни[634]. Втората възможност значително улеснява физическите лица при упражняването на техните права, тъй като им позволява да заведат дело в държавата, в която пребивават, и в рамките на позната юрисдикция. Ограничаването на мястото

630 Общ регламент относно защитата на данните, член 78.

631 *Пак там*, съображение 143.

632 *Пак там*, член 78, параграф 3.

633 *Пак там*, член 79.

634 *Пак там*, член 79, параграф 2.

на производствата срещу администратори и обработващи лични данни до държавата членка, в които същите имат място на установяване, би могло да обезкуражи субектите на данни, пребиваващи в други държави членки, да заведат съдебно дело, тъй като това би довело до разходи за пътуване и други разходи, а производствата може да бъдат на чужд език и под чуждестранна юрисдикция. Единственото изключение се отнася до случаите, в които администраторът или обработващият лични данни е публичен орган и обработването на лични данни се извършва при изпълнението на публичните им правомощия. В такъв случай за предявяването на иск са компетентни само съдилищата на държавата на съответния публичен орган[635].

Докато в повечето случаи делата, свързани с правилата за защита на данните, се решават от юрисдикциите на държавите членки, някои от делата може да бъдат заведени пред Съда на ЕС. Първата възможност е, когато субект на данни, администратор, обработващ лични данни или надзорен орган иска да внесе иск за отмяна на решение на ЕКЗД. За иска обаче са приложими условията на член 263 от ДФЕС, което означава, че за да бъде допустим, въпросните физически лица и предприятия трябва да докажат, че решението на Комитета ги засяга пряко и лично.

Вторият сценарий засяга случаи, в които институции или органи на ЕС незаконно обработват лични данни. В случаите, в които институции на ЕС нарушават законодателството за защита на данните, субектите на данни могат да подадат иск директно пред Общия съд на ЕС (Общият съд е част от Съда на ЕС). На първа инстанция компетентен за жалбите за нарушения на законодателството на ЕС от институции на ЕС е Общият съд. Следователно жалби срещу ЕНОЗД, който е институция на ЕС, може да бъдат подавани и пред Общия съд[636].

Пример: В делото *Bavarian Lager*[637] дружеството отправя искане към Европейската комисия да му предостави достъп до пълния протокол от събрание, проведено от Комисията, за което се твърди, че се отнася до правни въпроси, свързани с дружеството. Комисията отхвърля заявлението за достъп на дружеството по съображения за по-висши

635 *Пак там.*

636 Регламент (ЕО) № 45/2001, член 32, параграф 3.

637 Съд на ЕС, C-28/08 P, *Европейска комисия/The Bavarian Lager Co. Ltd.* [голям състав], 29 юни 2010 г.

интереси, свързани със защитата на данните[638]. Съгласно член 32 от Регламента относно защитата на данните при обработването им от институции на ЕС Bavarian Lager подава жалба срещу това решение пред Първоинстанционния съд (предшественика на Общия съд). Със своето решение (дело T-194/04, *Bavarian Lager Co. Ltd/Комисия на европейските общности*) Първоинстанционният съд отменя решението на Комисията да отхвърли заявлението за достъп. Европейската комисия обжалва това решение пред Съда на ЕС.

Съдът постановява решение (в голям състав), с което отменя решението на Първоинстанционния съд и потвърждава отказа на Европейската комисия да удовлетвори заявлението за достъп до пълния протокол от събранието, за да се защитят личните данни на лицата, участвали в него. Съдът на ЕС счита, че Комисията правилно е отказала да разкрие тази информация, като се има предвид, че участниците не са дали съгласието си техните лични данни да бъдат разкривани. Освен това Bavarian Lager не е доказало необходимостта от получаване на достъп до тази информация.

На последно място, субектите на данни, надзорните органи, администраторите или обработващите лични данни могат в хода на производство на национално равнище да поискат от националния съд да изиска разяснение от Съда на ЕС относно тълкуването и валидността на актове на институции, органи, служби или агенции на ЕС. Подобни разяснения се наричат преюдициални заключения. Те не предлагат пряка правна защита на жалбоподателя, но позволяват на националните съдилища да гарантират, че прилагат правилното тълкуване на правото на ЕС. Благодарение именно на този механизъм на преюдициални заключения знакови дела, като *Digital Rights Ireland* и *Kärntner Landesregierung и други*[639], както и *Schrems*[640], които повлияха в значителна степен върху развитието на правото на ЕС в областта на защитата на данните, достигнаха до Съда на ЕС.

638 За анализ на мотивите вж. ЕНОЗД (2011 г.), *Публичен достъп до съдържащи лични данни документи след решението по делото Bavarian Lager*, Брюксел, ЕНОЗД.

639 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

640 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

Пример: Съединени дела *Digital Rights Ireland* и *Kärntner Landesregierung и други*[641] са представени от ирландския High Court и австрийския Конституционен съд и се отнасят до съответствието на Директива 2006/24/ЕО (Директива за запазване на лични данни) със законодателството на ЕС в областта на защитата на данните. Австрийският Конституционен съд поставя на Съда на ЕС въпроси за валидността на членове 3—9 от Директива 2006/24/ЕО във връзка с членове 7, 9 и 11 от Хартата на основните права на ЕС. Въпросите включват дали определени разпоредби на австрийския федерален Закон за далекосъобщенията, с който се транспонира Директивата за запазване на лични данни, са несъвместими с елементи от предходната Директива за защита на личните данни и с Регламента относно защитата на данните при обработването им от институции на ЕС.

В делото *Kärntner Landesregierung и други* г-н Seitlinger, един от жалбоподателите по производството пред Конституционния съд, заявява, че използва телефона, интернет и електронната си поща както за служебни цели, така и в личния си живот. Следователно информацията, която изпраща и получава, минава през обществени далекосъобщителни мрежи. По силата на австрийския Закон за далекосъобщенията от 2003 г. неговият доставчик на далекосъобщителни услуги има законово задължение да събира и съхранява данни относно начина, по който той използва мрежата. Г-н Seitlinger счита, че това събиране и съхранение на личните му данни не е технически необходимо за изпращането и получаването на информация чрез мрежата. Събирането и съхранението на тези данни не е необходимо дори за целите на фактурирането. Г-н Seitlinger заявява, че не е дал съгласието си за използването по такъв начин на личните му данни, които са били събирани и съхранявани единствено на основание на австрийския Закон за далекосъобщенията от 2003 г.

Поради това г-н Seitlinger подава жалба пред австрийския Конституционен съд, в която твърди, че законовите задължения на неговия доставчик на далекосъобщителни услуги нарушават основните му права по член 8 от Хартата на основните права на ЕС. Като се има предвид, че в австрийското законодателство е въведено

641 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

правото на ЕС (тогавашната Директива за запазване на лични данни), Конституционният съд на Австрия отнася въпроса до Съда на ЕС, за да се произнесе относно съвместимостта на директивата с правата на неприкосновеност на личния живот и на защита на личните данни, залегнали в Хартата на основните права на ЕС.

Съдът на ЕС (голям състав) се произнася по делото, което води до отмяната на европейската Директива за запазване на лични данни. Съдът на ЕС констатира, че от директивата произтича особено тежка намеса в основните права на неприкосновеност на личния живот и на защита на личните данни, без тази намеса да е сведена до строго необходимото. Директивата преследва легитимна цел, тъй като предоставя на националните органи допълнителни възможности за разследването и наказателното преследване на тежки престъпления, поради което е полезен инструмент за разследването на престъпления. Съдът на ЕС обаче отбелязва, че ограничения на основните права следва да се прилагат само ако това е строго необходимо и следва да се придружават от ясни и точни правила относно техния обхват, както и от гаранции за физическите лица.

Според Съда на ЕС директивата не отговаря на критерия за необходимост. На първо място, тя не е установила ясни и точни правила, които да ограничават степента на намесата. Вместо да изисква наличието на връзка между запазваните данни и тежки престъпления, директивата е приложима за всички метаданни на всички потребители на всички електронни съобщителни средства. Следователно тя представлява намеса в правата на неприкосновеност на личния живот и на защита на личните данни на практически цялото население на ЕС, което може да се счита за непропорционално. Тя не съдържа условия за ограничаване на лицата, упълномощени да имат достъп до личните данни, нито този достъп е предмет на процедурни условия, като например изискване да е налице одобрение от административен орган или съд, преди той да бъде получен. Накрая, в директивата не са определени ясни гаранции за защита на запазените данни.

> Следователно тя не гарантира ефективна защита на данните срещу риска от злоупотреба и срещу всеки незаконен достъп и използване на данните[642].

По принцип Съдът на ЕС трябва да отговори на поставените въпроси и не може да откаже да даде преюдициално заключение с аргумента, че отговорът няма да е съотносим спрямо изходното дело, нито своевременен. Въпреки това той може да откаже, ако въпросът не попада в обхвата на неговата компетентност[643]. Съдът на ЕС излиза с решение само относно основните елементи на искането за преюдициално заключение, докато националният съд запазва своята компетентност да излезе с решение по изходното дело[644].

Съгласно правото на Съвета на Европа договарящите се страни трябва да предвидят подходящи съдебни и извънсъдебни средства за защита по отношение на нарушенията на разпоредбите на модернизираната Конвенция № 108[645]. Твърдения за нарушения на правата на защита на данните, които противоречат на член 8 от ЕКПЧ, срещу страна по ЕКПЧ може допълнително да бъдат внасяни в ЕСПЧ след изчерпване на всички достъпни средства за правна защита на национално равнище. Внасянето на жалба за нарушение на член 8 от ЕКПЧ пред ЕСПЧ трябва също така да отговаря и на други критерии за допустимост (членове 34—35 от ЕКПЧ)[646].

Въпреки че молбите до ЕСПЧ могат да се отнасят единствено до договарящи се страни, те могат частично да касаят действия или бездействия на частни лица, доколкото договарящата се страна не е изпълнила задълженията си по силата на ЕКПЧ и не е предоставила в своето национално законодателство достатъчна защита срещу нарушения на правата на защита на личните данни.

642 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г., параграф 69.

643 Съд на ЕС, C-244/80, *Pasquale Foglia/Mariella Novello (№ 2)*, 16 декември 1981 г.; и Съд на ЕС, C-467/04, *Наказателно производство срещу Gasparini и други*, 28 септември 2006 г.

644 Съд на ЕС, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union/Viking Line ABP, OÜ Viking Line Eesti* [голям състав], 11 декември 2007 г., параграф 85.

645 Модернизирана Конвенция № 108, член 12.

646 ЕКПЧ, членове 34—37.

Пример: Жалбоподателят по делото *K.U./Финландия*[647] е непълнолетно лице, което се оплаква, че на уебсайт за запознанства е публикувана обява със сексуален характер за него. Доставчикът на интернет услуги не разкрива самоличността на лицето, което е публикувало обявата, като се позовава на предвидените във финландското законодателство задължения за поверителност на информацията. Жалбоподателят твърди, че националното законодателство не предоставя достатъчна защита от действията на частно лице, което е публикувало в интернет данни, увреждащи интересите на жалбоподателя. ЕСПЧ постановява, че държавите не само са длъжни да се въздържат от произволна намеса в личния живот на хората, но имат и позитивни задължения, които включват „приемането на мерки, насочени да гарантират зачитането на неприкосновеността на личния живот дори в отношенията на лицата между самите тях". В случая на жалбоподателя неговата действена и ефективна защита предполага предприемане на ефективни действия за идентифициране и наказателно преследване на извършителя. Такава защита обаче не е била предприета от държавата и Съдът излиза със заключение, че в този случай е налице нарушение на член 8 от ЕКПЧ.

Пример: В делото *Köpke/Германия*[648] жалбоподателката е била заподозряна в извършване на кражба на работното си място и е била подложена на скрито видеонаблюдение. ЕСПЧ заключава, че „нищо не сочи, че местните органи не са успели да осигурят подходящ баланс, в рамките на своята възможност за преценка, между правото на зачитане на неприкосновеността на личния живот на жалбоподателката съгласно член 8, от една страна, и интереса на работодателя да защити своите права на собственост и обществения интерес, свързан с доброто правораздаване, от друга страна". Поради това молбата е обявена за недопустима.

Ако ЕСПЧ постанови, че договаряща се страна по конвенцията е нарушила някое от правата, защитени от ЕКПЧ, тази договаряща се страна по конвенцията е длъжна да изпълни решението на ЕСПЧ (член 46 от ЕКПЧ). Мерките за изпълнение трябва на първо място да прекратяват нарушението и да отстраняват, доколкото това е възможно, отрицателните последици за жалбоподателя. Изпълнението на решенията може да изисква също прилагането на

647 ЕСПЧ, *K.U./Финландия*, № 2872/02, 2 декември 2008 г.

648 ЕСПЧ, *Köpke/Германия* (реш.), № 420/07, 5 октомври 2010 г.

общи мерки за предотвратяване на нарушения, подобни на установените от Съда, било чрез промяна в законодателството, съдебна практика или други мерки.

В член 41 от ЕКПЧ се предвижда, че ако ЕСПЧ установи нарушение на ЕКПЧ, той може да постанови предоставянето на „справедлива компенсация" на потърпевшата страна за сметка на договарящата се страна.

Право на възлагане на подаването на жалба на структура, организация или сдружение с нестопанска цел

ОРЗД дава възможност на физическите лица, които искат да подадат жалба пред надзорен орган или да заведат дело в съда, да възложат на структура, организация или сдружение с нестопанска цел да ги представлява[649]. Тези субекти с нестопанска цел трябва да имат уставни цели, които са от обществен интерес, и да работят в областта на защитата на личните данни. Те може да подадат жалбата или да упражнят правото на съдебна защита от името на субекта на данни. Регламентът дава възможност на държавите членки да решат, в съответствие с националното си законодателство, дали дадена структура може да подава жалби от името на субектите на данните, без това да ѝ е било възложено от тях.

Това право на представителство дава възможност на физическите лица да се възползват от експертните знания и организационния и финансовия капацитет на тези предприятия с нестопанска цел, като този начин значително улеснява физическите лица при упражняването на техните права. ОРЗД допуска тези предприятия да завеждат колективни искове от името на множество субекти на данни. Това е от полза и за функционирането и ефективността на съдебната система, тъй като сходни искове се групират и се разглеждат заедно.

6.2.3 Отговорност и право на обезщетение

Правото на ефективни правни средства за защита трябва да оправомощава физическите лица да претендират за обезщетение за всяка претърпяна вреда в резултат на обработване на личните им данни по начин, който нарушава приложимото законодателство. Отговорността на администраторите

649 Общ регламент относно защитата на данните, член 80.

и обработващите лични данни за незаконно обработване е призната изрично в ОРЗД[650]. Регламентът дава право на физическите лица да получат обезщетение от администратора или от обработващия лични данни както за материални, така и за нематериални вреди, като в съображенията на регламента е определено, че „понятието „вреда“ следва да се тълкува в по-широк смисъл в контекста на съдебната практика на Съда по начин, който отразява напълно целите на настоящия регламент“[651]. Администраторите носят отговорност и могат да бъдат обект на искове за обезщетение, ако не спазват задълженията си съгласно регламента. Обработващият лични данни носи отговорност за вреди, произтичащи от извършеното обработване, само когато не е изпълнил задълженията по регламента, конкретно насочени към обработващите лични данни, или когато е действал извън законосъобразните указания на администратора или в противоречие с тях. Ако администратор или обработващ лични данни е изплатил пълното обезщетение, ОРЗД предвижда, че той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция по обработване на лични данни, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда[652]. В същото време освобождаването от отговорност е при много строги условия, като трябва да се докаже, че администраторът или обработващият лични данни по никакъв начин не е отговорен за събитието, причинило вредата.

Обезщетението за претърпяната вреда трябва да е „пълно и действително“. Когато вредата е причинена от обработване, извършвано от няколко администратора или обработващи лични данни, всеки администратор или обработващ лични данни трябва да носи отговорност за цялата вреда. Това правило цели да гарантира действително обезщетение за субектите на данни и координиран подход за спазването на регламента от страна на участващите в дейности по обработване администратори и обработващи лични данни.

Пример: От субектите на данни не се изисква да завеждат дело и да претендират за обезщетение от всички субекти, отговорни за вредата, тъй като това може да доведе до скъпи и продължителни производства. Достатъчно е да се заведе дело срещу един от съвместните администратори, от когото след това може да се търси отговорност

650 *Пак там*, член 82.

651 *Пак там*, съображение 146.

652 *Пак там*, член 82, параграфи 2 и 5.

за цялата вреда. В тези случаи администраторът или обработващият лични данни, който изплати обезщетението, има право заплатената сума впоследствие да му бъде възстановена от другите субекти, участвали в обработването и отговорни за нарушението, за тяхната част от отговорността за нанесената вреда. Тези производства между различните съвместни администратори и обработващи лични данни се водят, след като субектът на данни вече е получил обезщетението, като самият субект на данни не е част от тях.

В правната рамка на Съвета на Европа член 12 от модернизираната Конвенция № 108 изисква договарящите се страни да установят подходящи правни средства за защита по отношение на нарушенията на националното законодателство, с което са въведени изискванията на конвенцията. В Обяснителния доклад към модернизираната Конвенция № 108 се посочва, че правните средства за защита трябва да включват възможността за оспорване по съдебен път на дадено решение или практика, като същевременно трябва да се предоставят и извънсъдебни средства за защита[653]. Условията и различните правила, свързани с достъпа до тези правни средства за защита, както и процедурите, които трябва да бъдат следвани, са оставени на преценката на всяка от договарящите се страни. Договарящите се страни и националните съдилища следва също така да разгледат възможността за въвеждане на разпоредби за финансови обезщетения за материални и нематериални вреди, причинени от обработването, както и възможността за завеждане на колективни искове[654].

6.2.4 Санкции

В правото на Съвета на Европа член 12 от модернизираната Конвенция № 108 предвижда, че всяка договаряща се страна се задължава да установи съответстващи санкции и компенсации при нарушаване на разпоредбите на вътрешното право, с които се въвеждат в действие основните принципи за защита на данните, залегнали в Конвенция № 108. В конвенцията не се установява или налага конкретен набор от санкции. Напротив, в нея ясно се посочва, че всяка договаряща се страна има свободата да определи естеството на съдебните или извънсъдебните санкции, които може да бъдат наказателни, административни или граждански. В обяснителния доклад към

653 Обяснителен доклад към модернизираната Конвенция 108, параграф 100.

654 *Пак там*.

модернизираната Конвенция № 108 се предвижда, че санкциите трябва да бъдат ефективни, пропорционални и възпиращи[655]. Договарящите се страни трябва да зачитат този принцип при определянето на естеството и тежестта на санкциите във вътрешния си правен ред.

В правото на ЕС член 83 от ОРЗД оправомощава надзорните органи на държавите членки да налагат административно наказание „глоба“ или „имуществена санкция“ за нарушения на регламента. Размерът на наказанията „глоба“ или „имуществена санкция“, обстоятелствата, които националните органи вземат предвид, когато решават дали да наложат такова наказание, и общият максимален размер на тези наказания също са предвидени в член 83. По този начин режимът на санкциониране е хармонизиран в целия ЕС.

В ОРЗД се следва стъпаловиден подход за налагането на наказанията „глоба“ или „имуществена санкция“. Надзорните органи имат правомощието да налагат административни наказания „глоба“ или „имуществена санкция“ за нарушение на регламента в размер до 20 000 000 EUR или, в случай на предприятие — до 4 % от общия му годишен световен оборот, която от двете суми е по-висока. Нарушенията, които могат да доведат до такъв размер на наказанието „глоба“ или „имуществена санкция“, включват неспазване на основните принципи за обработване на лични данни и на условията, свързани с даването на съгласие, неспазване на правата на субектите на данни и на разпоредбите на регламента, които уреждат предаването на лични данни на получатели в трети държави. За други нарушения надзорните органи могат да налагат наказания „глоба“ или „имуществена санкция“ до 10 000 000 EUR или, в случай на предприятие — до 2 % от общия му годишен световен оборот, която от двете суми е по-висока.

При определянето на вида и размера на наказанието „глоба“ или „имуществена санкция“, което трябва да бъде наложено, надзорните органи трябва да вземат предвид редица елементи[656]. Например те трябва надлежно да разгледат естеството, тежестта и продължителността на нарушението, засегнатите категории лични данни и дали нарушението е извършено умишлено или по небрежност. Когато администратор или обработващ лични данни е предприел действия за смекчаване на последиците от вредите, претърпени от субектите на данни, това също следва да бъде взето предвид. Други важни

655 *Пак там*.

656 Общ регламент относно защитата на данните, член 83, параграф 2.

елементи, които ръководят надзорните органи при вземането на тяхното решение, са степента на сътрудничество с надзорния орган след извършване на нарушението и начинът, по който нарушението е станало известно на надзорния орган (например дали то е докладвано от предприятието, отговорно за обработването, или от субекта на данни, чиито права са били нарушени)[657].

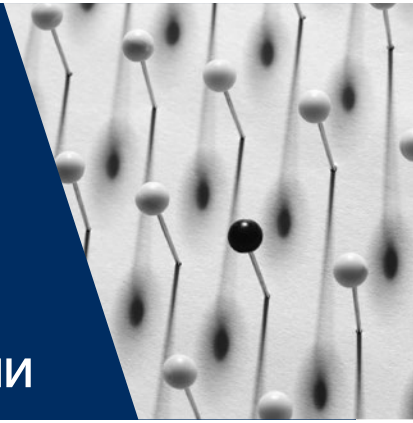
В допълнение към възможността да налагат административни наказания „глоба" или „имуществена санкция" надзорните органи разполагат и с широк кръг от други корективни правомощия. Така наречените „корективни" правомощия на надзорните органи са определени в член 58 от ОРЗД. Те варират от издаването на разпореждания и отправянето на предупреждения и официални предупреждения до администраторите и обработващите лични данни до налагането на временна или дори постоянна забрана на дейностите по обработване на данни.

Що се отнася до санкциите за нарушения на правото на ЕС от страна на институции или органи на ЕС, поради специалния обхват на компетентност на Регламента относно защитата на данните при обработването им от институции на ЕС, санкции може да бъдат предвидени под формата на дисциплинарни мерки. Съгласно член 49 от регламента „всяко неспазване на задълженията съгласно настоящия регламент от страна на служител или друго длъжностно лице на Европейските общности, независимо дали преднамерено или по непредпазливост, води до дисциплинарни санкции [...]".

657 Работна група по член 29 (2017 г.), *Насоки относно прилагането и определянето на административните наказания „глоба" или „имуществена санкция" за целите на Регламент 2016/679*, WP 253, 3 октомври 2017 г.

7

Международно предаване на данни и потоци от лични данни



ЕС	Обхванати въпроси	СЕ
Предаване на лични данни		
Общ регламент относно защитата на данните, член 44	Понятие	Модернизирана Конвенция № 108, член 14, параграфи 1 и 2
Свободно движение на лични данни		
Общ регламент относно защитата на данните, член 1, параграф 3 и съображение 170	Между държави членки на ЕС	
	Между договарящи се страни по Конвенция № 108	Модернизирана Конвенция № 108, член 14, параграф 1
Предаване на лични данни на трети държави или международни организации		
Общ регламент относно защитата на данните, член 45 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 2015 г.	Решение относно адекватното ниво на защита/трети държави или международни организации с подходящо ниво на защита	Модернизирана Конвенция № 108, член 14, параграф 2
Общ регламент относно защитата на данните, член 46, параграф 1 и член 46, параграф 2	Подходящи гаранции, включително приложими права и правни средства за защита на субектите на данни, предвидени чрез стандартни договорни клаузи, задължителни фирмени правила, кодекси за поведение и механизми за сертифициране	Модернизирана Конвенция № 108, член 14, параграфи 2, 3, 5 и 6

ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните, член 46, параграф 3	**След получаване на разрешение от компетентния надзорен орган: договорни клаузи и разпоредби, включени в административните договорености между публичните органи**	
Общ регламент относно защитата на данните, член 46, параграф 5	**Съществуващи разрешения въз основа на Директива 95/46**	
Общ регламент относно защитата на данните, член 47	**Задължителни фирмени правила**	
Общ регламент относно защитата на данните, член 49	**Дерогации в особени случаи**	Модернизирана Конвенция № 108, член 14, параграф 4
Примери: Споразумение между ЕС и САЩ относно резервационните данни на пътниците Споразумение между ЕС и САЩ относно SWIFT	**Международни споразумения**	Модернизирана Конвенция № 108, член 14, параграф 3, буква а)

Съгласно правото на ЕС Общият регламент относно защитата на данните предвижда свободното движение на данни в рамките на Европейския съюз. Той обаче съдържа специфични изисквания относно предаването на лични данни към трети държави извън ЕС и към международни организации. Регламентът признава важността на това предаване, особено с оглед на международната търговия и сътрудничество, но признава и увеличения риск по отношение на личните данни. По тази причина регламентът има за цел да предложи на личните данни, които се предават към трети държави, същото ниво на защита, каквото те имат в рамките на ЕС[658]. В правото на Съвета на Европа също се признава колко е важно да бъдат въведени правила за трансграничните потоци от данни, които се основават на свободно движение между страните по конвенцията и специфични изисквания за предаването на данни към държави, които не са страни по конвенцията.

658 Общ регламент относно защитата на данните, съображения 101 и 116.

7.1 Същност на предаването на лични данни

Ключови въпроси

- В законодателствата на ЕС и на Съвета на Европа се съдържат правила относно предаването на лични данни към получатели в трети държави или към международни организации.
- Гарантирането на защитата на правата на субекта на данни при предаването на данни извън ЕС дава възможност защитата, осигурена от правото на ЕС, да следва личните данни с произход от ЕС.

В **правото на Съвета на Европа** трансграничното движение на данни е описано като предаване на лични данни към получатели, които са субекти на чуждестранна юрисдикция[659]. Трансграничното движение на данни към получател, който не е субект на юрисдикцията на договаряща се страна, е разрешено само ако е налице подходящо ниво на защита[660].

Правото на ЕС урежда предаването „на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация[...]"[661]. Такова движение на данни е разрешено само ако се спазват правилата, определени в глава V от ОРЗД.

Допускат се трансгранични потоци от лични данни към получател, който е субект на юрисдикция съответно на договаряща се страна по конвенцията съгласно правото на Съвета на Европа или на държава членка съгласно правото на ЕС. И двете правни системи също така разрешават данни да бъдат предавани към държава, която не е договаряща се страна по конвенцията или държава членка, ако са изпълнени определени условия.

659 Обяснителен доклад към модернизираната Конвенция № 108, параграф 102.

660 Модернизирана Конвенция № 108, член 14, параграф 2.

661 Общ регламент относно защитата на данните, член 44.

7.2 Свободно движение/потоци от лични данни между държави членки или договарящи се страни

Ключови въпроси

- Движението на лични данни в целия ЕС, както и предаването на лични данни между договарящите се страни по модернизираната Конвенция № 108 трябва да бъде без ограничения. Тъй като обаче не всички договарящи се страни по модернизираната Конвенция № 108 са държави членки на ЕС, предаването на данни от държава членка на ЕС към трета държава, макар и тя да е договаряща се страна по модернизираната Конвенция № 108, не е възможно освен ако не са спазени условията, определени в ОРЗД.

Съгласно правото на Съвета на Европа трябва да е налице свободно движение на лични данни между договарящите се страни по модернизираната Конвенция № 108. Предаването на данни обаче може да бъде забранено, ако съществува „реален и сериозен риск трансферът до другата страна да доведе до заобикаляне на разпоредбите на Конвенцията“ или ако дадена страна е задължена да направи това поради „хармонизирани правила за защита, споделяни от държави, които принадлежат към регионална международна организация“[662].

Съгласно правото на ЕС са забранени ограниченията или забраните на свободното движение на лични данни между държавите членки на ЕС по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни[663]. Зоната на свободното движение на данни е разширена със Споразумението за Европейското икономическо пространство (ЕИП)[664], с което Исландия, Лихтенщайн и Норвегия се включват във вътрешния пазар.

662 Модернизирана Конвенция № 108, член 14, параграф 1.

663 Общ регламент относно защитата на данните, член 1, параграф 3.

664 Решение на Съвета и на Комисията от 13 декември 1993 г. за сключване на Споразумението за Европейското икономическо пространство между Европейските общности, техните държави членки и Република Австрия, Република Финландия, Република Исландия, Княжество Лихтенщайн, Кралство Норвегия, Кралство Швеция и Конфедерация Швейцария, ОВ L 1, 3.1.1994 г.

Пример: Ако съдружник в международна група от дружества, установени в няколко държави членки, сред които Словения и Франция, предава лични данни от Словения на Франция, подобен поток от данни не трябва да се ограничава или забранява от словенското национално законодателство по причини, свързани със защитата на личните данни.

Ако обаче същият словенски съдружник иска да предаде същите лични данни на дружеството майка в Малайзия, тогава словенският износител на данни трябва да вземе предвид правилата, установени в глава V от ОРЗД. Тази разпоредби са предназначени да защитят личните данни на субектите на данни, които са субект на юрисдикцията на ЕС.

Съгласно правото на ЕС потоците от лични данни към държави членки на ЕИП за цели, свързани с предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции, са предмет на Директива 2016/680[665]. Това също така гарантира, че обменът на лични данни от страна на компетентните органи в рамките на Съюза не се ограничава, нито забранява по причини, свързани със защитата на данните. Съгласно правото на Съвета на Европа обработването на всички лични данни (включително трансграничното им движение към други страни по Конвенция № 108) — без да има изключения на основание цели или области на действие — е включено в приложното поле на Конвенция № 108, макар че самите договарящи се страни може да предвидят изключения. Всички членове на ЕИП са страни и по Конвенция № 108.

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

7.3 Предаване на лични данни на трети държави/държави, които не са страни по конвенцията, или на международни организации

Ключови въпроси

- Както **Съветът на Европа**, така и **ЕС** разрешават предаване на лични данни на трети държави или на международни организации, ако са спазени определени условия за защита на личните данни.
  - **Съгласно правото на Съвета на Европа** подходящо ниво на защита може да бъде постигнато чрез законодателството на съответната държава или международна организация или чрез въвеждане на подходящи стандарти.
  - **Съгласно правото на ЕС** предаване на данни може да се осъществява, ако третата държава гарантира достатъчна степен на защита или ако администраторът или обработващият лични данни осигурят подходящи гаранции, включващи приложими права на субектите на данни и средства за правна защита, чрез използването на средства, като стандартни клаузи за защита на данните или задължителни фирмени правила.
- Както **правото на Съвета на Европа, така и правото на ЕС** предвиждат клаузи за дерогация, които допускат предаване на лични данни при специални обстоятелства, дори когато не са налице нито достатъчна степен на защита, нито подходящи гаранции.

Въпреки че и правото на Съвета на Европа, и правото на ЕС допускат движение на данни към трети държави или международни организации, те определят различни условия за това. Всеки набор от условия отчита различната структура и цели на съответната организация.

Съгласно **правото на ЕС** принципно съществуват два начина за допускане на предаването на лични данни към трети държави или към международни организации. Лични данни може да се предават въз основа на: решение на Европейската комисия относно адекватното ниво на защита[666] или, при липса на такова решение, когато администраторът или обработващият лични данни осигури подходящи гаранции, включително приложими права и правни

666 Общ регламент относно защитата на данните, член 45.

средства за защита на субекта на данни[667]. При липсата както на решение относно адекватното ниво на защита, така и на подходящи гаранции са налице редица дерогации.

Съгласно **правото на Съвета на Европа** обаче свободното предаване на данни към държави, които не са страни по конвенцията, се допуска само въз основа на:

- правото на тази държава или международна организация, включително приложимите международни договори или споразумения, които осигуряват подходящи гаранции;

- специални или одобрени стандартизирани гаранции, предоставени от правно обвързващи и приложими инструменти, приети и приложени от лицата, които участват в предаването и по-нататъшното обработване на лични данни[668].

Подобно на правото на ЕС, при липсата на подходящо ниво на защита на данните са налице редица дерогации.

7.3.1 Предаване на данни въз основа на решение относно адекватното ниво на защита

Съгласно правото на ЕС свободното движение на лични данни към трети държави с адекватно ниво на защита на данните е предвидено в член 45 от ОРЗД. Съдът на ЕС пояснява, че терминът „достатъчна степен на защита" изисква третата държава да гарантира степен на защита на основните права и свободи, която „по същество е равностойна"[669] на гаранциите, осигурени от правото на ЕС. В същото време средствата, които една трета държава може да използва с цел осигуряване на такава степен на защита, може да се различават от тези, използвани в рамките на ЕС; стандартът за адекватно ниво на защита не изисква буквалното възпроизвеждане на правилата на ЕС[670].

667 *Пак там*, член 46.

668 Модернизирана Конвенция № 108, член 14, параграф 3, букви а) и б).

669 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г., параграф 96.

670 *Пак там*, параграф 74. Вж. също Европейска комисия (2017 г.), Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят", COM(2017) 7 окончателен, 10 януари 2017 г., стр. 6.

Европейската комисия оценява нивото на защита на данните в третите държави, като прави преглед на техните национални законодателства и приложими международни задължения. Участието на държавата в многостранни или регионални системи, по-специално в такива, които са свързани със защитата на личните данни, също трябва да бъде взето предвид. Ако Европейската комисия прецени, че третата държава или международната организация осигурява адекватно ниво на защита, тя може да издаде решение относно адекватното ниво на защита, което е със задължителен характер[671]. Въпреки това Съдът на ЕС посочва, че националните надзорни органи продължават да са компетентни да разглеждат искането на лице, отнасящо се до защита на личните му данни, които са били предадени на трети държави, счетени от Комисията за осигуряващи достатъчна степен на защита, когато това лице твърди, че действащите в момента право и практики в третата държава не гарантират достатъчна степен на защита[672].

Европейската комисия може да оцени и наличието на адекватна защита в рамките на дадена територия в трета държава или да се ограничи до конкретни сектори, какъвто беше например случаят относно законодателството за частна търговия в Канада[673]. По отношение на предаването на данни въз основа на споразумения между ЕС и трети държави се издават и констатации за нивото на адекватна защита. Тези решения се отнасят единствено за еднократно предаване на данни, каквото е предаването на резервационни данни на пътниците от авиокомпаниите към чуждестранните органи за граничен контрол, когато авиокомпанията осъществява полети от ЕС до определени отвъдморски дестинации (вж. раздел 7.3.4).

Решенията относно адекватното ниво на защита са обект на постоянно наблюдение. Европейската комисия прави редовни прегледи на тези решения, за да проследи развитията, които биха могли да повлияят на техния статут. По този начин, ако Европейската комисия констатира, че третата държава или международната организация вече не отговаря на условията, обосновали вземането

671 За постоянно актуализиран списък на държавите, които са получили констатация за осигуряване на адекватна защита, вж. началната интернет страница на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия.

672 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г., параграфи 63 и 65—66.

673 Европейска комисия (2002 г.), Решение 2002/2/ЕО от 20 декември 2001 г. относно констатиране съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета нивото на адекватна защита на личните данни, осигурявано от канадския Закон за защита на личните данни и електронните документи, ОВ L 2, 4.1.2002 г.

на решението относно адекватното ниво на защита, тя може да измени или да отмени решението, или да спре неговото прилагане. Комисията може също така да започне преговори със засегнатата трета държава или международна организация, за да се разреши проблемът, довел до нейното решение.

Решенията относно адекватното ниво на защита, приети от Комисията въз основа на Директива 95/46/ЕО, остават в сила, докато не бъдат изменени, заменени или отменени с решение на Комисията, прието в съответствие с правилата на член 45 от ОРЗД.

Към днешна дата Европейската комисия е признала Андора, Аржентина, Канада (търговските организации, попадащи в обхвата на Закона за личните данни и електронните документи — PIPEDA), Фарьорските острови, остров Гърнзи, остров Ман, Израел, остров Джърси, Нова Зеландия, Швейцария и Уругвай за осигуряващи адекватно ниво на защита. По отношение на предаването на данни към САЩ Европейската комисия е приела решение относно адекватното ниво на защита през 2000 г., което разрешава предаване на данни към предприятия, които сами са се сертифицирали, че ще защитават личните данни, предавани от ЕС, и ще спазват така наречените „принципи за сфера на неприкосновеност на личния живот“[674]. През 2015 г. Съдът на ЕС обяви това решение за невалидно и през юли 2016 г. беше прието ново решение относно адекватното ниво на защита, позволяващо предприятията да се присъединят към механизма от 1 август 2016 г.

Пример: В делото *Schrems*[675] Maximilian Schrems, австрийски гражданин, е потребител на Facebook в продължение на няколко години. Предоставените от г-н Schrems данни на Facebook изцяло или частично са били прехвърлени от ирландското дъщерно дружество на Facebook върху разположени на територията на САЩ сървъри, където се обработват. Г-н Schrems подава жалба до ирландския надзорен орган, тъй като счита, че предвид направените разкрития от г-н Едуард

674 Решение 2000/520/ЕО на Комисията от 26 юли 2000 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета 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. Решението е обявено за невалидно от Съда на ЕС с решението по дело C-362/14, *Maximilian Schrems/Data Protection Commissioner* [голям състав].

675 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

Сноудън, подал сигнали за нарушения американски гражданин относно дейностите по наблюдение на разузнавателните служби на САЩ, правото и практиките на САЩ не предоставят достатъчна защита на прехвърляните към тази страна данни. Ирландският орган отхвърля жалбата по-специално с довода, че в решението си от 26 юли 2000 г. Комисията е приела, че в рамките на т.нар. схема за „сфера на неприкосновеност на личния живот" САЩ гарантират достатъчна степен на защита на прехвърляните лични данни. Върховният съд на Ирландия е сезиран със случая и отправя преюдициално запитване до Съда на ЕС.

Съдът на ЕС постановява, че решението на Комисията относно адекватността на рамката за „сферата на неприкосновеност на личния живот" е невалидно. Съдът на ЕС най-напред отбелязва, че решението позволява прилагането на „принципите за сфера на неприкосновеност на личния живот" да бъде ограничено с оглед спазване на изискванията, свързани с националната сигурност, с обществения интерес и с правоприлагането, или въз основа на вътрешното законодателство на САЩ. Следователно решението прави възможна намесата в упражняването на основните права на лицата, чиито лични данни се прехвърлят или биха могли да се прехвърлят към САЩ[676]. По нататък Съдът отбелязва, че решението не съдържа каквато и да било констатация относно наличието в Съединените щати на правила, предназначени за ограничаване на евентуалната намеса, нито пък ефективна правна защита срещу такава намеса[677]. Съдът на ЕС подчертава, че степента на защита на основните права и свободи, гарантирана в рамките на ЕС, изисква в съответната правна уредба, в която се предвижда намеса в членове 7 и 8, да бъдат предвидени ясни и точни правила, които да уреждат обхвата и прилагането на дадена мярка и да установяват минимални гаранции, дерогации и ограничения относно защитата на личните данни[678]. Като се има предвид, че в решението на Комисията не е посочено, че САЩ ефективно гарантират такава степен на защита по силата на вътрешното си законодателство или на международните си споразумения, Съдът на ЕС заключава, че то

676 *Пак там*, параграф 84.

677 *Пак там*, параграфи 88—89.

678 *Пак там*, параграфи 91—92.

не отговаря на изискванията на съответната разпоредба за прехвърляне на данни от Директивата за защита на личните данни, и следователно е невалидно[679].

Следователно степента на защита в САЩ не е „по същество равностойна" на гарантираните от ЕС основни права и свободи[680]. Според Съда на ЕС са нарушени различни членове от Хартата на основните права на ЕС. На първо място е засегната същността на член 7, тъй като правната уредба на САЩ „осигурява общ достъп на публичните органи до съдържанието на електронни съобщения". На второ място е нарушена и същността на член 47, тъй като в правната уредба не се предвижда никаква възможност лицето да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни. На последно място, предвид факта, че споразумението за „сферата на неприкосновеност на личния живот" е нарушило горните членове, личните данни вече не са били обработвани законно, което е довело до нарушение на член 8.

След като Съдът на ЕС обяви споразумението за „сферата на неприкосновеност на личния живот" за невалидно, Комисията и САЩ се споразумяха за нова уредба — „Щит за личните данни в отношенията между ЕС и САЩ". На 12 юли 2016 г. Комисията прие решение, в което обявява, че САЩ гарантират достатъчна степен на защита за личните данни, прехвърляни от Съюза на организации в САЩ съгласно Щита за личните данни[681].

Подобно на споразумението за „сферата на неприкосновеност на личния живот" правната рамка на Щита за личните данни в отношенията между ЕС

679 *Пак там*, параграфи 96—97.

680 *Пак там*, параграфи 73—74 и 96.

681 Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 г. съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield), ОВ L 207, 1.8.2016 г. Работната група по член 29 приветства подобренията, внесени от механизма на Щита за личните данни в сравнение с решението относно „сферата на неприкосновеност на личния живот", и поздрави Комисията и органите на САЩ за това, че в окончателния вариант на документите за Щита за лични данни са отчели опасенията, които тя е изразила в своето становище WP 238 относно проекта на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ. Въпреки това тя изтъкна редица нерешени въпроси. За повече подробности вж. Работна група за защита на данните по член 29, *Становище 1/2016 относно проект на решение за адекватността на Щита за личните данни в отношенията между ЕС и САЩ*, прието на 13 април 2016 г., 16/EN WP 238.

и САЩ има за цел да защити личните данни, прехвърляни от ЕС в САЩ за търговски цели[682]. Американските дружества могат доброволно сами да сертифицират своето придържане към Щита за личните данни, като се ангажират да спазват стандартите за защита на данните по тази рамка. Компетентните органи на САЩ наблюдават и проверяват дали сертифицираните дружества спазват тези стандарти.

Схемата на Щита за личните данни по-специално предвижда:

- задължения за защита на данните за дружествата, които получават лични данни от ЕС;
- защита и правна закрила за физическите лица, по-специално създаването на механизъм за омбудсман, който е независим от разузнавателните служби на САЩ и разглежда жалби от физически лица, които считат, че личните им данни са били използвани по незаконен начин от органите на САЩ в областта на националната сигурност;
- годишен съвместен преглед, за да се следи прилагането на правната рамка[683]; първият преглед се състоя през септември 2017 г.[684]

Правителството на САЩ е поело писмени ангажименти и уверения, които съпровождат решението за адекватността на Щита за личните данни. Те осигуряват ограничения и гаранции във връзка с достъпа на правителството на САЩ до лични данни за целите на правоприлагането и националната сигурност.

7.3.2 Предаване на данни с подходящи гаранции

Както в **правото на ЕС**, така и в **правото на Съвета на Европа** като възможно средство за гарантиране на достатъчно ниво на защита на данните при

682 За повече информация вж. Информационен бюлетин относно Щита за личните данни в отношенията между ЕС и САЩ.

683 За повече информация вж. уебстраницата на Европейската комисия относно Щита за личните данни в отношенията между ЕС и САЩ.

684 Европейска комисия, Доклад на Комисията до Европейския парламент и Съвета по първия годишен преглед на функционирането на Щита за личните данни в отношенията между ЕС и САЩ, COM(2017) 611 окончателен, 18 октомври 2017 г. Виж също Работна група по член 29, *Първи съвместен преглед на Щита за личните данни в отношенията между ЕС и САЩ*, приет на 28 ноември 2017 г., 17/EN РД 255.

получателя се признават подходящите гаранции между администратора, който изнася данни, и получателя в третата държава или международната организация.

Съгласно **правото на ЕС** предаването на лични данни на трета държава или на международна организация е разрешено, ако администраторът или обработващият лични данни осигури подходящи гаранции и приложими права и ако са налице ефективни правни средства за защита на субектите на данни[685]. Списъкът на приемливите „подходящи гаранции" е предвиден изключително в правото на ЕС в областта на защитата на данните. Подходящи гаранции могат да бъдат установени чрез:

- инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури;
- задължителни фирмени правила;
- стандартни клаузи за защита на данните, приети или от Европейската комисия, или от надзорен орган;
- кодекси за поведение;
- механизми за сертифициране[686].

Други средства за осигуряване на подходящи гаранции са специално създадени договорни клаузи между администратора или обработващия лични данни в ЕС и получателя на данни в трета държава. Тези договорни клаузи обаче трябва да бъдат разрешени от компетентния надзорен орган, преди да може да се разчита на тях като инструмент за предаване на лични данни. По подобен начин публичните органи могат да използват разпоредби за защита на данните, които да се включват в административните договорености между тях, при условие че надзорният орган ги е разрешил[687].

685 Общ регламент относно защитата на данните, член 46.

686 Общ регламент относно защитата на данните, член 46, параграф 1, букви в) и г), параграф 2, букви а), б), д) и е) и член 47.

687 *Пак там*, член 46, параграф 3.

Съгласно правото на Съвета на Европа движение на данни към държава или международна организация, която не е страна по модернизираната Конвенция № 108, е разрешено, ако е осигурено подходящо ниво на защита. Това може да се осъществи чрез:

- законодателството на съответната държава или международна организация; или
- специални или стандартизирани гаранции, съдържащи се в документ със задължителен характер[688].

Предаване на данни, което е обект на договорни клаузи

Както в **правото на Съвета на Европа,** така и в **правото на ЕС** като възможно средство за гарантиране на достатъчно ниво на защита на данните при получателя са признати договорните клаузи между администратора, който изнася данни, и получателя в третата държава[689].

На **равнището на ЕС** Европейската комисия с помощта на Работната група по член 29 разработи стандартни клаузи за защита на данните, които бяха официално признати като доказателство за подходяща защита на данните с решение на Комисията[690]. Тъй като решенията на Комисията са обвързващи в своята цялост за държавите членки, националните органи, които упражняват надзор върху предаването на данни, трябва да приемат тези стандартни договорни клаузи в своите процедури[691]. Така ако администраторът, който изнася данни, и получателят от трета държава се споразумеят и подпишат тези клаузи, това би трябвало да предостави на надзорния орган достатъчно доказателства за наличието на адекватни гаранции. Още в делото *Schrems* Съдът на ЕС постановява, че Европейската комисия няма право да ограничава правомощията на националните надзорни органи да упражняват контрол върху предаването на лични данни към трета държава, по отношение на

688 Модернизирана Конвенция № 108, член 14, параграф 3, буква б).

689 Общ регламент относно защитата на данните, член 46, параграф 3; модернизирана Конвенция № 108, член 14, параграф 3, буква б).

690 *Пак там*, член 46, параграф 2, буква б) и член 46, параграф 5.

691 *Пак там*, член 46, параграф 2, буква в); Договор за функционирането на Европейския съюз, член 288.

която има решение на Комисията относно адекватното ниво на защита[692]. По този начин националните надзорни органи не са възпрепятствани да упражняват правомощията си, включително правомощието да спират или забраняват предаването на лични данни, когато предаването се извършва в нарушение на правото на ЕС или на националното право в областта на защитата на данните, например когато вносителят на данните не зачита стандартните договорни клаузи[693].

Съществуването на стандартни клаузи за защита на данните в правната рамка на ЕС не възпрепятства администраторите да формулират други специални, индивидуални договорни клаузи, стига надзорният орган да ги е одобрил[694]. Те обаче трябва да гарантират същото ниво на защита, каквото се осигурява от стандартните клаузи за защита на данните. Когато одобряват специални клаузи, надзорните органи са длъжни да прилагат механизма за съгласуваност, така че да се гарантира съгласуван регулаторен подход в целия ЕС[695]. Това означава, че компетентният надзорен орган трябва да предаде на ЕКЗД своя проект за решение относно клаузите. ЕКЗД дава становище по въпроса, а надзорният орган в най-голяма степен взема предвид становището при следващите стъпки във връзка със своето решение. Ако органът възнамерява да не се съобрази със становището на ЕКЗД, се задейства механизмът за уреждане на спорове в ЕКЗД и Комитетът приема решение със задължителен характер[696].

Най-важните характеристики на стандартните договорни клаузи са:

- клауза в полза на трета страна, която дава възможност на субектите на данни да упражняват договорни права, дори и да не са страна по договора;

692 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г., параграфи 96—98 и 102—105.

693 За да се вземе под внимание позицията на Съда на ЕС по делото *Schrems*, Комисията измени решението си относно общите договорни клаузи. Решение за изпълнение (ЕС) 2016/2297 на Комисията от 16 декември 2016 година за изменение на решения 2001/497/ЕО и 2010/87/ЕС относно общите договорни клаузи за предаването на лични данни към трети страни и към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета, ОВ L 344, 17.12.2016 г.

694 Общ регламент относно защитата на данните, член 46, параграф 3, буква а).

695 *Пак там*, член 63 и член 64, параграф 1, буква д).

696 *Пак там*, член 64 и член 65.

- съгласието на получателя или вносителя на данни в случай на възникване на спор същият да се подчинява на националния надзорен орган и/или съдилищата с юрисдикция на територията, на която се намира администраторът, който изнася данни.

Понастоящем съществуват два набора от стандартни клаузи за предаването на данни между администратори, между които администраторът, който изнася данни, може да избира[697]. За предаването на данни между администратори и обработващи лични данни е налице само един набор от стандартни клаузи[698]. В момента обаче тези стандартни договорни клаузи са предмет на съдебно производство.

Пример: След като Съдът на ЕС обяви решението относно „сферата на неприкосновеност на личния живот" за невалидно[699], предаването на лични данни към САЩ вече не можеше да се основава на това решение относно адекватното ниво на защита. Докато продължаваха преговорите с органите на САЩ и до приемането на ново решение относно адекватното ниво на защита (в крайна сметка прието на 12 юли 2016 г.)[700] предаване на данни можеше да се извършва само на други правни основания, като например стандартни договорни клаузи или задължителни фирмени правила. Няколко дружества, включително Facebook Ирландия (срещу което беше заведено делото, което доведе

697 Комплект I се съдържа в приложението към Решение 2001/497/ЕО на Комисията от 15 юни 2001 г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО, ОВ L 181, 4.7.2001 г., Европейска комисия (2001 г.); Комплект II се съдържа в приложението към Решение 2004/915/ЕО на Комисията от 27 декември 2004 г. за изменение на Решение 2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни, ОВ L 385, 29.12.2004 г. Европейска комисия (2004 г.).

698 Европейска комисия (2010 г.), Решение 2010/87/ЕС на Комисията от 5 февруари 2010 г. относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета, ОВ L 39, 12.2.2010 г. Към момента на изготвяне на наръчника използването на стандартни договорни клаузи като основание за предаване на лични данни към САЩ беше предмет на съдебно производство във Върховния съд на Ирландия.

699 Съд на ЕС, C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

700 Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 г. съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield), ОВ L 207, 1.8.2016 г.

до обявяването за невалидно на решението относно „сферата на неприкосновеност на личния живот“), преминаха към стандартни договорни клаузи, за да продължат да предават данни от ЕС към САЩ.

Г-н Schrems подава жалба до ирландския надзорен орган с искане органът да преустанови предаването на данни към САЩ на основание стандартни договорни клаузи. По същество той твърди, че когато личните му данни се предават от ирландското дъщерно дружество на Facebook към Facebook Inc. и към разположени на територията на САЩ сървъри, няма никакви гаранции, че те ще бъдат защитени. Facebook Inc. е подчинено на американското законодателство, което може да го задължи да разкрие лични данни на правоприлагащите органи на САЩ, и европейските граждани не разполагат със средства за съдебна защита, за да оспорят тази практика[701]. По тези причини Съдът на ЕС заключава, че решението относно „сферата на неприкосновеност на личния живот“ е невалидно, и макар че решението на Съда се ограничава до разглеждането на това решение, жалбоподателят счита, че повдигнатите въпроси са от значение и когато предаването на данни е на основание договорни клаузи. Към момента на изготвяне на наръчника делото се разглеждаше във Върховния съд на Ирландия. Жалбоподателят очевидно възнамерява да отнесе делото до Съда на ЕС, където неговата цел е да оспори валидността на решението на Европейската комисия относно стандартните договорни клаузи. Както е описано в глава 5, единствено Съдът на ЕС е компетентен да обяви даден инструмент на ЕС за невалиден.

Предаване на данни, което е обект на задължителни фирмени правила

Правото на ЕС разрешава също така предаване на лични данни на основание задължителни фирмени правила по отношение на международно предаване на данни, осъществявано в рамките на дружества или предприятия от една и съща група, които участват в съвместна стопанска дейност[702]. Преди да може да се разчита на задължителните фирмени правила като инструмент за предаване на лични данни, компетентният надзорен орган трябва да ги

701 За повече информация вж. изменената жалба срещу Facebook Ireland Ltd, заведена пред Irish Data Protection Commissioner от Maximilian Schrems от 1 декември 2015 г.

702 Общ регламент относно защитата на данните, член 47.

одобри в съответствие с процедурите за одобрение на задължителните фирмени правила, като използва механизма за съгласуваност.

За да бъдат одобрени, задължителните фирмени правила трябва да са със задължителен характер, да обхващат всички съществени принципи на защита на данните и да се прилагат спрямо, и да се привеждат в изпълнение от всеки член на групата. Те трябва изрично да предоставят приложими права на субектите на данни, да включват всички съществени принципи на защита на данните и да отговарят на определени формални изисквания, като например в тях да се посочва структурата на предприятието, да се описва предаването на данни и начинът на прилагане на принципите на защита на данните. Това включва и предоставянето на тази информация на субектите на данни. В задължителните фирмени правила трябва да се уточняват, наред с другото, правата на субектите на данни и разпоредбите относно отговорността за всяко нарушение на правилата[703]. При одобряването на задължителните фирмени правила се задейства механизмът за съгласуваност относно сътрудничеството между надзорните органи (описан в глава 5).

В рамките на механизма за съгласуваност водещият надзорен орган прави преглед на предложените задължителни фирмени правила, приема проект за решение и го предава на ЕКЗД. Комитетът издава становище по въпроса и водещият надзорен орган може официално да одобри задължителните фирмени правила, като същевременно взема предвид „в най-голяма степен“ становището на Комитета. Това становище няма задължителен характер, но ако надзорният орган възнамерява да не се съобрази с него, се задейства механизмът за уреждане на спорове и Комитетът трябва да бъде призован да приеме решение със задължителен характер с мнозинство от две трети от неговите членове[704].

Съгласно **правото на Съвета на Европа** специалните или стандартизираните гаранции, съдържащи се в документ със задължителен характер[705], включват и задължителните фирмени правила.

703 За по-подробно описание вж. Общия регламент относно защитата на данните, член 47.

704 *Пак там,* член 57, параграф 1, буква т), член 58, параграф 1, буква й), член 64, параграф 1, буква е), член 65, параграфи 1 и 2.

705 Модернизирана Конвенция № 108, член 14, параграф 3, буква б).

7.3.3 Дерогации в особени случаи

Съгласно правото на ЕС предаването на лични данни към трета държава може да бъде обосновано дори и при отсъствието на решение относно адекватното ниво на защита или на гаранции, като например стандартни договорни клаузи или задължителни фирмени правила, при някое от следните обстоятелства:

- субектът на данни изрично е дал съгласието си за предаването на данни;
- съответният субект на данни влиза — или се подготвя да влезе — в договорни отношения, при които е необходимо предаване на данните в чужбина;
- предаването е необходимо за сключването на договор в интерес на субекта на данни между администратора и трета страна;
- предаването е необходимо поради важни причини от обществен интерес;
- предаването е необходимо за установяването, упражняването или защитата на правни претенции;
- предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данни;
- предаването е на данни от публични регистри (това е пример за преимуществените интереси на обществеността да има достъп до информацията, съхранявана в публичните регистри)[706].

Когато не е приложимо нито едно от тези условия и предаването на данни не може да бъде на основание решение относно адекватното ниво на защита или на подходящи гаранции, то може да се извършва само ако не е повторяемо, засяга само ограничен брой субекти на данни и е необходимо за целите на неоспоримите законни интереси на администратора, при условие че над тях не стоят правата на субекта на данни[707]. В тези случаи администраторът трябва да оцени обстоятелствата, свързани с предаването, и да предостави гаранции. Администраторът уведомява надзорния орган и засегнатия субект

706 Общ регламент относно защитата на данните, член 49.

707 *Пак там*.

на данни както за предаването на данни, така и за законния интерес, който обосновава това предаване.

Фактът, че дерогациите са крайна мярка, за да бъде предаването на данни законно[708] (която се използва само при липса на решение относно адекватното ниво на защита и ако не са налице никакви други гаранции), подчертава обстоятелството, че те са изключение, и е допълнително изтъкнат в съображенията на ОРЗД[709]. Дерогациите като такива се приемат като възможност „да се предават данни при определени обстоятелства" въз основа на дадено съгласие и когато „предаването засяга отделни случаи и е необходимо"[710] във връзка с договор или правна претенция.

Освен това, в съответствие с насоките на Работната група по член 29, позоваването на дерогации в особени случаи трябва да бъде по изключение, въз основа на отделни случаи и не може да бъде използвано за мащабно или повторяемо предаване на данни[711]. Европейският надзорен орган по защита на данните също подчертава изключителния характер на дерогациите, използвани като правно основание за предаването на данни по Регламент 45/2001, като отбелязва, че това решение „трябва да се използва в ограничени случаи" и „да засяга отделни случаи"[712].

Пример: Дружеството Global Distribution System (GDS) със седалище в САЩ осигурява системата за онлайн резервации на редица авиокомпании, хотели и параходни дружества по целия свят, като обработва данните на десетки милиони лица в ЕС. За да прехвърли първоначално данните на сървърите си в САЩ, дружеството GDS се позовава на дерогация като правно основание за предаването, поточно на необходимостта от сключване на договор. Поради това дружеството не е предоставило никакви други гаранции за личните

708 *Пак там*, член 49, параграф 1,

709 Виж Общ регламент за защита на данните, член 49, параграф 1, букви а), б) и д) и съображение 113.

710 *Пак там,* член 49, параграф 1.

711 Работна група по член 29 (2005 г.), *Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.*, WP 114, Брюксел, 25 ноември 2005 г.

712 Европейски надзорен орган по защита на данните (2014 г.), *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Документ за позиция, Брюксел, 14 юли 2014 г., стр. 15.

данни с произход от Европа, които са предадени на САЩ и след това са пренасочени към хотели навсякъде по света (което означава, че няма гаранции и за последващото предаване). Дружеството GDS не спазва изискванията на ОРЗД за законно международно предаване на данни, защото се позовава на дерогация като законово основание за мащабно предаване на данни.

Ако липсва решение относно адекватното ниво на защита, по важни причини от обществен интерес ЕС или неговите държави членки имат правомощията да наложат ограничения върху предаването на специални категории лични данни на трета държава, въпреки че са спазени другите условия за това предаване. Тези ограничения следва да се възприемат като изключения и държавите членки трябва да уведомят Комисията за съответните разпоредби[713].

Правото на Съвета на Европа разрешава движението на данни към територии, в които няма подходяща защита на личните данни, в случаите, когато:

- съответният субект на данни е дал съгласие за това;
- интересите на субекта на данни изискват подобно движение на данни;
- налице са преимуществени законни интереси, по-специално важни обществени интереси, предвидени в законодателството;
- предаването представлява необходима и пропорционална мярка в едно демократично общество[714].

7.3.4 Предавания на данни, които се основават на международни споразумения

ЕС може да сключва международни споразумения с трети държави, с които се урежда предаването на лични данни за специални цели. Тези споразумения трябва да включват подходящи гаранции за осигуряване на защитата на

713 Вж.Общ регламент за защита на данните, член 49, параграф 5.

714 Модернизирана Конвенция № 108, член 14, параграф 4.

личните данни на въпросните физически лица. Съществуването на ОРЗД не засяга разпоредбите на тези международни споразумения[715].

Държавите членки също могат да сключват международни споразумения с трети държави или международни организации, които осигуряват подходящо ниво на защита на основните права и свободи на физическите лица, доколкото тези споразумения не засягат прилагането на ОРЗД.

Подобно правило е предвидено в член 12, параграф 3, буква а) от модернизираната Конвенция № 108.

Примери за международни споразумения, които включват предаване на лични данни, са споразуменията за резервационни данни на пътниците.

Резервационни данни на пътниците

Резервационните данни на пътниците (PNR) се събират от въздушните превозвачи при извършването на резервация за полети и включват, освен другото, имената, адресите, подробности за кредитни карти и номерата на местата на пътниците във въздушния транспорт. Въздушните превозвачи събират тази информация и за собствените си търговски цели. ЕС е сключил споразумения с някои трети държави (Австралия, Канада и САЩ) относно предаването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки транснационални престъпления. Освен това през 2016 г. Съюзът прие Директива (ЕС) 2016/861, известна като Директива относно използването на резервационни данни на пътниците[716]. Тази директива осигурява правна рамка, по силата на която държавите членки на ЕС да предават резервационни данни на пътниците на компетентните органи в други трети държави, за да могат те също да предотвратяват, разследват, разкриват и преследват наказателно терористични престъпления и тежки престъпления. Предаването на резервационни данни на пътниците на органите на трети държави се извършва на база на конкретен случай и е предмет на индивидуална оценка дали

715 Общ регламент относно защитата на данните, съображение 102.

716 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.

предаването е необходимо за определените в директивата цели; то се извършва и при условие че се зачитат основните права.

Що се отнася до споразуменията за резервационните данни на пътниците между ЕС и трети държави, тяхната съвместимост с основните права на неприкосновеност на личния живот и защита на личните данни, залегнали в Хартата на основните права на ЕС, се оспорва. Когато през 2014 г., след преговори с Канада, ЕС подписа споразумение относно предаването и обработването на резервационни данни на пътниците, Европейският парламент реши да сезира Съда на ЕС с искането да прецени съвместимостта на споразумението с правото на ЕС, и по-специално с членове 7 и 8 от Хартата.

Пример: В Становището си относно законосъобразността на споразумението за резервационни данни на пътниците между ЕС и Канада[717] Съдът на ЕС постановява, че в настоящия си вид предвиденото споразумение е несъвместимо с признатите в Хартата основни права и следователно не може да бъде сключено. Тъй като включва обработване на лични данни, то представлява намеса в правото на защита на личните данни, гарантирано от член 8 от Хартата. В същото време той представлява и ограничение на правото на зачитане на личния живот, закрепено в член 7, като се има предвид, че взети заедно, резервационните данни на пътниците могат да бъдат обобщени и анализирани по начин, който да разкрие навиците при пътуване, отношенията между различни лица, информация относно финансовото положение на пътниците, техните хранителни навици и здравословно състояние, като по този начин засяга личния им живот.

Намесата в основните права, породена от предвиденото споразумение, преследва цел от общ интерес, а именно защита на обществената сигурност и борба с тероризма и тежките транснационални престъпления. Съдът на ЕС обаче припомня, че за да бъде оправдана, намесата трябва да бъде ограничена до строго необходимото за постигане на преследваната цел. След като анализира разпоредбите на предвиденото споразумение, Съдът на ЕС заключава, че то не отговаря на критерия за „строга необходимост". Сред факторите, които Съдът на ЕС взема предвид, за да достигне до това заключение, са следните:

717 Съд на ЕС, *Становище 1/15 на Съда* [голям състав], 26 юли 2017 г.

- Фактът, че предвиденото споразумение води до предаване на чувствителни данни. Резервационните данни на пътниците, събрани в съответствие с предвиденото споразумение, могат да включват чувствителни данни, като например информация, разкриваща расовия или етническия произход, религиозните убеждения или здравословното състояние на даден пътник. Предаването и обработването на чувствителни данни от канадските органи може да представлява риск за принципа на недопускане на дискриминация и следователно изисква точна и солидна обосновка, изведена от мотиви, различни от защитата на обществената сигурност и борбата с тежките престъпления. В предвиденото споразумение липсва подобна обосновка[718].

- Продължителното съхраняване на резервационни данни на всички пътници за период от пет години, дори след като те са напуснали Канада, също е счетено за надхвърлящо границите на строгата необходимост. Съдът на ЕС приема, че е допустимо канадските органи да запазват данните на пътници, за които са налице обективни доказателства, че биха могли да представляват заплаха за обществената сигурност, дори след заминаването си от Канада. За разлика от горното, съхраняването на личните данни на *всички* пътници, за които няма дори непряко доказателство, че представляват риск за обществената сигурност, не е обосновано[719].

Консултативният комитет по Конвенция № 108 е представил становище относно последствията върху защитата на данните, които могат да предизвикат споразуменията относно резервационните данни на пътниците съгласно правото на Съвета на Европа[720].

Изпращане на финансови данни

Установеното в Белгия „Дружество за световни междубанкови финансови телекомуникации“ (SWIFT), което обработва по-голямата част от световните парични преводи от европейски банки, извършва операции в подобни

718 *Пак там*, параграф 165.

719 *Пак там*, параграфи 204–207.

720 Съвет на Европа, *Становище относно последиците за защитата на данните от обработването на резервационните данни на пътниците*, T-PD(2016)18rev, 19 август 2016 г.

центрове в САЩ и му е предявено искане да разкрие данни на Министерството на финансите на САЩ за целите на разследването на тероризма съгласно програмата на Министерството за проследяване на финансирането на тероризма[721].

От гледната точка на ЕС няма налице достатъчно правно основание за разкриването на тези данни — отнасящи се главно за граждани на ЕС — на САЩ само поради факта, че местонахождението на един от центровете на SWIFT за обработване на данни, свързани с услугата, е установен в САЩ.

През 2010 г. между ЕС и САЩ е сключено специално споразумение, известно като Споразумението относно SWIFT, което да предостави необходимото правно основание и да гарантира подходящи стандарти за защита на данните[722].

Съгласно това споразумение финансовите данни, съхранявани от SWIFT, продължават да се предоставят на Министерството на финансите на САЩ за целите на предотвратяването, разследването, разкриването или наказателното преследване на тероризма или финансирането на тероризма. Министерството на финансите на САЩ може да изисква финансови данни от SWIFT, при условие че искането:

- посочва по възможно най-ясен начин финансовите данни;
- ясно обосновава необходимостта от данните;
- е формулирано възможно най-тясно, за да се сведе до минимум обемът на исканите данни;

721 Вж. в този контекст Работна група по член 29 (2011 г.), Становище 14/2011 по въпроси за защита на личните данни, свързани с предотвратяването на изпирането на пари и финансирането на тероризма, WP 186, Брюксел, 13 юни 2011 г.; Работна група по член 29 (2006 г.), *Становище 10/2006 относно обработката на лични данни от Дружеството за световни междубанкови финансови телекомуникации (SWIFT)*, WP 128, Брюксел, 22 ноември 2006 г; Комисията на Белгия за защита на неприкосновеността на личния живот (*Commission de la protection de la vie privée*) (2008 г.), *„Процедура за контрол и препоръки, започната по отношение на дружеството SWIFT scrl“*, Решение, 9 декември 2008 г.

722 Решение 2010/412/ЕС на Съвета от 13 юли 2010 г. относно сключването на Споразумението между Европейския съюз и Съединените американски щати относно обработката и изпращането на данни за финансови съобщения от Европейския съюз до Съединените щати за целите на Програмата за проследяване на финансирането на тероризма, ОВ L 195, 27.7.2010 г., стр. 3—4. Текстът на споразумението е приложен към решението, ОВ L 195, 2010 г., стр. 5—14.

- не се отнася за данни, свързани с Единната европейска платежна зона (SEPA)[723].

Европол трябва да получи копие от всяко искане на Министерството на финансите на САЩ и да провери дали то съответства на принципите на Споразумението относно SWIFT[724]. Ако се потвърди съответствието на искането, SWIFT трябва да предостави финансовите данни непосредствено на Финансовото министерство на САЩ. Министерството трябва да съхранява финансовите данни в защитена физическа среда, където те са достъпни само за специалисти в разследването на терористични дейности или тяхното финансиране, като финансовите данни не трябва да бъдат свързани с никаква друга база данни. По принцип финансовите данни, получени от SWIFT, трябва да бъдат заличени не по-късно от пет години след получаването им. Тези данни, които са от значение за конкретни разследвания или наказателни преследвания, могат да се съхраняват само за период, не по-дълъг от необходимото за тези разследвания или наказателни преследвания.

Министерството на финансите на САЩ може да предава информация от данните, получени от SWIFT, на конкретни правоприлагащи органи, органи за обществена сигурност или органи за борба с тероризма в рамите на САЩ или извън тях единствено за разследването, разкриването, предотвратяването или наказателното преследване на тероризма и неговото финансиране. Когато последващото предаване на финансови данни засяга гражданин на държава членка на ЕС или лице, пребиваващо на територията на държава членка, всяко споделяне на данни с органи на трета държава е възможно само с предварителното съгласие на компетентните органи на засегнатата държава членка. Изключение може да се направи, когато споделянето на данни е от съществено значение за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност.

Независими наблюдатели, включващи и лице, посочено от Европейската комисия, осъществяват мониторинг на спазването на принципите на Споразумението относно SWIFT. Те имат възможността да преглеждат в реално време и назад във времето всички извършени търсения във връзка с предоставените данни и да изискват допълнителна информация, за да се обоснове

723 *Пак там*, член 4, параграф 2.

724 Съвместният надзорен орган на Европол е извършил одити на дейностите на Европол в тази област.

връзката на тези търсения с тероризма, както и правомощията да блокират някое или всички търсения, които изглежда, че са в нарушение на гаранциите, предвидени в споразумението.

Лицата, чиито данни се обработват, имат право да получат потвърждение от компетентния надзорен орган на ЕС, че техните права по отношение на защитата на личните данни са спазени. Съгласно Споразумението относно SWIFT лицата, чиито данни се обработват, имат право също така на коригиране, изтриване или блокиране на данните, които са били събрани и съхранявани за тях от Министерството на финансите на САЩ. Въпреки това обаче правата на достъп на лицата, чиито данни се обработват, може да подлежат на определени правни ограничения. При отказан достъп субектът на данни трябва да бъде информиран в писмена форма за отказа и за правото му да потърси административна и съдебна защита в САЩ.

Споразумението относно SWIFT е в сила за срок от пет години, като първият му срок на действие беше до август 2015 г. Този срок се удължава автоматично за последващи срокове от една година освен ако някоя от страните уведоми другата най-малко шест месеца предварително за своето намерение да не продължава действието на споразумението. Автоматичното удължаване на срока е приложено през август 2015, 2016 и 2017 г. и гарантира валидността на Споразумението относно SWIFT поне до август 2018 г.[725]

725 *Пак там*, член 23, параграф 2.

8 Защитата на данните в контекста на полицията и наказателното правосъдие

ЕС	Обхванати въпроси	СЕ
Директива за защита на данните, обработвани от полицейските и наказателноправните органи	**Общо по въпросите**	Модернизирана Конвенция № 108
	Полиция	Препоръка за сектора на полицията Практически наръчник относно използването на лични данни от полицията
	Наблюдение	ЕСПЧ, *B.B/Франция*, № 5335/06, 2009 г. ЕСПЧ, *S. и Marper/ Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 2008 г. ЕСПЧ, *Allan/ Обединеното кралство*, № 48539/99, 2002 г. ЕСПЧ, *Malone/ Обединеното кралство*, № 8691/79, 1984 г. ЕСПЧ, *Klass и други/ Германия*, № 5029/71, 1978 г. ЕСПЧ, *Szabó и Vissy/Унгария*, № 37138/14, 2016 г. ЕСПЧ, *Vetter/Франция*, № 59842/00, 2005 г.

ЕС	Обхванати въпроси	СЕ
	Киберпрестъпност	Конвенция за престъпления в кибернетичното пространство
Други специални правни инструменти		
Решението от Прюм	**За специални данни: дактилоскопични отпечатъци, ДНК данни, хулиганство, информация за пътуващите с въздушен транспорт, данни на далекосъобщителните дружества и т.н.**	Модернизирана Конвенция № 108, член 6 Препоръка за сектора на полицията, Практически наръчник относно използването на лични данни от полицията
Шведската инициатива (Рамково решение 2006/960/ПВР на Съвета)	**Опростяване на обмена на информация и разузнавателни данни между правоприлагащите органи**	ЕСПЧ, *S. и Marper/ Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 2008 г.
Директива(ЕС) 2016/681 относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления Съд на ЕС, съединени дела C-293/12 и C-594/12 *Digital Rights Ireland и Kärntner Landesregierung и други* [голям състав], 2014 г. Съд на ЕС, съединени дела C-203/15 и C-698/15, *Tele2 Sverige и Home Department/ Tom Watson и други* [голям състав], 2016 г.	**Запазване на лични данни**	ЕСПЧ, *B.B/Франция*, № 5335/06, 2009 г.
Регламентът за Европол Решението за Евроюст	**Чрез специални агенции**	Препоръка за сектора на полицията
Решението за Шенген II Регламентът за ВИС Регламентът за Евродак Решението за МИС	**Чрез специални съвместни информационни системи**	Препоръка за сектора на полицията ЕСПЧ, *Dalea/Франция*, № 964/07, 2010 г.

За да се балансират интересите на физическите лица в областта на защитата на данните и интересите на обществото при събирането на данни за целите на борбата с престъпността и гарантирането на националната и обществената сигурност, Съветът на Европа и ЕС са приели специални правни инструменти. В този раздел се съдържа преглед на правото на Съвета на Европа (раздел 8.1) и на правото на ЕС (раздел 8.2) по отношение на защитата на данните във връзка с полицейски и наказателноправни въпроси.

8.1 Право на Съвета на Европа относно защитата на данните във връзка с въпроси на националната сигурност, полицейски и наказателноправни въпроси

Ключови въпроси

- Модернизираната Конвенция № 108 и Препоръката на Съвета на Европа за сектора на полицията са приложими за защитата на данните във всички области на полицейската работа.
- Конвенцията за престъпления в кибернетичното пространство (Конвенцията от Будапеща) е задължителен международен правен инструмент, в който са обхванати престъпленията, извършени срещу и посредством електронни мрежи. Тя е от значение и за разследването на престъпления, които не са свързани с кибернетичното пространство, но в които се използват доказателства в електронен вид.

Важно различие между правото на Съвета на Европа и правото на ЕС е, че за разлика от правото на ЕС, **правото на Съвета на Европа** се прилага и в областта на националната сигурност. Това означава, че договарящите се страни трябва да се придържат в рамките на член 8 от ЕКПЧ, дори и за дейности, свързани с националната сигурност. Няколко решения на ЕСПЧ са свързани с дейности на държавните органи в чувствителни области на правото и практиката относно националната сигурност[726].

726 Вж. например ЕСПЧ, *Klass и други/Германия*, № 5029/71, 6 септември 1978 г., ЕСПЧ, *Rotaru/Румъния* [голям състав], № 28341/95, 4 май 2000 г.; и ЕСПЧ, *Szabó и Vissy/Унгария*, № 37138/14, 12 януари 2016 г.

Що се отнася до полицията и наказателното правосъдие, на европейско равнище, модернизираната Конвенция № 108 обхваща всички сфери на обработването на лични данни, като нейните разпоредби имат за цел да регламентират обработването на лични данни по принцип. Следователно модернизираната Конвенция № 108 се прилага по отношение на защитата на данните в областта на полицията и наказателното правосъдие. Обработването на генетични данни, на лични данни, свързани с престъпления, наказателни производства и присъди и свързаните с тях мерки за сигурност, на биометрични данни, които уникално идентифицират дадено лице, както и на всякакви чувствителни лични данни е разрешено само когато съществуват подходящи гаранции срещу рисковете, които обработването на такива данни може да породи за интересите, правата и основните свободи на субектите на данни, по-специално риска от дискриминация[727].

Установените от закона задачи на органите на полицията и наказателното правосъдие често налагат обработването на лични данни, което може да има сериозни последици за засегнатите физически лица. Препоръката за сектора на полицията, приета от Съвета на Европа през 1987 г., дава насоки на държавите членки на Съвета на Европа относно начина, по който те следва да приложат в действие принципите на Конвенция № 108 в контекста на обработването на лични данни от полицейските органи[728]. Препоръката беше придружена с практически наръчник относно използването на лични данни в полицейския сектор, приет от Консултативния комитет на Конвенция № 108[729].

Пример: По делото *Д.Л./България*[730] социалните служби настаняват по съдебен ред жалбоподателката във възпитателно заведение от затворен тип. Всички писма и телефонни разговори са били обект на автоматична и недиференцирана проверка и надзор от страна на възпитателното заведение. ЕСПЧ постановява, че е налице нарушение на член 8, като се има предвид, че въпросната мярка не е необходима в едно демократично общество. Съдът посочва, че трябва всичко да се предвиди, за да могат непълнолетните, настанени в институция,

727 Модернизирана Конвенция № 108, член 6.

728 Съвет на Европа, Комитет на министрите (1987 г.), Препоръка Rec(87)15 до държавите членки за уреждане на използването на лични данни в сектора на полицията, 17 септември 1987 г.

729 Съвет на Европа (2018 г.), Консултативен комитет на Конвенция № 108, Практически наръчник относно използването на лични данни в полицейския сектор, T-PD(2018)1.

730 ЕСПЧ, *Д.Л./България*, № 7472/14, 19 май 2016 г.

да имат достатъчно външни контакти, защото това е неразделна част от правото им на достойно отношение и е абсолютно необходима, за да ги подготви за завръщането им в обществото. Това важи в еднаква степен както за посещенията, така и за писмата или телефонните разговори. Освен това режимът на надзор не прави никаква разлика между комуникациите с членовете на семейството и НПО за закрила на правата на детето или адвокати. Също така решението да се подслушват телефонните разговори не почива върху индивидуален анализ на рисковете за всеки отделен случай.

Пример: По делото *Dragojević/Хърватия*[731] жалбоподателят е бил заподозрян в участие в трафик на наркотици. Той е признат за виновен, след като разследващият съдия дава разрешение за използването на мерки за тайно наблюдение с цел подслушване на телефонните разговори на жалбоподателя. ЕСПЧ постановява, че мярката, срещу която е подадена жалбата, представлява намеса в правото на зачитане на личния живот и кореспонденцията. Разрешението, дадено от разследващия съдия, се основава само на изявление на прокуратурата, че „разследването не може да бъде проведено с други средства". ЕСПЧ отбелязва също така, че наказателните съдилища са ограничили оценката си относно използването на средствата за наблюдение и че правителството не е предложило правните средства за защита, които съществуват. Следователно е налице нарушение на член 8.

8.1.1 Препоръката за сектора на полицията

ЕСПЧ многократно постановява, че съхраняването и запазването на лични данни от органите на полицията или на националната сигурност представлява намеса в правата по член 8, параграф 1 от ЕКПЧ. В много решения на ЕСПЧ се разглежда обосноваването на подобна намеса[732].

731 ЕСПЧ, *Dragojević/Хърватия*, № 68955/11, 15 януари 2015 г.

732 Вж. например ЕСПЧ, *Leander/Швеция*, № 9248/81, 26 март 1987 г.; ЕСПЧ, *M.M./Обединеното кралство*, № 24029/07, 13 ноември 2012 г.; ЕСПЧ, *M.K./Франция*, № 19522/09, 18 април 2013 г.; или ЕСПЧ, *Aycaguer/Франция*, № 8806/12, 22 юни 2017 г.

Пример: По делото *B.B./Франция*[733] жалбоподателят е осъден на лишаване от свобода за извършването на сексуални престъпления срещу 15-годишни непълнолетни лица в качеството си на лице в позиция на доверие. През 2000 г. той излиза от затвора. Година по-късно отправя искане тази присъда да бъде заличена от регистъра за съдимост, но искането е отхвърлено. През 2004 г. с френски закон се създава национална съдебна база данни за извършителите на сексуални престъпления и жалбоподателят е информиран, че е включен в нея. ЕСПЧ решава, че включването на осъден извършител на сексуално престъпление в национална съдебна база данни попада в обхвата на член 8 от ЕКПЧ. Въпреки това, предвид факта, че са били приложени достатъчно гаранции за защита на данните, като правото на субекта на данни да поиска изтриването на данните, ограниченото времетраене на тяхното съхранение и ограничения достъп до тях, е намерен справедлив баланс между заложените противоречащи си частни и обществени интереси. Съдът заключава, че не е налице нарушение на член 8 от ЕКПЧ.

Пример: По делото *S. и Marper/Обединеното кралство*[734] и двамата жалбоподатели са били обвинени в извършването на престъпление, но не са били осъдени. Независимо от това техните дактилоскопични отпечатъци, проби от клетки и ДНК профили се запазват и съхраняват от полицията. Неограниченото запазване на посочените по-горе биометрични данни е позволено от закона, ако лицето е заподозряно в извършването на престъпление, дори ако по-късно заподозреният е намерен за невинен или е оправдан. ЕСПЧ постановява, че повсеместното и неизбирателно запазване на лични данни без ограничение на периода от време и ограничените възможности на оправданите лица да поискат заличаване представлява непропорционална намеса в правото на зачитане на личния живот на жалбоподателите. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

Решаващ въпрос в контекста на електронните комуникации е намесата от страна на публичните органи в правата на неприкосновеност на личния живот

733 ЕСПЧ, *B.B./Франция*, № 5335/06, 17 декември 2009 г.

734 ЕСПЧ, *S. и Marper/Обединеното кралство* [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г., параграфи 119 и 125.

и на защита на данните. Способите за наблюдение или прихващане на комуникации, като например устройствата за подслушване или записване, са допустими само ако това е предвидено в закон и представлява необходима мярка в едно демократично общество в интерес на:

- защитата на държавната сигурност;
- обществената безопасност;
- паричните интереси на държавата;
- борбата с престъпленията; или
- защитата на субекта на данните или на правата и свободите на другите.

В много последващи решения на ЕСПЧ се разглежда обосноваването на намесата в правото на неприкосновеност на личния живот при извършване на полицейско наблюдение.

Пример: По делото *Allan/Обединеното кралство*[735] органите тайно записват частните разговори на затворник с приятел в зоната за посетители в затвора и със съобвинен в затворническата килия. ЕСПЧ постановява, че използването на устройства за аудио- и видеозапис в килията на жалбоподателя, в зоната за посетители в затвора и носени от съзатворник означават намеса в правото на неприкосновеност на личния живот на жалбоподателя. Тъй като не е налице правно установена система, регламентираща използването на скрити записващи устройства от полицията в съответния момент, тази намеса не е в съответствие със закона. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

Пример: В делото *Roman Zakharov/Русия*[736] жалбоподателят завежда съдебно производство срещу три оператора на мобилни мрежи. Той твърди, че е нарушено правото му на неприкосновеност на телефонните разговори, тъй като операторите са инсталирали оборудване, позволяващо на Федералната служба за сигурност да прихваща

735 ЕСПЧ, *Allan/Обединеното кралство*, № 48539/99, 5 ноември 2002 г.

736 ЕСПЧ, *Roman Zakharov/Русия* [голям състав], № 47143/06, 4 декември 2015 г.

телефонните му разговори без предварително разрешение от съда. ЕСПЧ постановява, че националните правни разпоредби, които уреждат прихващането на комуникации, не осигуряват подходящи и ефективни гаранции срещу произвол и срещу риска от злоупотреби. По-специално националното право не изисква заличаване на съхранените данни, след като е постигната целта на съхраняването. Освен това, макар да се изисква съдебно разрешение, съдебният контрол е ограничен.

Пример: В делото *Szabó и Vissy/Унгария*[737] жалбоподателите твърдят, че унгарското законодателство нарушава член 8 от ЕКПЧ, тъй като не е достатъчно подробно и точно. Освен това те твърдят, че законодателството не осигурява достатъчни гаранции срещу злоупотреби и произвол. ЕСПЧ постановява, че унгарското право не изисква извършването на наблюдение да бъде обект на съдебно разрешение. Въпреки това Съдът отбелязва, че макар и да е било необходимо одобрението на Министъра на правосъдието, това наблюдение е имало изцяло политически характер и е било невъзможно да се осигури изискваната оценка за „строга необходимост". Освен това националното право не предвижда съдебен контрол, като се има предвид, че не се изпраща уведомление на лицата. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

Тъй като обработването на данни от полицейските органи може да има значително въздействие върху засегнатите лица, подробни правила относно защитата на данните са особено необходими при обработването на лични данни в тази област. Целта на препоръката на Съвета на Европа за сектора на полицията е да разгледа този въпрос, като предостави насоки относно начините, по които следва да се събират личните данни за полицейска работа; как следва да се съхраняват досиетата в тази област; кой следва да има разрешение за достъп до досиетата, включително условията за предаване на лични данни на чуждестранни полицейски органи; как съответните физически лица да могат да упражняват своите права на защита на данните; как да се упражнява контрол от независимите органи. Взето е под внимание и задължението за осигуряване на подходяща сигурност на данните.

737 ЕСПЧ, *Szabó и Vissy/Унгария*, № 37138/14, 12 януари 2016 г.

Препоръката не предвижда неограничено неизбирателно събиране на лични данни от полицейските органи. Тя ограничава събирането на лични данни от полицейските органи до необходимото за предотвратяването на реална опасност или наказателното преследване на конкретно престъпление. Всяко събиране на допълнителни данни би трябвало да се основава на специално национално законодателство. Обработването на чувствителни данни следва да бъде ограничено до това, което е абсолютно необходимо в контекста на конкретно проучване.

Ако личните данни се събират без знанието на съответния субект на данни, той трябва да бъде информиран за събирането на данните веднага щом подобно разкриване вече не възпрепятства разследването. Събирането на данни със средства за техническо наблюдение или други автоматизирани средства трябва да има специални правни основания.

Пример: По делото *Versini-Campinchi и Crasnianski/Франция*[738] жалбоподателката, която е адвокат, е имала телефонен разговор с клиент, чийто телефон е бил подслушван по искане на разследващ съдия. Протоколът от разговора показва, че тя е разкрила информация, която е била обект на професионална тайна. Прокурорът изпраща тази информация на адвокатската колегия, която налага наказание на жалбоподателката. ЕСПЧ признава наличието на намеса в правото на зачитане на личния живот и кореспонденцията не само по отношение на лицето, чийто телефон е бил подслушван, но и по отношение на жалбоподателката, чийто разговор е бил прихванат и записан. Намесата е извършена в съответствие със закона и преследва законната цел за предотвратяване на безредици. Жалбоподателката отправя искане за проверка на законосъобразността на предоставянето на протокола от записите от подслушването в хода на образуваното срещу нея дисциплинарно производство, което искане е удовлетворено. Макар и да не е могла да поиска отмяна на протокола от телефонния разговор, ЕСПЧ счита, че е имало ефективен контрол, който е бил в състояние да ограничи обжалваната намеса до необходимото в едно демократично общество. ЕСПЧ постановява, че аргументът, че възможността за наказателно производство срещу адвокат въз основа на записа би могла да има възпиращ ефект върху свободата на общуване между адвокат

738 ЕСПЧ, *Versini-Campinchi u Crasnianski/Франция*, № 49176/11, 16 юни 2016 г.

и клиент и по този начин върху правата на защита на последния, не е убедителен, тъй като направеното от самата адвокатка разкриване на информация би могло да представлява незаконно поведение от нейна страна. При това положение не се констатира нарушение на член 8.

В препоръката на Съвета на Европа за сектора на полицията се предвижда, че когато се съхраняват лични данни, следва да се направят ясни разграничения между: административни и полицейски данни; лични данни на различните видове субекти на данни, например заподозрени, осъдени лица, жертви и свидетели; данни, считани за установени факти, и такива, основаващи се на подозрения или предположение.

Целта, за която може да се използват полицейски данни, трябва да бъде строго ограничена. Това има последици за разкриването на полицейски данни на трети страни: предаването или съобщаването на такива данни в рамките на сектора на полицията следва да се ръководи от това дали е налице законен интерес от обмена на информацията. Предаването или разкриването на такива данни извън сектора на полицията следва да се допуска само ако е налице ясно правно задължение или разрешение.

Пример: По делото *Karabeyoğlu/Турция*[739] телефонните линии на жалбоподателя, който е съдия, са следени в контекста на наказателно разследване на незаконна организация, към която той е заподозрян, че принадлежи, или на която се предполага, че предоставя помощ и подкрепа. След решението да не бъде образувано съдебно производство прокурорът, който отговаря за наказателното разследване, унищожава въпросните записи. Едно копие обаче остава притежание на съдебните следователи, които след това използват съответния материал в контекста на дисциплинарно разследване срещу жалбоподателя. ЕСПЧ постановява, че е налице нарушение на съответното законодателство, тъй като информацията е била използвана за цели, различни от тези, за които е била събрана, и не е била унищожена в законно определения срок. Намесата в правото на зачитане на личния живот на жалбоподателя не е била в съответствие със закона, що се отнася до дисциплинарното производство срещу него.

739 ЕСПЧ, *Karabeyoğlu/Турция*, № 30083/10, 7 юни 2016 г.

Международното предаване или разкриване на данни следва да се ограничава до чуждестранни полицейски органи и да се основава на специални правни разпоредби, по възможност международни споразумения, освен ако не са необходими за предотвратяването на сериозна и непосредствена опасност.

Обработването на данни от полицията трябва да подлежи на независим надзор, за да се гарантира съответствието с националното законодателство за защита на данните. Субектите на данни трябва да имат всички права за достъп до данните, включени в модернизираната Конвенция № 108. Ако правата за достъп на субектите на данни са ограничени в съответствие с член 9 от Конвенция № 108 в интерес на провеждането на ефективни полицейски разследвания и изпълнението на наложените наказания, те трябва да имат право съгласно националното законодателство да подадат жалба до националния надзорен орган за защита на данните или до друг независим орган.

8.1.2 Конвенцията от Будапеща за престъпленията в кибернетичното пространство

Престъпната дейност все повече използва и засяга електронни системи за обработване на данни, поради което са необходими нови наказателноправни разпоредби за справяне с това предизвикателство. По тази причина Съветът на Европа прие международен правен инструмент – Конвенция за престъпленията в кибернетичното пространство, известна също като Конвенцията от Будапеща, за да се разгледа въпросът за престъпленията, извършени срещу и с помощта на електронни мрежи[740]. Конвенцията е отворена за присъединяване и на държави, които не са членки на Съвета на Европа. Към началото на 2018 г. 14 държави извън Съвета на Европа[741] станаха страни по конвенцията, а още седем други държави, които не са членки, са били поканени да се присъединят към нея.

740 Съвет на Европа, Комитет на министрите (2001 г.), Конвенция за престъпленията в кибернетичното пространство, CETS № 185, Будапеща, 23 ноември 2001 г., влязла в сила на 1 юли 2004 г.

741 Австралия, Канада, Чили, Колумбия, Доминиканската република, Израел, Япония, Мавриций, Панама, Сенегал, Шри Ланка, Тонга, Тунис и Съединените американски щати. Вж. Диаграма на подписванията и ратификациите по член 185 от Договора, състояние към юли 2017 г.

Конвенцията за престъпленията в кибернетичното пространство остава най-влиятелният международен договор, разглеждащ нарушенията на законодателството в интернет или други информационни мрежи. Тя изисква от страните по нея да актуализират и хармонизират своите наказателни закони срещу компютърното пиратство и други нарушения на сигурността, включително нарушения на авторското право, компютърни измами, детска порнография и други незаконни дейности в кибернетичното пространство. Конвенцията предвижда също така процесуални правомощия, обхващащи претърсването на компютърни мрежи и прихващането на съобщения в контекста на борбата с престъпленията в кибернетичното пространство. Накрая, тя позволява ефективното международно сътрудничество. В допълнителен протокол към конвенцията се разглежда инкриминирането на расистка и ксенофобска пропаганда в компютърните мрежи.

Конвенцията не е инструмент за насърчаване на защитата на данните, но тя инкриминира дейности, които е възможно да нарушат правото на съответния субект на данни на защита на неговите данни. Освен това тя изисква от договарящите се страни да приемат законодателни мерки, за да могат националните им органи да прихващат данни за трафика и съдържанието[742]. Тя също така задължава договарящите се страни, когато прилагат конвенцията, да предвидят адекватна защита на правата и свободите на човека, включително правата, гарантирани от ЕКПЧ, например правото на защита на данните[743]. За да се присъединят към Конвенцията от Будапеща за престъпленията в кибернетичното пространство, от договарящите се страни не се изисква да се присъединят и към Конвенция № 108.

742 Съвет на Европа, Комитет на министрите (2001 г.), Конвенция за престъпленията в кибернетичното пространство, CETS № 185, Будапеща, 23 ноември 2001 г., членове 20 и 21.

743 *Пак там*, член 15, параграф 1.

8.2 Право на ЕС относно защитата на данните във връзка с полицейски и наказателноправни въпроси

Ключови въпроси

- В рамките на ЕС защитата на данните в сектора на полицията и наказателното правосъдие е уредена в контекста както на националното, така и на трансграничното обработване на данни от полицейски и наказателноправни органи на държавите членки и участниците от ЕС.
- На равнището на държавите членки Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, трябва да бъде включена в националното право.
- Защитата на данните в рамките на трансграничното сътрудничество между полицейските и правоприлагащите органи, по-специално в областта на борбата с тероризма и трансграничната престъпност, се регламентира от специални правни инструменти.
- Специални правила за защита на данните съществуват за Европейската полицейска служба (Европол), Европейското звено за съдебно сътрудничество (Евроюст) и новосъздадената Европейска прокуратура, които са органи на ЕС, подпомагащи и насърчаващи трансграничното правоприлагане.
- Специални правила за защита на данните съществуват и за съвместните информационни системи, установени на равнището на ЕС за трансграничен обмен на информация между компетентните полицейски и съдебни органи. Важни примери са Шенгенската информационна система от второ поколение (ШИС II), Визовата информационна система (ВИС) и Евродак — централизирана система, съдържаща данни за дактилоскопични отпечатъци на граждани на трети държави и лица без гражданство, кандидатстващи за убежище в една от държавите членки на ЕС.
- ЕС е в процес на актуализиране на посочените по-горе разпоредби относно защитата на данните, така че те да бъдат приведени в съответствие с разпоредбите на Директивата за защита на данните, обработвани от полицейските и наказателноправните органи.

8.2.1 Директива за защита на данните, обработвани от полицейските и наказателноправните органи

Директива 2016/680/ЕС 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 (Директива за защита на данните, обработвани от полицейските и наказателноправните органи)[744] има за цел да защити личните данни, събирани и обработвани за целите на наказателното правосъдие, които включват:

- предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;
- изпълнението на наложените наказания; и
- случаите, когато полицейски или други правоприлагащи органи действат в подкрепа на закона и вземат предпазни мерки и предотвратяват заплахи за обществената сигурност и основните права на обществото, които могат да изпълняват състава на престъпление.

Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, защитава личните данни на различни категории физически лица, участващи в наказателно производство, като свидетели, информатори, жертви, заподозрени и съучастници. Полицейските и наказателноправните органи са длъжни да спазват разпоредбите на директивата

744 Директива 2016/680/ЕС на Европейския парламент и на Съвета от 27 април 2016 г. 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 (Директива за защита на данните, обработвани от полицейските и наказателноправните органи).

винаги когато обработват такива лични данни за целите на правоприлагането, както в персоналния, така и в материалния обхват на директивата[745].

Използването на данни за друга цел обаче също е разрешено при определени условия. Обработването на лични данни за различна цел на правоприлагането от тази, за която са били събрани, е разрешено само ако това е законно, необходимо и пропорционално съгласно националното право или правото на ЕС[746]. За другите цели се прилагат правилата на Общия регламент относно защитата на данните. Регистрирането и документирането на споделянето на данни е специално задължение на компетентните органи, за да съдействат за изясняване на отговорностите, произтичащи от жалбите.

Компетентните органи, работещи в сферата на полицията и наказателното правосъдие, са публични органи или органи, които по силата на националното право разполагат с публична власт и публични правомощия да изпълняват функциите на публичен орган[747], например частни затвори[748]. Приложимостта на директивата обхваща едновременно обработването на лични данни на национално ниво и трансграничното обработване между полицейски и съдебни органи на държавите членки, а също и международното предаване на данни от компетентните органи към трети държави и международни организации[749]. Директивата не обхваща областта на националната сигурност или обработването на лични данни от институции, органи, служби и агенции на ЕС[750].

Директивата се основава в голяма степен на принципите и определенията, които се съдържат в Общия регламент относно защитата на данните, като

745 Директива за защита на данните, обработвани от полицейските и наказателноправните органи, член 2, параграф 1.

746 *Пак там*, член 4, параграф 2.

747 *Пак там*, член 3, параграф 7.

748 Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент съгласно член 294, параграф 6 от Договора за функционирането на Европейския съюз относно позицията на Съвета във връзка с приемането на Директива на Европейския парламент и на Съвета 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 наказателни санкции и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета, COM(2016) 213 окончателен, Брюксел, 11 април 2016 г.

749 Директива за защита на данните, обработвани от полицейските и наказателноправните органи, глава V.

750 *Пак там,* член 2, параграф 3.

отчита специфичния характер на секторите на полицията и наказателното правосъдие. Надзорът може да бъде извършван от същите органи на държавите членки, които упражняват такъв и по силата на Общия регламент относно защитата на данните. Назначаването на длъжностни лица по защита на данните и извършването на оценки на въздействието върху защитата на данните са въведени в директивата като нови задължения за полицейските и наказателноправните органи[751]. Въпреки че тези понятия са вдъхновени от Общия регламент относно защитата на данните, директивата е насочена към специфичния характер на полицейските и наказателноправните органи. В сравнение с обработването на данни за търговски цели, което се урежда от регламента, свързаното със сигурността обработване може да изисква известна гъвкавост. Например предоставянето на субектите на данни на същото ниво на защита по отношение на правата им на информация, на достъп или на заличаване на личните им данни, каквото те имат по силата на Общия регламент относно защитата на данните, може да означава, че всяка операция по наблюдение, извършвана за целите на правоприлагането, ще стане неефективна в контекста на правоприлагането. По тази причина директивата не съдържа принципа на прозрачност. По подобен начин принципите на свеждане на данните до минимум и на ограничение на целите, които изискват личните данни да бъдат ограничени само до необходимото по отношение на целите, за които се обработват, и да бъдат обработвани за конкретни и ясно формулирани цели, също трябва да се прилагат гъвкаво при обработване, което е свързано със сигурността. Информацията, която е събрана и съхранена от компетентните органи за конкретен случай, може да се окаже изключително полезна за разрешаването на бъдещи случаи.

Принципи, свързани с обработването

В Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, се посочват няколко основни гаранции по отношение на използването на лични данни. В нея също така са определени принципите, които ръководят обработването на тези данни. Държавите членки трябва да гарантират, че личните данни са:

- обработвани законосъобразно и добросъвестно;

751 *Пак там*, съответно член 32 и член 27.

- събирани за конкретни, изрично указани и легитимни цели и не се обработват по начин, който е несъвместим с тези цели;

- подходящи, относими и не надхвърлят необходимото във връзка с целите, за които данните се обработват;

- точни и, при необходимост, поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

- съхранявани във вид, който позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които те се обработват;

- обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки[752].

Съгласно директивата обработването е законосъобразно само доколкото то е необходимо за изпълнението на съответната задача. Освен това то следва да се извършва от компетентен орган за постигане на целите, определени в директивата, и да е въз основа на правото на ЕС или правото на държава членка[753]. Данните не трябва да се съхраняват за период, по-дълъг от необходимия, и трябва да бъдат изтрити или периодично преразглеждани в определени срокове. Данните трябва да се използват само от дадения компетентен орган и за целта, за която са били събрани, предадени или предоставени.

Права на субекта на данни

В директивата са определени и правата на субекта на данни. Те включват:

- Право на получаване на информация. Държавите членки трябва да задължат администратора на данни да предоставя на субектите на данни:

752 *Пак там*, член 4, параграф 1.

753 *Пак там*, член 8.

1) данни за идентифициране и координатите за връзка на администратора; 2) координатите за връзка на длъжностното лице по защита на данните; 3) информация за целите на планираното обработване; 4) информация за правото на подаване на жалба до надзорен орган и координатите за връзка с него; и 5) информация за правото на достъп до, коригиране или изтриване на лични данни и ограничаване на обработването на лични данни[754]. В допълнение към тези общи изисквания относно информацията директивата предвижда, че в конкретни случаи и с цел да се даде възможност на субектите на данните да упражнят своите права, те трябва да бъдат информирани от администраторите за правното основание на обработването и за срока, за който ще се съхраняват личните данни. Ако личните данни се предават на други получатели, включително в трети държави или международни организации, субектите на данни трябва да бъдат информирани за категориите на тези получатели. И накрая, администраторите трябва да предоставят всяка допълнителна информация, като отчитат конкретните обстоятелства, при които се обработват данните — например когато те са събрани по време на скрито наблюдение, т.е. без знанието на субекта на данните. Това гарантира добросъвестно обработване по отношение на субекта на данните[755].

- Право на достъп до лични данни. Държавите членки трябва да гарантират, че субектът на данни има правото да знае дали личните му данни се обработват. Ако случаят е такъв, субектът на данните следва да има достъп до определена информация, като например категориите данни, които се обработват[756]. Това право обаче може да бъде ограничено — например за да се предотврати възпрепятстването на разследване или оказването на неблагоприятно влияние върху наказателното преследване на престъпления, или за да се защитят обществената сигурност и правата и свободите на други лица[757].

- Право на коригиране на лични данни. Държавите членки са длъжни да гарантират, че субектът на данни може да поиска коригирането на неточни

754 *Пак там*, член 13, параграф 1.

755 *Пак там*, член 13, параграф 2.

756 *Пак там*, член 14.

757 *Пак там*, член 15.

лични данни без излишно забавяне. Освен това субектът на данните има и право да поиска непълните лични данни да бъдат попълнени[758].

- Право на изтриване на лични данни и ограничаване на обработването. В определени случаи администраторът трябва да изтрие личните данни. Освен това субектът на данните може да осигури изтриването на личните си данни, но само в случай че те са обработвани незаконно[759]. В определени ситуации обработването на лични данни може да бъде ограничено, вместо те да бъдат изтрити. Това може да се случи, когато 1) точността на личните данни се оспорва, но това не може да бъде проверено, или 2) когато личните данни са необходими за доказателствени цели[760].

Винаги когато администраторът откаже да коригира или да изтрие лични данни, или да ограничи обработването на данните, субектът на данните трябва да бъде информиран за това в писмена форма. Държавите членки могат да ограничат това право на информация, за да може, наред с другото, да се защитят обществената сигурност или правата и свободите на други лица, по същите причини, по които може да се ограничи правото на достъп[761].

Субектът на данни обикновено има право на информация относно обработването на личните му данни, както и право на достъп, коригиране или заличаване, а също и на ограничаване на обработването, което той може да упражнява пряко пред администратора. В допълнение, непрякото упражняване на правата на субекта на данните чрез неговия надзорен орган за защита на данните е възможно и съгласно Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, като това влиза в действие, когато администраторът ограничава правото на субекта на данните[762]. Член 17 от директивата изисква държавите членки да приемат мерки, които гарантират, че правата на субектите на данни може да бъдат упражнени и чрез техния надзорен орган. Ето защо администраторът на данни трябва да информира субекта на данните относно възможността за непряк достъп.

758 *Пак там*, член 16, параграф 1.

759 *Пак там*, член 16, параграф 2.

760 *Пак там*, член 16, параграф 3.

761 *Пак там*, член 16, параграф 4.

762 *Пак там*, член 17.

Задължения на администратора и обработващия лични данни

В контекста на Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, администраторите на данни са компетентни публични органи или други структури със съответните публични правомощия и публична власт, които определят целите и средствата на обработването на лични данни. Директивата определя няколко задължения за администраторите на данни, за да се гарантира високо ниво на защита на личните данни, които се обработват за целите на правоприлагането.

Компетентните органи трябва да водят записи за операциите по обработване, които извършват в системите за автоматизирано обработване. Записите трябва да се водят най-малко за събирането, промяната, справките, разкриването, включително предаването, комбинирането и изтриването на личните данни[763]. Директивата предвижда, че записите за извършена справка или разкриване трябва да дават възможност за установяване на датата и часа на такива операции, тяхната обосновка и доколкото е възможно — идентификацията на лицето, което е направило справка в системата или е разкрило лични данни, както и на получателите на тези лични данни. Записите трябва да се използват единствено за проверяване на законосъобразността на обработването, за самоконтрол, за гарантиране на целостността и сигурността на личните данни и при наказателни производства[764]. При поискване от надзорния орган администраторът и обработващият лични данни трябва да му предоставят тези записи.

По-специално, налице е общо задължение на администраторите да прилагат подходящи технически и организационни мерки, за да гарантират, че обработването се извършва в съответствие с директивата, и да са в състояние да докажат законосъобразността му[765]. При разработването на тези мерки те трябва да отчитат естеството, обхвата, контекста на обработването и, което е особено важно, всички възможни рискове за правата и свободите на физическите лица. Администраторите следва да приемат вътрешни политики и да прилагат мерки, които подпомагат спазването на принципите за защита на данните, по-специално на принципа за защита на данните на етапа на

763 *Пак там*, член 25, параграф 1.

764 *Пак там*, член 25, параграф 2.

765 *Пак там*, член 19.

проектирането и по подразбиране[766]. Когато има вероятност обработването да породи висок риск за правата на физическите лица — например поради използването на нови технологии — администраторите трябва да извършат оценка на въздействието върху защитата на данните, преди да започнат обработването[767]. В директивата са изброени и мерките, които трябва да бъдат прилагани от администраторите за гарантиране на сигурността на обработването. Това включва мерки с цел да се предотврати неразрешеният достъп до личните данни, обработвани от тях, и да се гарантира, че оправомощените лица имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп, че функциите на системата за обработване работят правилно и че съхранените лични данни не могат да бъдат увредени вследствие на неправилно функциониране на системата[768]. Ако възникне нарушение на сигурността на личните данни, администраторите трябва да уведомят надзорния орган в срок от три дни, като опишат естеството на нарушението, евентуалните му последици, категориите лични данни, които са засегнати, и приблизителния брой на засегнатите субекти на данни. Нарушенията на сигурността на лични данни трябва да бъдат съобщавани „без излишно забавяне“ и на субекта на данните, когато има вероятност нарушението да доведе до висок риск за неговите права и свободи[769].

Директивата съдържа принципа на отчетност, като създава задължение за администраторите да прилагат мерки за гарантиране на спазването на този принцип. Администраторите трябва да поддържат регистри с всички категории дейности по обработване под тяхна отговорност; подробното съдържание на тези регистри е посочено в член 24 от директивата. При поискване регистрите трябва да бъдат предоставени на надзорния орган, така че той да може да упражнява наблюдение върху операциите по обработване на администратора. Друга важна мярка за подобряване на отчетността е определянето на длъжностно лице по защита на данните. Администраторите трябва да определят длъжностно лице по защита на данните, макар че директивата позволява на държавите членки да освободят съдилищата и други независими съдебни органи от това задължение[770]. Задълженията на длъжностното лице по защита на данните са сходни с тези съгласно Общия регламент

766 *Пак там*, член 20.

767 *Пак там*, член 27.

768 *Пак там*, член 29.

769 *Пак там*, членове 30 и 31.

770 *Пак там*, член 32.

относно защитата на данните. Длъжностното лице по защита на данните наблюдава спазването на директивата, информира и съветва служителите, които извършват обработване на лични данни, за техните задължения по силата на законодателството в областта на защитата на данните. Длъжностното лице по защита на данните също така предоставя съвети относно необходимостта от извършване на оценка на въздействието върху защитата на данните и действа като точка за контакт за надзорния орган.

Предаване на данни на трети държави или международни организации

Подобно на Общия регламент относно защитата на данните, директивата урежда условията за предаването на лични данни на трети държави или международни организации. Гаранциите и строгата защита, осигурени по силата на правото на ЕС, могат да бъдат застрашени, ако личните данни се предават свободно извън юрисдикцията на ЕС. Условията сами по себе си обаче са много различни от тези съгласно Общия регламент относно защитата на данните. Предаването на лични данни на трети държави или международни организации е разрешено, ако[771]:

- Предаването е необходимо за целите на директивата.

- Личните данни се предават на компетентен орган по смисъла на директивата в трета държава или международна организация, въпреки че е налице дерогация от това правило в отделни и особени случаи[772].

- За предаването на трети държави или международни организации на лични данни, получени в хода на трансграничното сътрудничество, е необходимо разрешението на държавата членка, от която са получени данните, въпреки че за спешни случаи са предвидени изключения.

- Европейската комисия е приела решение относно адекватното ниво на защита на личните данни, установени са подходящи гаранции или се прилагат дерогации за предаване на данни в особени случаи.

771 *Пак там*, член 35.

772 *Пак там*, член 39.

- За последващо предаване на лични данни на друга трета държава или на международна организация се изисква предварително разрешение от компетентния орган, извършил първоначалното предаване, който взема предвид, наред с другото, тежестта на престъплението и нивото на защита на данните в държавата на местоназначение на второто международно предаване[773].

По силата на директивата предаване на лични данни може да се извърши, ако е спазено едно от трите условия. Първото условие е Европейската комисия да е издала решение относно адекватното ниво на защита на личните данни съгласно директивата. Решението може да е приложимо за цялата територия на трета държава, за конкретни сектори в трета държава или за международна организация. Това може да бъде направено обаче само ако е гарантирано подходящо ниво на защита и са спазени условията, определени в директивата[774]. В такива случаи предаването на лични данни не е обект на разрешение от държавата членка[775]. Европейската комисия трябва да наблюдава развитието, което би могло да повлияе на действието на решението относно адекватното ниво на защита. Освен това решението трябва да съдържа механизъм за периодичен преглед. Комисията също така може да отменя, изменя или спира действието на решението при наличие на съответна информация, че условията в третата държава или международната организация вече не осигуряват адекватно ниво на защита. Ако случаят е такъв, Комисията трябва да започне консултации с третата държава или международната организация с цел да коригира положението.

При липса на решение относно адекватното ниво на защита на личните данни предаването на данни може да се основава на подходящи гаранции. Те може да бъдат предвидени в правно обвързващ инструмент или администраторът може сам да извърши оценка на обстоятелствата около предаването на лични данни и да стигне до заключението, че съществуват подходящи гаранции. Оценката, извършена от самия администратор, следва да вземе предвид възможните споразумения за сътрудничество, сключени между Европол или Евроюст и третата държава или международната организация, наличието на задължения за поверителност и принципа на ограничението на целите, както и увереността, че личните данни няма да бъдат използвани за каквато

773 *Пак там*, член 35, параграф 1.

774 *Пак там*, член 36.

775 *Пак там*, член 36, параграф 1.

и да е форма на жестоко и нечовешко отношение, включително налагане на смъртно наказание[776]. В последния случай администраторът трябва да информира компетентния надзорен орган за категориите предавания[777].

Когато не е прието решение относно адекватното ниво на защита или не са установени подходящи гаранции, все пак може да бъде разрешено предаване на данни в особени случаи, описани в директивата. Те включват, наред с другото, защитата на жизненоважни интереси на субекта на данните или на друго лице и предотвратяването на непосредствена и сериозна заплаха за обществената сигурност на държава членка или на трета държава[778].

В отделни и специфични случаи може да се осъществи предаване от компетентните органи на получатели, които са установени в трети държави и не са компетентни органи, ако в допълнение към едно от описаните по-горе три условия са изпълнени и допълнителните условия, предвидени в член 39 от директивата. По-специално, предаването трябва да е строго необходимо за изпълнението на задача на предаващия компетентен орган, който също така носи отговорността да реши, че никое от основните права и свободи на физическите лица не надделява над обществения интерес, който обосновава предаването на данни. Такова предаване трябва да бъде документирано и предаващият компетентен орган трябва да уведоми компетентния надзорен орган[779].

И накрая, по отношение на трети държави и международни организации, директивата изисква също така да бъдат разработени механизми за международно сътрудничество с цел подпомагане на ефективното прилагане на законодателството, като по този начин помага на надзорните орган за защита на данните да си сътрудничат с техните чуждестранни партньори[780].

776 *Пак там*, съображение 71.

777 *Пак там*, член 37, параграф 1.

778 *Пак там*, член 38, параграф 1.

779 *Пак там*, член 37, параграф 3.

780 *Пак там*, член 40.

Независим надзор и правни средства за защита за субектите на данни

Всяка държава членка трябва да гарантира, че един или повече независими национални надзорни органи отговарят за консултиране и наблюдение на прилагането на разпоредбите, приети съгласно директивата[781]. Надзорният орган, създаден за целите на директивата, може да бъде същият като надзорния орган, създаден съгласно Общия регламент относно защитата на данните, но държавите членки са свободни да определят друг орган, при условие че той отговаря на критериите за независимост. Надзорните органи също така разглеждат искове, подадени от което и да е лице, отнасящи се до защитата на неговите права и свободи във връзка с обработването на лични данни от страна на компетентните органи.

Когато упражняването на правата на субекта на данни е отказано въз основа на първостепенни съображения, физическото лице трябва да има право да обжалва пред компетентния национален надзорен орган и/или съд. Ако дадено лице претърпи вреди в резултат на нарушения на националното законодателство за прилагане на директивата, това лице има право да получи обезщетение от администратора или от друг компетентен съгласно правото на държава членка орган[782]. По принцип субектите на данни трябва да имат достъп до средство за съдебна защита в случай на нарушение на техните права, гарантирани от националното законодателство за прилагане на директивата[783].

8.3 Други специални правни инструменти за защита на данните в областта на правоприлагането

В допълнение към Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, обменът на информация, съхранявана от държавите членки в специфични области, се урежда от редица правни инструменти — като например Рамково решение 2009/315/ПВР на Съвета относно организацията и съдържанието на обмена на информация,

781 *Пак там*, член 41.

782 *Пак там*, член 56.

783 *Пак там*, член 54.

получена от регистрите за съдимост, между държавите членки, Решение 2000/642/ПВР на Съвета относно условията за сътрудничество и обмен на информация между звената за финансово разузнаване на държавите членки и Рамково решение 2006/960/ПВР на Съвета от 18 декември 2006 година за опростяване обмена на информация и сведения между правоприлагащите органи на държавите членки на Европейския съюз[784].

Най-важното е, че трансграничното сътрудничество[785] между компетентните органи включва във все по-голяма степен обмена на имиграционни данни. Счита се, че тази област от правото не касае полицията и наказателното правосъдие, но в много отношения тя е свързана с работата на полицията и правосъдните органи. Същото важи и за данните за стоките, които се внасят във или се изнасят от ЕС. Премахването на контрола по вътрешните граници в рамките на Шенгенското пространство увеличава риска от измами, което налага засилване на сътрудничеството между държавите членки, най-вече чрез увеличаване на трансграничния обмен на информация, за да може по-ефективно да се разкриват и да се преследват наказателно нарушенията на националното и европейското митническо законодателство. Освен това през последните години в света се наблюдава увеличаване на тежката и организираната престъпност и тероризма, като действията на организираната престъпност може да включват международни пътувания, разкривайки в много случаи необходимост от засилено трансгранично сътрудничество в областта на полицията и правоприлагането[786].

784 Съвет на Европейския съюз (2009 г.), Рамково решение 2009/315/ПВР на Съвета от 26 февруари 2009 г. относно организацията и съдържанието на обмена на информация, получена от регистрите за съдимост, между държавите членки, ОВ L 93, 7.4.2009 г.; Съвет на Европейския съюз (2000 г.), Решение 2000/642/ПВР на Съвета от 17 октомври 2000 г. относно условията за сътрудничество и обмен на информация между звената за финансово разузнаване на държавите членки, ОВ L 271, 24.10.2000 г.; Рамково решение 2006/960/ПВР на Съвета от 18 декември 2006 година за опростяване обмена на информация и сведения между правоприлагащите органи на държавите членки на Европейския съюз, ОВ L 386, 29.12.2006 г.

785 Европейска комисия (2012 г.), *Съобщение на Комисията до Европейския парламент и Съвета — Засилване на сътрудничеството в областта на правоприлагането в ЕС: Европейският модел за обмен на информация (ЕІХМ),* COM(2012) 735 окончателен, Брюксел, 7 декември 2012 г.

786 Вж. Европейска комисия (2011 г), Предложение за директива на Европейския парламент и на Съвета относно използването на резервационни данни на пътниците за предотвратяване, разкриване, разследване и наказателно преследване на престъпления, свързани с тероризъм, и на тежки престъпления, COM(2011) 32 окончателен, Брюксел, 2 февруари 2011 г., стр. 1.

Решението от Прюм

Важен пример за институционализирано трансгранично сътрудничество чрез обмен на съхранявани на национално равнище данни е Решение 2008/615/ПВР на Съвета и неговите правила за прилагане в Решение 2008/615/ПВР за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност (Решението от Прюм), с което Договорът от Прюм беше въведен в правото на ЕС през 2008 г.[787] Договорът от Прюм беше международно споразумение за полицейско сътрудничество, подписано през 2005 г. от Австрия, Белгия, Франция, Германия, Люксембург, Нидерландия и Испания[788].

Целта на решението от Прюм е да се помогне на подписалите го държави членки да подобрят обмена на информация за целите на предотвратяването и борбата с престъпността в три области: тероризма, трансграничната престъпност и незаконната миграция. За тази цел решението определя разпоредби по отношение на:

- автоматичния достъп до ДНК профили, дактилоскопични данни и определени данни от националната регистрация на превозните средства;
- предоставянето на данни, свързани с големи събития с трансгранично измерение;
- предоставянето на информация за предотвратяване на терористични престъпления;
- други мерки за засилване на трансграничното полицейско сътрудничество.

Базите данни, които са предоставени на разположение по силата на Решението от Прюм, се уреждат изцяло от националното законодателство, но обменът на данни допълнително се регламентира в решението, чиято

787 Съвет на Европейския съюз (2008 г.), Решение 2008/615/ПВР на Съвета от 23 юни 2008 г. за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност, ОВ L 210, 6.8.2008 г.

788 Конвенция между Кралство Белгия, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия и Република Австрия относно засилване на презграничното сътрудничество, особено в борбата с тероризма, презграничната престъпност и нелегалната миграция.

съвместимост с Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, ще трябва да бъде оценена. Компетентните органи за надзор на тези предавания на данни са националните надзорни органи за защита на данните.

Рамково решение 2006/960/ПВР — Шведската инициатива

Рамково решение 2006/960/ПВР (Шведската инициатива)[789] е друг пример за трансгранично сътрудничество по отношение на обмена на данни, съхранявани на национално равнище, между правоприлагащите органи. Шведската инициатива акцентира специално върху обмена на сведения и информация, като в член 8 от решението са предвидени специални правила за защита на данните.

Съгласно този инструмент използването на информация и сведения, които са били обменени, се подчинява на националните разпоредби за защита на данните на държавата членка, която получава информацията, в съответствие със същите правила, както в случай че информацията и сведенията са били събрани в тази държава членка. В член 8 също така се посочва, че при предоставяне на информация и сведения компетентният правоприлагащ орган може по силата на националното си законодателство да наложи условия за използването на информацията и сведенията от получаващия компетентен правоприлагащ орган. Тези условия може да са приложими и за докладването на резултата от наказателното разследване или операцията за събиране на сведения за целите на наказателното производство, за които е бил необходим обменът на информация и сведения. Когато обаче националното законодателство предвижда изключения от ограниченията за използването (например за съдебните органи, законодателните органи и т.н.), информацията и сведенията могат да се използват само след предварително съгласуване със съобщаващата държава членка.

Предоставените информация и сведения може да бъдат използвани:

- за целите, за които те са били предоставени; или

789 Съвет на Европейския съюз (2006 г.), Рамково решение 2006/960ПВР от 18 декември 2006 г. за опростяване обмена на информация и сведения между правоприлагащите органи на държавите членки на Европейския съюз, OB L 386/89 от 29 декември 2006 г.

- за предотвратяването на неизбежна и сериозна заплаха за обществената сигурност.

Обработване с друга цел може да бъде разрешено, но само с предварително разрешение на съобщаващата държава членка.

В Шведската инициатива се посочва също така, че обработваните лични данни трябва да бъдат защитени в съответствие с международни инструменти, като например:

- Конвенция на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни[790];

- Допълнителен протокол относно контролните органи и трансграничните потоци от данни към същата конвенция, 8 ноември 2001 г.[791];

- Препоръка № R(87) 15 на Съвета на Европа, с която се урежда използването на лични данни в сектора на полицията[792].

Директива на ЕС за резервационните данни на пътниците

Резервационните данни на пътниците се отнасят до информацията за пътуващите със самолет пътници, събирана и съхранявана в системите за резервации, и системите за контрол на излитанията на превозвачите за техни собствени търговски цели. Тези данни съдържат няколко различни вида информация, като например дати на пътуване, маршрут на пътуване, информация за билета, информация за контакт, туристически агент, чрез когото е направена резервацията за полета, използвано средство за плащане,

790 Съвет на Европа (1981 г.), Конвенция за защита на лицата при автоматизираната обработка на лични данни, ETS № 108.

791 Съвет на Европа (2001 г.) , Допълнителен протокол към Конвенцията за защита на лицата при автоматизирана обработка на лични данни относно надзорните органи и трансграничните потоци от данни, ETS № 108.

792 Съвет на Европа (1987 г.), Препоръка № R (87) 15 на Комитета на министрите към държавите членки, с която се урежда използването на лични данни в сектора на полицията (приета от Комитета на министрите на 17 септември 1987 г., на 140-ото заседание на заместник-министрите).

номер на мястото и информация за багажа[793]. Обработването на резервационни данни на пътниците може да помогне на правоприлагащите органи да идентифицират известни или потенциални заподозрени и да извършват оценки въз основа на определени модели на пътуване и други показатели, които обикновено са свързани с престъпни дейности. Анализите на резервационни данни на пътниците също така позволяват проследяване назад във времето на маршрутите на пътуване и контактите на лица, които са заподозрени за участие в престъпни дейности, което може да даде възможност на правоприлагащите органи да идентифицират престъпни мрежи[794]. Както е обяснено в раздел 7, ЕС сключи няколко споразумения с трети държави за обмен на резервационни данни на пътниците. Освен това той въведе обработването на резервационни данни на пътниците в рамките на ЕС чрез Директива 2016/681/ЕС относно използването на резервационни данни на пътниците за предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления (Директива на ЕС за резервационните данни на пътниците)[795]. Тази директива предвижда задължения за въздушните превозвачи да предават резервационни данни на пътниците на компетентните органи и въвежда строги гаранции за защита на данните във връзка с тяхното обработване и събиране. Директивата на ЕС за резервационните данни на пътниците се прилага за международните полети към и от ЕС, но също така и за вътрешните полети в рамките на ЕС, ако държава членка реши това[796].

Събраните резервационни данни на пътниците трябва да съдържат само информацията, която е разрешена от Директивата на ЕС за резервационните данни на пътниците. Те трябва да се съхраняват в единно звено за данни за пътниците, на защитено място във всяка от държавите членки. Резервационните данни на пътниците трябва да се деперсонализират шест месеца след

793 Европейска комисия (2011 г), Предложение за директива на Европейския парламент и на Съвета относно използването на резервационни данни на пътниците за предотвратяване, разкриване, разследване и наказателно преследване на престъпления, свързани с тероризъм, и на тежки престъпления, COM(2011) 32 окончателен, Брюксел, 2 февруари 2011 г., стр. 1.

794 Европейска комисия (2015 г.), Информационен бюлетин „Борбата с тероризма на равнище ЕС, преглед на действията, мерките и инициативите на Комисията“, Брюксел, 11 януари 2015 г.

795 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.

796 Директива за резервационните данни на пътниците, ОВ L 119, стр. 132, член 1, параграф 1 и член 2, параграф 1.

тяхното предаване от въздушния превозвач и да се съхраняват за период не по-дълъг от пет години[797]. Резервационни данни на пътниците се обменят между държавите членки, между държавите членки и Европол и с трети държави, но само въз основа на оценка на всеки отделен случай.

Предаването и обработването на резервационните данни на пътниците и гарантираните права на субектите на данни трябва да бъдат в съответствие с Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, и трябва да осигуряват високото ниво на защита на неприкосновеността на личния живот и на личните данни, което се изисква от Хартата, от модернизираната Конвенция № 108 и от ЕКПЧ.

Съгласно Директивата на ЕС за резервационните данни на пътниците независимите национални надзорни органи, които са компетентни по силата на Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, отговарят и за даването на указания и упражняването на наблюдение във връзка с прилагането на разпоредбите, приети от държавите членки.

Запазване на телекомуникационни данни

Директивата за запазване на лични данни[798], обявена за невалидна на 8 април 2014 г. в решението по дело *Digital Rights Ireland*, задължаваше доставчиците на съобщителни услуги да запазват метаданни, по-специално за целите на борбата с тежките престъпления, за срок от най-малко шест месеца и най-много 24 месеца, независимо от това дали доставчикът все още е имал нужда от тези данни за изготвяне на абонатни сметки или за техническо предоставяне на услугата.

Запазването на телекомуникационни данни очевидно представлява намеса в правото на защита на данните[799]. Дали тази намеса е обоснована или не,

797 *Пак там*, член 12, параграф 1 и член 12, параграф 2.

798 Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени във връзка с предоставянето на общественодостъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г.

799 ЕНОЗД (2011 г.), *Становище на Европейския надзорен орган по защита на данните (ЕНОЗД) от 31 май 2011 г. относно доклада на Комисията до Съвета и Европейския парламент за оценка на директивата за запазване на данни (Директива 2006/24/ЕО),* 31 май 2011 г.

е било предмет на спор в няколко съдебни производства в държави членки на ЕС[800].

Пример: В делата *Digital Rights Ireland* и Kärntner Landesregierung и *други*[801] групата Digital Rights и г-н Seitlinger подават жалба съответно до High Court в Ирландия и до Конституционния съд в Австрия, като оспорват законосъобразността на националните мерки, които позволяват запазването на електронни телекомуникационни данни. Digital Rights иска ирландският съд да установи недействителността на Директива 2006/24 и на частта от националния Закон за наказателно правораздаване, свързана с терористични престъпления. По същия начин г-н Seitlinger и повече от 11 000 други жалбоподатели оспорват и искат да се отмени разпоредба от австрийското законодателство за далекосъобщенията, с което се транспонира Директива 2006/24.

При разглеждането на тези преюдициални въпроси Съдът на ЕС обявява Директивата за запазване на лични данни за невалидна. Според Съда на ЕС, ако бъдат разгледани в съвкупност, данните, които може да бъдат запазвани съгласно директивата, предоставят точна информация за лицата. Освен това Съдът на ЕС разглежда тежестта на намесата в основните права на зачитане на неприкосновеността на личния живот и на защита на личните данни. Той установява, че запазването изпълнява цел от обществен интерес, а именно борбата с тежките престъпления, а с това в крайна сметка и целта за обществена сигурност. Въпреки това Съдът на ЕС постановява, че с приемането на директивата законодателят на ЕС е нарушил принципа на пропорционалност. Въпреки че директивата може да е подходяща за постигането на необходимата цел, „от тази директива произтича особено обширна и тежка за правния ред на Съюза намеса в тези основни права, без тази намеса да е точно уредена с разпоредби, които да могат да гарантират, че тя действително се свежда до строго необходимото“.

800 Германия, Федерален конституционен съд (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 март 2010 г.; Румъния, Конституционен съд (*Curtea Constituţională a României*), № 1258, 8 октомври 2009 г.; Чешката република, Конституционен съд (*Ústavní soud České republiky*), 94/2011 Сб., 22 март 2011 г.

801 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г., параграф 65.

При липсата на специално законодателство относно запазването на данни то е разрешено като изключение от изискването за поверителност на телекомуникационните данни съгласно Директива 2002/58/ЕО (Директивата за правото на неприкосновеност на личния живот и електронни комуникации)[802] като превантивна мярка, но трябва да е единствено за целите на борбата с тежките престъпления. Това запазване трябва да е ограничено до строго необходимото, що се отнася до категориите запазвани данни, засегнатите съобщителни средства, заинтересованите лица и избрания период на запазване. Националните органи може да получат достъп до запазените данни при строги условия, в т.ч. след предварителен контрол от страна на независим орган. Данните трябва да бъдат пазени на територията на ЕС.

Пример: След решението по делата *Digital Rights Ireland* и *Kärntner Landesregierung и други*[803] в Съда на ЕС са внесени още две дела във връзка с общото задължение в Швеция и Обединеното кралство за доставчиците на далекосъобщителни услуги да запазват телекомуникационните данни съгласно изискванията на обявената за невалидна Директива за запазване на лични данни. В делата *Tele2 Sverige* и *Home Department/Tom Watson и други*[804] Съдът на ЕС постановява, че национална правна уредба, която предвижда общо и неизбирателно запазване на данни, без да се изисква никаква връзка между данните, които трябва да бъдат запазвани, и наличието на заплаха за обществената сигурност и без да се уточняват каквито и да било условия — например период на запазване, географска зона, кръг от определени лица, които е възможно да са участвали в тежки престъпления — надхвърля границите на строго необходимото и не може да се счита за обоснована в едно демократично общество, както изисква Директива 2002/58/ЕО, тълкувана в светлината на Хартата на основните права на ЕС.

802 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. 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 електронни комуникации), ОВ L 201, 31.7.2002 г.

803 Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.

804 Съд на ЕС, съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], 21 декември 2016 г.

Перспективи

През януари 2017 г. Европейската комисия публикува предложение за регламент относно зачитането на личния живот и защитата на личните данни в електронните съобщения, който беше предназначен да отмени и замени Директива 2002/58/ЕО[805]. Предложението не включва никакви конкретни разпоредби относно запазването на данни. То обаче предвижда, че държавите членки могат да наложат със закон ограничения върху определени задължения и права по регламента, ако такова ограничение представлява необходима и пропорционална мярка за защита на конкретни обществени интереси, например националната сигурност, отбраната, обществената сигурност и предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания[806]. Следователно държавите членки ще могат да запазят или създадат национални рамки за запазването на данни, които предвиждат целенасочени мерки за запазване, доколкото такива рамки съответстват на правото на Съюза и отчитат съдебната практика на Съда на ЕС относно тълкуването на Директивата за правото на неприкосновеност на личния живот и електронни комуникации и Хартата на основните права на ЕС[807]. Към момента на изготвяне на наръчника обсъжданията по приемането на регламента все още продължаваха.

Рамково споразумение между ЕС и САЩ относно защитата на лични данни, обменяни за целите на правоприлагането

На 1 февруари 2017 г. влезе в сила Рамковото споразумение между ЕС и САЩ за обработването на лични данни с оглед на предотвратяването, разследването, разкриването и наказателното преследване на престъпления със САЩ[808]. Неговата цел е да гарантира високо ниво на защита на данните за гражданите

805 Европейска комисия (2017 г.), *Предложение за регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения)*, COM(2017) 10 окончателен, Брюксел, 10 януари 2017 г.

806 *Пак там*, съображение 26.

807 Вж. обяснителния меморандум към Предложението за регламент относно зачитането на личния живот и защитата на личните данни в електронните съобщения, COM(2017) 10 окончателен, т. 1.3.

808 Вж. Съвет на ЕС (2016 г.), *„Засилване на правата на защита на данните за гражданите на ЕС в рамките на сътрудничеството в областта на правоприлагането: ЕС и САЩ подписват Рамково споразумение“*, Съобщение за медиите 305/16, 2 юни 2016 г.

на ЕС, като същевременно засили сътрудничеството между правоприлагащите органи на ЕС и САЩ. То допълва съществуващите споразумения между правоприлагащите органи на ЕС и САЩ и държавите членки и САЩ, като същевременно спомага да се въведат ясни и хармонизирани правила за защита на данните за бъдещите споразумения в тази област. В тази връзка целта на споразумението е да създаде дългосрочна правна уредба, за да се улесни обменът на информация.

Само по себе си споразумението не осигурява подходящо правно основание за обмена на лични данни; вместо това то предлага подходящи гаранции за защита на данните на засегнатите физически лица. То обхваща всички дейности, свързани с обработването на лични данни, необходими за целите на предотвратяването, разследването, разкриването и наказателното преследване на престъпления, включително тероризъм[809].

В споразумението са включени множество гаранции, така че личните данни да се използват само за целите, посочени в споразумението. По-специално то предвижда следните защита за гражданите на ЕС:

- ограничения по отношение на използването на данните: личните данни може да се използват само за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления;

- защита срещу произволна и необоснована дискриминация;

- последващо предаване: за всяко последващо предаване на данни към държава, която е различна от САЩ или е извън ЕС, или към международна организация трябва да е получено предварителното съгласие на компетентния орган на държавата, която първоначално е изпратила тази информация.

809 Споразумение между Съединените американски щати и Европейския съюз относно защитата на личната информация във връзка с предотвратяването, разследването, разкриването и наказателното преследване на престъпления от 18 май 2016 г., (OR.en) 8557/16, член 3, параграф 1. Вж. също уведомлението на Комисията относно преговорите за споразумение за защита на личните данни между ЕС и САЩ от 26 май 2010 г., MEMO/10/216, и Съобщението за медиите на Европейската комисия (2010 г.) относно високи стандарти за закрила на неприкосновеността на личния живот в рамките на Споразумението за защита на данните между ЕС и САЩ от 26 май 2010 г., IP/10/609.

- качество на данните: при поддържането на личните данни трябва да се обръща внимание на тяхната точност, съотносимост, актуалност и пълнота;

- сигурност на обработването, включително уведомяване за нарушения на сигурността на личните данни;

- обработването на чувствителни данни е разрешено само при наличието на подходящи гаранции в съответствие със закона;

- срокове на съхранение: личните данни не може да се съхраняват по-дълго, отколкото е необходимо или подходящо;

- права на достъп и поправяне: всяко лице има право на достъп до своите лични данни, при спазване на определени условия, и може да подаде искане данните да бъдат коригирани, ако са неточни;

- автоматизираните решения изискват подходящи гаранции, които включват възможността да се изиска човешка намеса;

- ефективен надзор, включително сътрудничество между надзорните органи на ЕС и САЩ; и

- защита по съдебен ред и приложимост: гражданите на ЕС имат право[810] да потърсят защита по съдебен ред в съдилищата на САЩ, когато органите на САЩ откажат достъп или поправяне или незаконно разкриват техни лични данни.

С Рамковото споразумение е създадена и система за уведомяване на компетентния надзорен орган в държавата членка на засегнатите физически лица относно всякакви нарушения на защитата на данните, когато това е необходимо. Осигурените от споразумението правни гаранции осигуряват равно

810 Американският Закон за съдебната защита беше утвърден от президента Обама на 24 февруари 2016 г.

третиране на гражданите на ЕС в САЩ при наличие на нарушение на неприкосновеността на личния живот[811].

8.3.1 Защита на данните в съдебните и правоприлагащите органи на ЕС

Европол

Европол, правоприлагащият орган на ЕС, е със седалище в Хага и разполага с национални звена на Европол (НЗЕ) във всяка държава членка. Европол е създадена през 1998 г.; настоящият ѝ правен статут като институция на ЕС се основава на Регламента относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Регламента за Европол)[812]. Целта на Европол е да съдейства за предотвратяването и разследването на организираната престъпност, тероризма и други форми на тежка престъпност, посочени в приложение I към Регламента за Европол, които засягат две или повече държави членки. Тя постига това, като обменя информация, а също и като действа като информационен център на ЕС, който прави анализи на разузнавателните данни и оценки на заплахите.

За да постигне своите цели, Европол е създала информационната система на Европол, която представлява база данни за обмен на разузнавателни данни и информация, свързани с престъпления, между държавите членки чрез техните НЗЕ. Информационната система на Европол може да се използва за предоставяне на данни, които се отнасят до: лица, които са заподозрени или които са били осъдени за извършването на престъпление, което попада в компетентността на Европол, или лица, за които са налице факти да се

811 Европейският надзорен орган по защита на данните издаде становище относно споразумението между ЕС и САЩ, в което препоръчва, наред с другото, да бъдат направени следните адаптации: 1) да се добави текстът „специално за целите, за които са били предадени“ към члена относно съхранението на данните не по-дълго, отколкото е необходимо или подходящо; и 2) да се изключи масовото прехвърляне на чувствителни данни, което би могло да е възможно. Вж. Европейски надзорен орган по защита на данните, Становище 1/2016, *Предварително становище на Европейския надзорен орган по защита на данните относно споразумението между Съединените американски щати и Европейския съюз за защита на личните данни във връзка с предотвратяването, разследването, разкриването и наказателното преследване на престъпления*, § 35.

812 Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета, ОВ L 135, 24.5.2016 г., стр. 53.

счита, че ще извършат такива престъпления. Европол и НЗЕ могат да въвеждат директно данни в информационната система на Европол и да извличат данни от нея. Единствено страната, която е въвела данните в системата, може да ги променя, коригира или заличава. Органите на ЕС, трети държави и международни организации също може да предоставят информация на Европол.

Европол може да получава данни и от публично достъпни източници, например интернет. Предаването на лични данни на органи на ЕС е разрешено само ако това е необходимо за изпълнението на задачите на Европол или на получаващия орган на ЕС. Предаването на лични данни на трети държави или международни организации се допуска единствено ако Европейската комисия реши, че тази държава или международна организация гарантира адекватно ниво на защита на личните данни („решение относно адекватното ниво на защита на личните данни"), или ако е налице международно споразумение или споразумение за сътрудничество. Европол може да получава и обработва лични данни, произхождащи от частноправни субекти и частни лица, само при стриктните условия, че посочените данни са предадени от НЗЕ в съответствие с националното му право, от точка за контакт в трета държава или международна организация, с която е установено сътрудничество посредством споразумение за сътрудничество, или от орган на трета държава или международна организация съгласно решение за адекватно ниво на защита на личните данни или с която ЕС е сключил международно споразумение. Целият обмен на информация се извършва чрез мрежово приложение за защитен обмен на информация (SIENA).

В отговор на новите развития бяха създадени специализирани центрове в Европол. През 2013 г. в Европол беше създаден Европейски център по киберпрестъпност[813]. Центърът служи като централно европейско информационно звено по въпросите на киберпрестъпността, което допринася за по-бързи реакции в случай на онлайн престъпления, разработва и разгръща цифрови съдебно-технически възможности и предоставя добри практики от разследвания на престъпления в кибернетичното пространство. Центърът акцентира върху престъпления в кибернетичното пространство, които:

- са извършени от организирани престъпни групи с цел реализиране на големи печалби, като например онлайн измами;

813 Вж. също ЕНОЗД (2012 г.), *Становище на Европейския надзорен орган по защита на данните относно съобщението на Европейската комисия до Съвета и Европейския парламент за създаването на Европейски център по киберпрестъпност*, Брюксел, 29 юни 2012 г.

- причиняват тежки щети на жертвите, например сексуална експлоатация на деца онлайн;

- засягат ключова инфраструктура и информационни системи в ЕС.

Европейският център за борба с тероризма беше създаден през януари 2016 г., за да оказва оперативна подкрепа на държавите членки при разследванията, свързани с терористични престъпления. Той прави кръстосани проверки на оперативни данни в реално време спрямо данните, с които Европол вече разполага, като бързо установява финансовите данни, съдържащи насочваща информация, и анализира цялата налична информация от разследванията, за да подпомогне съставянето на структурирана картина на дадена терористична мрежа[814].

Европейският център за борба с контрабандата на мигранти беше създаден през февруари 2016 г., след заседание на Съвета от ноември 2015 г., с цел да оказва подкрепа на държавите членки при разкриването и разбиването на престъпните мрежи, занимаващи се с контрабанда на мигранти. Той действа като информационен център за подпомагане на службите на Регионалната работна група на ЕС в Катания (Италия) и Пирея (Гърция), които съдействат на националните органи в няколко области, включително обмен на разузнавателна информация, наказателни разследвания и наказателно преследване на престъпни мрежи за контрабанда на хора[815].

Режимът за защита на данните, който урежда дейността на Европол, е засилен и използва за основа принципите на Регламента относно защитата на данните при обработването им от институции на ЕС[816], като е съобразен и с Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, модернизираната Конвенция № 108 и Препоръката за сектора на полицията.

Обработката на лични данни по отношение на пострадали от престъпления, свидетели или други лица, които могат да предоставят информация относно престъпления, или по отношение на лица под осемнадесетгодишна възраст

814 Вж. уебстраницата на Европол за Европейския център за борба с тероризма.

815 Вж. уебстраницата на Европол за Европейския център за борба с контрабандата на мигранти.

816 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

се позволява, ако е строго необходима и пропорционална за предотвратяване или борба с престъпления, попадащи в обхвата на целите на Европол[817]. Обработката на чувствителни лични данни е забранена, освен ако тази обработка не е строго необходима и пропорционална за предотвратяване или борба с престъпления, попадащи в обхвата на целите на Европол, и ако тези данни допълват други лични данни, които се обработват от Европол[818]. И в двата посочени по-горе случая единствено Европол има пряк достъп до съответните данни[819].

Съхранението на данните е разрешено само за такъв срок, какъвто е необходим и пропорционален, и неговото продължаване подлежи на преразглеждане на всеки три години; ако не бъде взето решение за продължаване, данните се заличават автоматично[820].

При определени условия Европол може да предава лични данни пряко на орган на ЕС или на орган на трета държава, или на международна организация[821]. Когато дадено нарушение на сигурността на личните данни може да има сериозни и неблагоприятни последици за правата и свободите на субекта на данните, то се съобщава без неоснователно забавяне на субекта на данните[822]. На равнището на държавите членки се определя национален надзорен орган, който да наблюдава обработването на лични данни от страна на Европол[823].

ЕНОЗД има отговорността да следи и осигурява защитата на основните права и свободи на физическите лица във връзка с обработката на лични данни от Европол, както и да предоставя съвети на Европол и на субектите на данните по всички въпроси, свързани с обработката на лични данни. За тази цел ЕНОЗД действа като орган, който разглежда жалби и извършва разследване по тях, като си сътрудничи тясно с националните надзорни органи[824]. ЕНОЗД и националните надзорни органи провеждат заседания най-малко два пъти годишно

817 Регламент за Европол, член 30, параграф 1.

818 *Пак там*, член 30, параграф 2.

819 *Пак там,* член 30, параграф 3.

820 *Пак там,* член 31.

821 *Пак там*, съответно член 24 и член 25.

822 *Пак там*, член 35.

823 Регламент за Европол, член 42.

824 *Пак там*, член 43 и член 44.

в рамките на Съвета за сътрудничество, който има консултативни функции[825]. Държавите членки са задължени да определят национален надзорен орган, който има за задача да извършва контрол на допустимостта на предаването на лични данни от съответната държава членка на Европол, както и на допустимостта на извличането и съобщаването на Европол на лични данни от съответната държава членка[826]. Държавите членки трябва също така да гарантират, че националният надзорен орган може да действа напълно независимо при изпълнението на неговите задачи и задължения по Регламента за Европол[827]. С цел проверка на законосъобразността на обработването на данни, самоконтрол и гарантиране на надлежната ненарушимост и сигурност на данните Европол води дневници или документация за своите дейности по обработване на данните. Тези дневници съдържат информация за операциите по обработване в автоматизираните системи за обработване на данни, свързани със събирането, промяната, достъпа, разкриването, комбинирането или заличаването на лични данни[828].

Решенията на ЕНОЗД може да се обжалват пред Съда на ЕС[829]. Всяко лице, което е претърпяло вреда в резултат на неправомерна операция по обработване на данни, има право да получи обезщетение за претърпяната вреда или от Европол, или от отговорната държава членка, като предяви иск пред Съда на ЕС в първия случай или пред компетентния национален съд във втория случай[830]. Освен това специална съвместна група за парламентарен контрол (СГПК), създадена съвместно от националните парламенти и Европейския парламент, може да упражнява контрол върху действията на Европол[831]. Всяко лице има право на достъп до личните данни, които Европол може да съхранява за него, както и право да поиска тези лични данни да бъдат проверени, коригирани или заличени. Тези права може да подлежат на изключения и ограничения.

825 *Пак там*, член 45.

826 *Пак там*, член 42, параграф 1.

827 *Пак там*, член 42, параграф 1.

828 *Пак там*, член 40.

829 *Пак там*, член 48.

830 *Пак там, член 50.*

831 *Пак там*, член 51.

Евроюст

Евроюст е създадена през 2002 г. като орган на ЕС с централен офис в Хага. Тя насърчава съдебното сътрудничество в разследванията и наказателните преследвания на сериозни престъпления, които засягат поне две държави членки[832]. Евроюст има компетенции:

- да стимулира и подобрява координацията на разследванията и наказателните преследвания между компетентните органи на отделните държави членки;

- да улеснява изпълнението на искания и решения, отнасящи се до съдебното сътрудничество.

Функциите на Евроюст се изпълняват от национални членове. Всяка държава членка изпраща съдия или прокурор в Евроюст, чийто статут се подчинява на националното право и който е овластен с необходимите правомощия, за да изпълнява необходимите задачи за стимулиране и подобряване на съдебното сътрудничество. Освен това националните членове действат съвместно като колегиален орган за изпълнението на специалните задачи на Евроюст.

Евроюст може да обработва лични данни, доколкото това е необходимо за постигането на нейните цели. Това обаче е ограничено до точно определена информация относно лицата, които са заподозрени в извършване или участие в престъпление или са осъдени за престъпление, което попада в областта на компетентност на Евроюст. Евроюст може също така да обработва определена информация относно свидетели или жертви на престъпления, които попадат в областта на нейната компетентност[833]. В извънредни случаи Евроюст може също, за ограничен период от време, да обработва по-широк кръг от лични данни, свързани с обстоятелствата на нарушението, когато тези данни имат непосредствено отношение към текущи разследвания. В рамките на своята

832 Съвет на Европейския съюз (2002 г.), Решение 2002/187/ПВР на Съвета от 28 февруари 2002 г. за създаване на Евроюст с оглед засилване на борбата срещу сериозната престъпност, ОВ L 63, 6.3.2002 г.; Съвет на Европейския съюз (2003 г.), Решение 2003/659/ПВР на Съвета от 18 юни 2003 г. за изменение на Решение 2002/187/ПВР за създаване на Евроюст за засилване борбата срещу сериозната престъпност, ОВ L 44, 29.9.2003 г.; Съвет на Европейския съюз (2009 г.), Решение 2009/426/ПВР на Съвета от 16 декември 2008 г. за укрепване на Евроюст и за изменение на Решение 2002/187/ПВР за създаване на Евроюст с оглед засилване на борбата срещу сериозната престъпност, ОВ L 138, 4.6.2009 г. (решенията относно Евроюст).

833 Консолидиран текст на Решение 2002/187/ПВР на Съвета, изменено с Решение 2003/659/ПВР на Съвета и с Решение 2009/426/ПВР на Съвета, член 15, параграф 2.

компетентност Евроюст може да си сътрудничи с други институции, органи и агенции на ЕС и да обменя лични данни с тях. Евроюст може също така да си сътрудничи и да обменя лични данни с трети държави и организации.

По отношение на защитата на данните Евроюст трябва да гарантира ниво на защита поне еквивалентно на принципите на модернизираната Конвенция № 108 и нейните последващи изменения. В случаи на обмен на данни трябва да се спазват определени правила и ограничения, които се въвеждат или в споразумение за сътрудничество, или в работно споразумение в съответствие с решенията на Съвета относно Евроюст и нейния процедурен правилник за защита на данните[834].

Създаден е независим съвместен надзорен орган (СНО) със задача да наблюдава обработването на лични данни, осъществявано от Евроюст. Лицата могат да подават жалби пред СНО, ако не са удовлетворени от решението на Евроюст на искането им за достъп, коригиране, блокиране или изтриване на лични данни. Ако Евроюст обработва незаконно лични данни, тя подлежи на отговорност в съответствие с националното законодателство на държавата членка, където са разположени централните ѝ офиси — Нидерландия, за всяка вреда, причинена на съответния субект на данни.

Перспективи

През юли 2013 г. Европейската комисия представи предложение за регламент за реформиране на Евроюст. Предложението беше придружено от предложение за създаване на Европейска прокуратура (вж. по-долу). Регламентът има за цел да рационализира нейните функции и структура, така че те да бъдат в съответствие с Договора от Лисабон. Освен това целта на реформата е да се направи ясно разграничение между оперативните задачи на Евроюст, изпълнявани от колегиалния орган на Евроюст, и нейните административни задачи. Това също така ще даде възможност на държавите членки да се съсредоточат в по-голяма степен върху оперативните задачи. Ще бъде създаден нов изпълнителен съвет, който ще подпомага колегиалния орган при изпълнението на административни задачи[835].

834 Процедурен правилник за обработване и защита на лични данни в Евроюст, ОВ C 68/01, 19 март 2005 г., стр. 1.

835 Вж. уебстраницата относно Евроюст на Европейската комисия.

Европейска прокуратура

Държавите членки притежават изключителна компетентност в областта на наказателното преследване на измамите и неправомерното прилагане на бюджета на ЕС, които имат и потенциални трансгранични последици. Разследването, повдигането и поддържането на обвинението и предаването на съд на извършителите на такива престъпления става все по-важно, особено предвид продължаващата икономическа криза[836]. Европейската комисия представи предложение за регламент за създаване на независима Европейска прокуратура[837] с цел борба с престъпленията, засягащи финансовите интереси на ЕС. Европейската прокуратура ще бъде създадена чрез процедурата на засилено сътрудничество, при която най-малко девет държави членки имат право да създадат разширено сътрудничество в дадена област в рамките на структурите на ЕС, но без участието на останалите държави от ЕС[838]. Белгия, България, Хърватия, Кипър, Чешката република, Естония, Финландия, Франция, Германия, Гърция, Латвия, Литва, Люксембург, Португалия, Румъния, Словения, Словакия и Испания вече се присъединиха към засиленото сътрудничество; Австрия и Италия изразиха намерение да се присъединят[839].

Европейската прокуратура ще бъде компетентна да разследва и повдига и поддържа обвинението за измами със средства на ЕС и други престъпления против финансовите интереси на ЕС с цел ефективно координиране на разследванията и наказателното преследване в различните видове национален правен ред и подобряване на използването на ресурсите и обмена на информация на европейско равнище[840].

Европейската прокуратура ще се оглавява от европейски прокурор, като във всяка държава членка ще има поне по един европейски делегиран прокурор,

836 Вж. Европейска комисия (2013 г.), Предложение за регламент на Съвета за създаване на Европейска прокуратура, COM(2013) 534 окончателен, Брюксел, 17 юли 2013 г., стр. 1 и 51. Виж също уебстраницата относно Европейската прокуратура на Комисията.

837 Европейска комисия (2013 г.), Предложение за регламент на Съвета за създаване на Европейска прокуратура, COM(2013) 534 окончателен, Брюксел, 17 юли 2013 г.

838 Договор за функционирането на Европейския съюз, член 86, параграф 1 и член 329, параграф 1.

839 Вж. Съвет на Европейския съюз (2017 г.), *„20 държави членки постигнаха съгласие по подробностите около създаването на Европейска прокуратура“*, Съобщение за медиите, 8 юни 2017 г.

840 Европейска комисия (2013 г.), Предложение за регламент на Съвета за създаване на Европейска прокуратура, COM(2013) 534 окончателен, Брюксел, 17 юли 2013 г., стр. 1 и стр. 51. Вж. също уебстраницата относно Европейската прокуратура на Комисията.

който ще отговаря за провеждането на разследванията и повдигането и поддържането на обвинението в тази държава членка.

В предложението се посочват строги предпазни мерки, за да се гарантират правата на лицата, участващи в разследванията на Европейската прокуратура, както е предвидено в националното законодателство, законодателството на ЕС и Хартата на основните права на ЕС. За действията по разследване, които засягат главно основните права, е необходимо предварително разрешение от национален съд[841]. Разследванията на Европейската прокуратура ще подлежат на съдебен контрол от националните съдилища[842].

За обработването на административни лични данни от страна на Европейската прокуратура е приложим Регламентът относно защитата на данните при обработването им от институции на ЕС[843]. За обработването на лични данни, свързани с оперативни въпроси, подобно на Европол и Европейската прокуратура ще има самостоятелен режим за защита на данните, сходен с този, който урежда дейностите на Европол и Евроюст, като се има предвид, че упражняването на функциите на Европейската прокуратура ще включва обработването на лични данни в рамките на правоприлагащите органи и прокуратурите на равнището на държавите членки. Ето защо правилата за защита на данните на Европейската прокуратура са почти идентични с правилата по Директивата за защита на данните, обработвани от полицейските и наказателноправните органи. Съгласно предложението за създаване на Европейска прокуратура обработването на лични данни трябва да е съобразено с принципите на законосъобразност и добросъвестност, ограничаване на целите, свеждане на данните до минимум, точност, цялост и поверителност. Европейската прокуратура трябва да прави, доколкото е възможно, ясно разграничение между личните данни на различните видове субекти на данни, например лица, осъдени за престъпление, лица, които просто са заподозрени, жертви и свидетели. Тя трябва също така да се стреми да проверява качеството на обработваните лични данни и да прави разграничение, доколкото е възможно, между личните данни, основани на факти, и личните данни, основани на лични оценки.

841 Европейска комисия (2013 г.), Предложение за регламент на Съвета за създаване на Европейска прокуратура, COM(2013) 534 окончателен, Брюксел, 17 юли 2013 г., член 26, параграф 4.

842 *Пак там*, член 36.

843 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

Предложението съдържа разпоредби относно правата на субектите на данни, по-специално правото на информация, правото на достъп до техните лични данни, на коригиране, заличаване и ограничаване на обработването, като предвижда, че тези права могат да бъдат упражнявани и косвено, чрез ЕНОЗД. В него са определени и принципите на сигурност на обработването и на отчетност, като Европейската прокуратура трябва да въведе подходящи технически и организационни мерки, за да се гарантира ниво на сигурност, съобразено с рисковете, породени от обработването, да води дневници на всички дейности по обработване и да извършва оценка на въздействието върху защитата на данните преди обработването, когато определен вид обработване (например обработване, включващо използването на нови технологии) може да доведе до висок риск за правата на лицата. На последно място, предложението предвижда определянето на длъжностно лице по защита на данните от колегиалния орган, което трябва да участва по подходящ начин във всички въпроси, свързани със защитата на личните данни, и да осигури спазването от страна на Европейската прокуратура на приложимото законодателство за защита на данните.

8.3.2 Защита на данните в рамките на съвместните информационни системи на равнището на ЕС

В допълнение към обмена на данни между държавите членки и създаването на специализирани органи на ЕС за борба с трансграничната престъпност, като например Европол, Евроюст и Европейската прокуратура, са изградени няколко съвместни информационни системи на равнището на ЕС, които да осигурят възможност за и да улеснят сътрудничеството и обмена на данни между компетентните национални органи и органи на ЕС за точно определени цели в областта на защитата на границите, имиграцията, предоставянето на убежище и митническите въпроси. Тъй като Шенгенското пространство първоначално беше създадено чрез международно споразумение и функционираше независимо от правото на ЕС, Шенгенската информационна система (ШИС) беше разработена на базата на многостранни споразумения и впоследствие стана обект правото на ЕС. Визовата информационна система (ВИС), Евродак, Европейската система за наблюдение на границите (Eurosur) и Митническата информационна система (МИС) бяха създадени като инструменти, регулирани от правото на ЕС.

Надзорът върху тези системи се споделя между националните надзорни органи и ЕНОЗД. За да се гарантира високо ниво на защита, тези органи си сътрудничат в рамките на координационни групи за надзор, които отговарят за следните широкомащабни информационни системи: 1) Евродак; 2) Визовата информационна система; 3) Шенгенската информационна система; 4) Митническата информационна система; и 5) Информационната система за вътрешния пазар[844]. Координационните групи за надзор обикновено заседават два пъти годишно, под ръководството на избран председател, и приемат насоки, обсъждат трансгранични случаи или приемат общи рамки за инспекции.

Европейската агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието (eu-LISA)[845], създадена през 2012 г., отговаря за оперативното управление на Шенгенската информационна система от второ поколение (ШИС II), Визовата информационна система (ВИС) и Евродак. Основната задача на eu-LISA е да осигурява ефективно, защитено и непрекъснато функциониране на информационните системи. Тя отговаря също така за приемането на необходимите мерки за гарантиране на сигурността на системите и сигурността на данните.

Шенгенска информационна система

През 1985 г. няколко държави членки от предишните Европейски общности се присъединиха към Споразумението между държавите от Икономическия съюз на Бенелюкс, Германия и Франция относно постепенната отмяна на проверките по общите граници (Шенгенското споразумение), което имаше за цел създаването на пространство за свободното движение на хора, невъзпрепятствано от гранични проверки в рамките на Шенгенската територия[846]. С цел неутрализиране на заплахата за обществената сигурност, която би могла да произтича от отворените граници, бяха въведени засилени гранични

844 Вж. уебстраницата относно координацията на надзора на Европейския надзорен орган по защита на данните.

845 Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета от 25 октомври 2011 година за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието, ОВ L 286, 2011 г.

846 Споразумение 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.

проверки по външните граници на Шенгенското пространство, както и тясно сътрудничество между националните полицейски и съдебни органи.

Като последица от присъединяването на още държави към Шенгенското споразумение, накрая Шенгенската система беше включена в правната рамка на ЕС с Договора от Амстердам[847]. Това решение беше въведено през 1999 г. Най-новата версия на Шенгенската информационна система, т. нар. ШИС II, започна да функционира на 9 април 2013 г. Сега тя служи на всички държави членки на ЕС[848], плюс Исландия, Лихтенщайн, Норвегия и Швейцария[849]. Европол и Евроюст също имат достъп до ШИС II.

ШИС II се състои от централна система (Ц-ШИС), национална система (Н-ШИС) във всяка държава членка и комуникационна инфраструктура между централната система и националните системи. Ц-ШИС съдържа определени данни относно лица и обекти, въвеждани от държавите членки. ШИС се използва от националните органи за граничен контрол, полицейските, митническите, визовите и съдебните органи в рамките на цялото Шенгенско пространство. Всяка държава членка управлява национално копие на Ц-ШИС, известно като национална Шенгенска информационна система (Н-ШИС), която се актуализира постоянно, като по този начин актуализира Ц-ШИС. В Н-ШИС се подават различни видове сигнали, когато:

- лицето няма право да влиза или пребивава на Шенгенска територия; или
- лицето или обектът се издирват от съдебни или правоприлагащи органи (напр. Европейски заповеди за арест, искания за проверки от разстояние); или

847 Европейски общности (1997 г.), Договор от Амстердам, изменящ Договора за Европейския съюз, Договорите за създаване на Европейските общности и някои свързани с тях актове, ОВ C 340, 1997 г.

848 Хърватия, Кипър и Ирландия извършват подготвителни дейности за интегриране в ШИС II, но все още не са част от нея. Вж. информацията относно Шенгенската информационна система, която е на разположение на уебсайта на Генерална дирекция „Миграция и вътрешни работи“ на Европейската комисия.

849 Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), ОВ L 381, 28.12.2006 г., и Съвет на Европейския съюз (2007 г.), Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), ОВ L 205, 7.8.2007 г.

- лицето е обявено за изчезнало; или

- стоки, като например банкноти, автомобили, камиони, огнестрелно оръжие и документи за самоличност, са обявени за откраднати или изгубени.

При подаден сигнал трябва да започнат последващи действия чрез бюрата SIRENE. ШИС II има нови функции, като възможността за въвеждане на биометрични данни, например дактилоскопични отпечатъци и снимки, на нови категории сигнали, като откраднати плавателни съдове, самолети, контейнери или платежни средства, както и по-разширени сигнали относно лица и обекти, копия на европейски заповеди за арест по отношение на лица, издирвани за арест, предаване или екстрадиране.

ШИС II се основава на два акта, които се допълват: Решението за ШИС II[850] и Регламента за ШИС II[851]. Законодателят на ЕС е използвал различни правни основания за приемането на решението и на регламента. С решението се урежда използването на ШИС II за цели, обхванати от полицейското и съдебното сътрудничество по наказателноправни въпроси (предишния трети стълб на ЕС). Регламентът се прилага за процедурите за подаване на сигнали в рамките на политиките в областта на визите, убежището, имиграцията, както и на другите политики, свързани със свободното движение на лицата (предишния първи стълб). Процедурите за подаване на сигнали във връзка с първия стълб трябваше да бъдат уредени с отделни актове предвид обстоятелството, че двата правни акта бяха приети преди Договора от Лисабон и премахването на структурата с няколко стълба.

И двата правни акта съдържат правила относно защитата на данните. Решението за ШИС II забранява обработването на чувствителни данни[852]. Обработването на лични данни е включено в обхвата на модернизираната Конвенция

850 Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), ОВ L 205, 7 август 2007 г.

851 Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), ОВ L 381, 28 декември 2006 г.

852 Решение за ШИС II, член 56; Регламент за ШИС II, член 40.

№ 108[853]. Освен това лицата имат право на достъп до свързаните с тях лични данни, въведени в ШИС II[854].

Регламентът за ШИС II урежда условията и процедурите за въвеждане и обработване на сигнали за отказ за влизане или пребиваване на граждани на държави извън ЕС. В него също така са предвидени правила за обмена на допълнителна информация и допълнителни данни във връзка с влизането на територията на държава членка или престоя там[855]. Този регламент също съдържа правила относно защитата на данните. Обработването на чувствителните категории данни, посочени в член 9, параграф 1 от Общия регламент относно защитата на данните, е забранено[856]. Регламентът за ШИС II също така съдържа определени права за субекта на данни, а именно:

- право на достъп до личните данни, свързани със субекта на данни[857];
- право на поправка на фактически неточните данни[858];
- право на заличаване на незаконно съхраняваните данни[859]; и
- право на уведомяване при издаване на сигнал срещу субекта на данни. Тази информация се предоставя в писмен вид заедно с копие на националното решение за издаване на сигнала или с позоваване на това решение[860].

Правото на информация не се предоставя, ако: 1) личните данни не са били получени от въпросния субект на данни и предоставянето на информацията е невъзможно или изисква непропорционални усилия, 2) субектът на данни вече разполага с информацията, или 3) когато националното законодателство позволява ограничаване правото на информация с цел, наред

853 Решение за ШИС II, член 57.

854 Решение за ШИС II, член 58; Регламент за ШИС II, член 41.

855 Регламент за ШИС II, член 2.

856 *Пак там*, член 40.

857 *Пак там*, член 41, параграф 1.

858 *Пак там*, член 41, параграф 5.

859 *Пак там*, член 41, параграф 5.

860 *Пак там*, член 42, параграф 1.

с другото, опазване на националната сигурност или предотвратяване на престъпления[861].

Както за Решението за ШИС II, така и за Регламента за ШИС II правото на достъп на лицата по отношение на ШИС II може да се упражнява във всяка държава членка съгласно нейното национално законодателство[862].

Пример: По делото *Dalea/Франция*[863] жалбоподателят е получил отказ за виза за посещение във Франция, тъй като френските органи са съобщили в Шенгенската информационна система, че следва да му бъде отказано влизане. Жалбоподателят се е опитал безуспешно да получи достъп и коригиране или заличаване на данните пред френската Комисия за защита на данните, а накрая — пред Държавния съвет. ЕСПЧ постановява, че съобщението за жалбоподателя в Шенгенската информационна система е било в съответствие със закона и е преследвало законната цел за защита на националната сигурност. Тъй като жалбоподателят не е доказал по какъв начин е бил наистина засегнат в резултат на отказа за влизане в Шенгенското пространство и тъй като са били приложени достатъчно мерки, за да бъде защитен той от произволни решения, намесата в правото му на зачитане на личния живот е била пропорционална. Така жалбата по член 8 на жалбоподателя е обявена за недопустима.

Компетентният национален надзорен орган във всяка държава членка осъществява надзор върху вътрешната Н-ШИС. Националният надзорен орган трябва да осигури извършването на одит на операциите по обработване на данните в рамките на вътрешната Н-ШИС поне веднъж на всеки четири години[864]. Националните надзорни органи и ЕНОЗД си сътрудничат и осигуряват координиран надзор на ШИС, докато ЕНОЗД отговоря за надзора на Ц-ШИС. С цел осигуряване на прозрачност съвместен доклад за дейностите се изпраща на Европейския парламент, Съвета и eu-LISA веднъж на всеки две години. Координационната група за надзор на ШИС II е създадена с цел да се гарантира координацията на ШИС II и тя заседава най-много два пъти

861 *Пак там*, член 42, параграф 2.

862 Регламент за ШИС II, член 41, параграф 1 и Решение за ШИС II, член 58.

863 ЕСПЧ, *Dalea/Франция,* № 964/07, 2 февруари 2010 г.

864 Регламент за ШИС II, член 60, параграф 2.

годишно. В тази група влизат ЕНОЗД и представители на надзорните органи на държавите членки, които са въвели ШИС II, а също и на Исландия, Лихтенщайн, Норвегия и Швейцария, тъй като ШИС важи и за тях, като се има предвид, че те са членове на Шенген[865]. Кипър, Хърватия и Ирландия все още не са част от ШИС II и поради това участват само като наблюдатели в координационната група за надзор. В рамките на координационната група за надзор ЕНОЗД и националните надзорни органи си сътрудничат активно, като обменят информация, взаимно си оказват съдействие при изпълнението на одити и проверки, съставят хармонизирани предложения за съвместни решения на потенциалните проблем и насърчават информираността по отношение на правата, свързани със защитата на данни[866]. Координационната група за надзор на ШИС II също така приема насоки, за да помогне на субектите на данни. Пример за това е наръчникът за подпомагане на субектите на данни при упражняването на техните права на достъп[867].

Перспективи

През 2016 г. Европейската комисия извърши оценка на ШИС[868], която показва, че са въведени национални механизми за субектите на данни за достъп, поправка и заличаване на техните лични данни в ШИС II или за получаване на компенсация във връзка с неточни данни. За да се подобрят ефикасността и ефективността на ШИС II, Европейската комисия представи три предложения за регламенти:

- регламент относно създаването, функционирането и използването на ШИС в областта на граничните проверки, който ще отмени Регламента за ШИС II;

- регламент относно създаването, функционирането и използването на ШИС в областта на полицейското сътрудничество и съдебното сътрудничество

865 Вж. уебстраницата на Шенгенската информационна система на Европейския надзорен орган по защита на данните.

866 Регламент за ШИС II, член 46 и Решение за ШИС II, член 62.

867 Вж. Координационна група за надзор на ШИС II, *Шенгенската информационна система. Ръководство за упражняване правото на достъп*, на разположение на уебсайта на ЕНОЗД.

868 Европейска комисия (2016 г.), Доклад на Комисията до Европейския парламент и Съвета относно оценката на Шенгенската информационна система от второ поколение (ШИС II) в съответствие с член 24, параграф 5, член 43, параграф 3 и член 50, параграф 5 от Регламент (ЕО) № 1987/2006 и член 59, параграф 3 и член 66, параграф 5 от Решение 2007/533/ПВР, COM(2016) 880 окончателен, Брюксел, 21 декември 2016 г.

по наказателноправни въпроси, който, наред с другото, ще отмени Решението за ШИС II; и

- регламент относно използването на ШИС за връщането на незаконно пребиваващи граждани на трети държави.

Важно е да се отбележи, че в допълнение към снимките и дактилоскопичните отпечатъци, които вече са част от настоящия режим на ШИС II, предложенията позволяват обработването и на други категории биометрични данни. В базата данни на ШИС ще се съхраняват и портретни снимки, отпечатъци на длани и ДНК профили. Освен това, въпреки че в Регламента за ШИС II и Решението за ШИС II се предоставя възможност за търсене по пръстови отпечатъци за идентифициране на дадено лице, с предложенията това търсене става задължително, ако самоличността на лицето не може да бъде установена по никакъв друг начин. Портретни снимки, снимки и отпечатъци на длани ще се използват за търсене в системата и за установяване на самоличността на лицата, когато това стане технически възможно. Новите правила относно биометричните характеристики пораждат специфични рискове за правата на лицата. В становището си относно предложенията на Комисията[869] ЕНОЗД отбелязва, че биометричните данни са изключително чувствителни и въвеждането им в такава широкомащабна база данни следва да се основава на подкрепена с доказателства оценка на необходимостта от включването им в ШИС. С други думи, следва да бъде доказана необходимостта от обработване на новите характеристики. ЕНОЗД също така счита, че е необходимо допълнително да се поясни какъв вид информация може да бъде включена в ДНК профила. Тъй като ДНК профилът може да включва чувствителна информация (най-показателният пример би бил информация, разкриваща здравословни проблеми), ДНК профилите, съхранявани в ШИС, следва да съдържат: „единствено минималната строго необходима информация за установяване на самоличността на изчезналото лице, като изключват изрично информацията относно расовия произход или здравословното състояние на това лице, както и всяка друга чувствителна информация“[870]. С предложенията обаче са въведени допълнителни предпазни мерки за ограничаване на събирането и по-нататъшното обработване на данни до това, което е строго необходимо за оперативни цели, както и за ограничаване на достъпа до тези лични данни до онези лица,

869 ЕНОЗД (2017 г.), Становище на ЕНОЗД относно новата правна основа на Шенгенската информационна система, Становище 7/2017, 2 май 2017 г.

870 *Пак там*, параграф 22.

които по оперативни причини трябва да ги обработват[871]. С предложенията eu-LISA се оправомощава да изготвя редовни доклади за държавите членки относно качеството на данните, за да се извършва редовен преглед на сигналите с цел гарантиране на качеството на данните[872].

Визова информационна система

Визовата информационна система (ВИС), също управлявана от eu-LISA, е разработена в подкрепа на прилагането на общата визова политика на ЕС[873]. ВИС позволява на държавите от Шенген да обменят данни относно кандидатите за виза чрез напълно централизирана система, която свързва консулствата и посолствата на държавите от Шенген извън ЕС с външните гранично-пропускателни пунктове на всички шенгенски държави. ВИС обработва данни във връзка с молбите за краткосрочни визи за посещение или транзитно преминаване през Шенгенското пространство. ВИС позволява на граничните органи да проверяват чрез биометрични характеристики, по-специално дактилоскопични отпечатъци, дали лицето, представящо визата, е нейният законен притежател, а също и да идентифицират лицата без или с фалшиви документи.

Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (Регламентът за ВИС) урежда условията и процедурите за предаване на лични данни по отношение на заявленията за издаване на визи за краткосрочно пребиваване. Той също така урежда решенията, вземани във връзка със заявленията, включително

871 Европейска комисия (2016 г.), Предложение за регламент на Европейския парламент и на Съвета относно създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение на Регламент (ЕС) № 515/2014 и за отмяна на Регламент (ЕО) № 1986/2006, Решение 2007/533/ПВР на Съвета и Решение 2010/261/ЕС на Комисията, COM (2016) 883 окончателен, Брюксел, 21 декември 2016 г.

872 *Пак там*, стр. 15.

873 Съвет на Европейския съюз (2004 г.), Решение 2004/512/ЕО на Съвета от 8 юни 2004 г. за създаване на Визова информационна система (ВИС), ОВ L 213, 15.6.2004 г.; Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (Регламент за ВИС), ОВ L 218, 13.8.2008 г.; Съвет на Европейския съюз (2008 г.), Решение 2008/633/ПВР на Съвета от 23 юни 2008 г. относно достъпа до Визовата информационна система (ВИС) за справки от оправомощени органи на държавите членки и от Европол с цел предотвратяване, разкриване и разследване на терористични действия и други тежки престъпления, ОВ L 218, 13.8.2008 г.

решенията за анулиране, отнемане или удължаване на дадена виза[874]. Регламентът за ВИС обхваща най-вече данните относно кандидата, неговите визи, снимки, дактилоскопични отпечатъци, връзки към предишни заявления за виза и досиета със заявленията на придружаващите го лица[875]. Достъпът до ВИС с цел да се въвеждат, изменят или заличават данни, се ограничава само до визовите органи, като се има предвид, че достъпът за преглед на данни се предоставя на визовите органи и на компетентните органи, отговарящи за проверките на външните гранично-пропускателни пунктове, имиграционните проверки и предоставянето на убежище.

При определени условия компетентните национални полицейски органи и Европол могат да поискат достъп до данни, въведени във ВИС, с цел предотвратяване, разкриване или разследване на терористични действия и други тежки престъпления[876]. Тъй като ВИС е разработена като инструмент за подпомагане на прилагането на общата визова политика, принципът на ограничение на целите, който – както е обяснено в глава 3.2 – изисква личните данни да бъдат обработвани само за конкретни, изрично указани и законни цели и да бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват, ще бъде нарушен, ако ВИС се превърне в инструмент за целите на правоприлагането. Поради тази причина националните правоприлагащи органи и Европол не разполагат с постоянен достъп до базата данни на ВИС. Достъп може да бъде предоставен единствено на база конкретен случай и при наличие на строги гаранции. Условията и гаранциите по отношение на достъпа и справките във ВИС от страна на тези органи са уредени в Решение 2008/633/ПВР на Съвета[877].

874 Регламент за ВИС, член 1.

875 Член 5 от Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (Регламент за ВИС), ОВ L 218, 13.8.2008 г.

876 Съвет на Европейския съюз (2008 г.), Решение 2008/633/ПВР на Съвета от 23 юни 2008 година относно достъпа до Визовата информационна система (ВИС) за справки от оправомощени органи на държавите членки и от Европол с цел предотвратяване, разкриване и разследване на терористични действия и други тежки престъпления, ОВ L 218, 13.8.2008 г.

877 *Пак там.*

Освен това Регламентът за ВИС урежда правата на субектите на данни. Те са:

- правото да бъдат информирани от отговорната държава членка за самоличността на проверяващия орган, който отговаря за обработването на лични данни в държавата членка, включително неговите данни за връзка; целите, за които техните лични данни ще бъдат обработени във ВИС; категориите лица, на които може да бъдат предадени данните (получателите); и срока за съхранение на данните. Освен това кандидатите за виза трябва да бъдат уведомени за факта, че събирането на техните лични данни във връзка с ВИС е задължително за разглеждането на тяхното заявление; държавите членки трябва също така да ги информират, че имат право на достъп до свързаните с тях данни, както и да изискат корекция или заличаване на тези данни, а също и право за получаване на информация относно процедурите за упражняване на тези права[878];

- право на достъп до свързаните с тях лични данни, въведени във ВИС[879];

- право на коригиране на неточните данни[880];

- право на заличаване на незаконно съхраняваните данни[881].

За да се гарантира упражняването на надзор върху ВИС, беше създадена координационната група за надзор на ВИС. Тя включва представители на ЕНОЗД и на националните надзорни органи и заседава два пъти годишно. Тази група се състои от представители на 28-те държави членки на ЕС, а също и на Исландия, Лихтенщайн, Норвегия и Швейцария.

Евродак

Евродак означава европейска дактилоскопия[882]. Евродак е централизирана система, съдържаща дактилоскопични данни на граждани на трети държави и лица без гражданство, които кандидатстват за убежище в една от

878 Регламент за ВИС, член 37.

879 *Пак там*, член 38, параграф 1.

880 *Пак там*, член 38, параграф 2.

881 *Пак там*, член 38, параграф 2.

882 Вж. уебстраницата относно Евродак на Европейския надзорен орган по защита на данните.

държавите членки на ЕС[883]. Системата е в действие от януари 2003 г., след приемането на Регламент № 2725/2000 на Съвета; от 2015 г. се прилага негов преработен текст. Целта на системата е най-вече да спомага за определянето на компетентната държава членка за разглеждането на дадена молба за убежище съгласно Регламент (ЕО) № 604/2013. Този регламент установява критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство (Регламент „Дъблин III“)[884]. Личните данни в Евродак могат да се използват само с цел улесняване на прилагането на Регламент „Дъблин III“[885].

Националните правоприлагащи органи и Европол имат право да сравняват дактилоскопични отпечатъци, свързани с наказателни разследвания, с дактилоскопичните отпечатъци, съдържащи се в Евродак, но единствено с цел предотвратяване, разкриване или разследване на терористични действия и други тежки престъпления. Тъй като Евродак е разработена като инструмент за подпомагане на прилагането на политиката на ЕС в областта на убежището, а не като инструмент за целите на правоприлагането, правоприлагащите органи имат достъп до базата данни само в определени случаи, при определени обстоятелства и при строго регламентирани условия[886]. За по-нататъшното използване на данните за целите на правоприлагането се

883 Регламент (ЕО) № 2725/2000 на Съвета от 11 декември 2000 г. за създаване на система „Евродак“ за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Дъблинската конвенция, ОВ L 316, 15.12.2000 г.; Регламент (ЕО) № 407/2002 на Съвета от 28 февруари 2002 г. за определяне на някои условия за прилагането на Регламент (ЕО) № 2725/2000 относно създаването на системата „Евродак“ за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Дъблинската конвенция, ОВ L 62, 5.3.2002 г. (регламенти за Евродак); Регламент (ЕС) № 603/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство и за искане на сравнения с данните в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането и за изменение на Регламент (ЕС) № 1077/2011 за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието, ОВ L 180, 29.6.2013 г., стр. 1 (Преработен регламент за Евродак).

884 Регламент (ЕС) № 604/2013 на Европейския парламент и на Съвета от 26 юни 2013 година за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство, ОВ L 180, 29.6.2013 г. (Регламент „Дъблин III“).

885 Преработен регламент за Евродак, ОВ L 180, 29.6.2013 г., стр. 1, член 1, параграф 1.

886 *Пак там*, член 1, параграф 2.

прилага Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, като данните, използвани за основната цел за улесняване на прилагането на Регламента Дъблин III, са защитени по Общия регламент относно защитата на данните. По-нататъшното предаване на лични данни, получени от държава членка или Европол по силата на преработения текст на Регламента за Евродак, на трета държава, международна организация или частен субект, установен във или извън ЕС, е забранено[887].

Евродак се състои от централно звено, управлявано от eu-LISA, за съхранение и съпоставяне на дактилоскопични отпечатъци и от система за електронно предаване на данни между държавите членки и централната база данни. Държавите членки снемат и предават отпечатъците на всяко лице на възраст поне 14 години, което потърси убежище на тяхната територия, и на всеки гражданин на държава извън ЕС или на лице без гражданство на възраст поне 14 години, което е задържано за неразрешено преминаване на техните външни граници. Освен това държавите членки могат да снемат и предават отпечатъците на граждани на държави извън ЕС или лица без гражданство, за които е установено, че пребивават на тяхната територия без разрешение.

Въпреки че всички държави членки могат да правят справки в Евродак и да искат сравняване с данните за дактилоскопични отпечатъци, единствено държавата членка, която е събрала дактилоскопичните отпечатъци и ги е предала на централното звено, има право да променя данните, като ги поправя, допълва или заличава[888]. Агенцията eu-LISA води записи за всяко обработване на данни, за да упражнява наблюдение върху защитата на данните и да гарантира сигурността на данните[889]. Националните надзорни органи подпомагат и съветват субектите на данни при упражняването на техните права[890]. Събирането и предаването на данните за дактилоскопични отпечатъци подлежат на съдебен контрол от националните съдилища[891]. За дейностите по обработване в централната система, която се управлява от eu-LISA що се отнася до Евродак, е приложим Регламентът относно защитата на данните

887 *Пак там*, член 35.

888 *Пак там*, член 27.

889 *Пак там*, член 28.

890 *Пак там*, член 29.

891 *Пак там*, член 29.

при обработването им от институции на ЕС[892] и върху тях се упражнява надзор от ЕНОЗД[893]. Ако дадено лице претърпи вреди поради неправомерно обработване или поради действие, несъвместимо с Регламента за Евродак, то има право да получи от отговорната държава членка обезщетение за претърпените вреди[894]. Следва обаче да се подчертае, че търсещите убежище са особено уязвима група от хора, които често са предприели дълго и рисковано пътуване. Поради тяхната уязвимост и несигурното положение, в което често се намират, докато очакват решението от разглеждането на тяхната молба за убежище, на практика упражняването на техните права, включително правото на обезщетение, може да се окаже трудно.

За да използват Евродак за целите на правоприлагането, държавите членки трябва да определят органите, които ще имат право да искат достъп, както и органите, които ще проверяват законосъобразността на исканията за сравняване[895]. Достъпът на националните органи и на Европол до данните за дактилоскопични отпечатъци в Евродак се подчинява на много строги условия. Запитващият орган трябва да подаде обосновано искане в електронна форма едва след като сравни данните с тези в другите съществуващи информационни системи, като например националните бази данни с дактилоскопични отпечатъци и ВИС. За да бъде сравняването пропорционално, следва да са налице много сериозни опасения за обществената сигурност. Сравняването трябва да е наистина необходимо, да е свързано с определен случай и да съществуват основателни причини да се смята, че сравняването ще подпомогне съществено предотвратяването, разкриването или разследването на което и да е от въпросните престъпления, особено когато има основателно подозрение, че заподозряно лице, извършител или жертва на терористично престъпление или друго тежко престъпление попада в категория, която е предмет на събирането на дактилоскопични отпечатъци в рамките на системата Евродак. Сравняването трябва да е ограничено единствено до данните за дактилоскопични отпечатъци. Европол също трябва да получи разрешение от държавата членка, която е събрала данните за дактилоскопични отпечатъци.

892 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

893 Преработен регламент за Евродак, ОВ L 180, 29.6.2013 г., стр. 1, член 31.

894 *Пак там*, член 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination“, *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, No. 2, pp. 108–129.

Личните данни, съхранявани в Евродак, които се отнасят за лица, търсещи убежище, се запазват за срок от 10 години, считано от датата, на която са взети дактилоскопичните отпечатъци, освен когато физическото лице получи гражданство на държава членка на ЕС. В този случай данните трябва да бъдат изтривани незабавно. Данните, отнасящи се за чужди граждани, задържани заради неразрешено преминаване на външната граница, се съхраняват за срок от 18 месеца. Тези данни трябва да бъдат изтрити незабавно, ако физическото лице получи разрешително за пребиваване, напусне територията на ЕС или получи гражданство в държава членка. Данните на лицата, на които е предоставено убежище, остават на разположение за сравняване в контекста на предотвратяването, разкриването и разследването на терористични действия и други тежки престъпления за период от три години.

Освен от всички държави членки на ЕС, Евродак се прилага също така и от Исландия, Норвегия, Лихтенщайн и Швейцария въз основа на международни споразумения.

За да се гарантира упражняването на надзор върху Евродак, беше създадена координационната група за надзор на Евродак. Тя включва представители на ЕНОЗД и на националните надзорни органи и заседава два пъти годишно. Тази група се състои от представители на 28-те държави членки на ЕС, а също и на Исландия, Лихтенщайн, Норвегия и Швейцария[896].

Перспективи

През май 2016 г. Комисията публикува предложение за нов преработен текст на Регламента за Евродак като част от реформа, чиято цел е да се подобри функционирането на общата европейска система за убежище (ОЕСУ)[897]. Предложеният преработен текст е важен, защото с него значително ще се разшири обхватът на първоначалната база данни на Eurodac. Първоначално Евродак

896 Вж. уебстраницата относно Евродак на Европейския надзорен орган по защита на данните.

897 Европейска комисия, Предложение за регламент на Европейския парламент и на Съвета за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство, за идентифициране на незаконно пребиваващ гражданин на трета държава или лице без гражданство и за искане на сравнения с данните в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането (преработен текст), COM(2016) 0272 окончателен, 4 май 2016 г.

беше създадена, за да подпомага прилагането на ОЕСУ, като предоставя дактилоскопични отпечатъци като доказателствен материал за оказване на помощ при определянето на държавата членка, компетентна за разглеждането на молба за международна закрила, подадена в ЕС. С предложения преработен текст ще се разшири обхватът на базата данни, за да се улесни връщането на незаконни мигранти[898]. Националните органи ще могат да правят справки с базата данни с цел идентифициране на граждани на трети държави, които пребивават незаконно в ЕС или които са влезли незаконно в ЕС, за да получат доказателства, които да помогнат на държавите членки да върнат тези лица. Освен това, докато сега действащият правен режим изисква събирането и съхраняването единствено на дактилоскопични отпечатъци, с предложението се въвежда събирането на портретни снимки на лицето[899], които са друг вид биометрични данни. С предложението също така ще се намали минималната възраст на децата, от които може да бъдат снемани биометрични данни — шест[900] вместо 14 години, което е минималната възраст съгласно регламента от 2013 г. Разширеният обхват на предложението означава, че то ще представлява намеса в правата на неприкосновеност на личния живот и защита на данните на по-голям брой лица, които може да бъдат включени в базата данни. За да се неутрализира тази намеса, в самото предложение и в измененията, предложени от комисията по граждански свободи, правосъдие и вътрешни работи на Европейския парламент[901], са положени усилия за засилване на изискванията за защита на данните. Към момента на

898 Вж. обяснителния меморандум към предложението, стр. 3.

899 Европейска комисия, Предложение за регламент на Европейския парламент и на Съвета за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство, за идентифициране на незаконно пребиваващ гражданин на трета държава или лице без гражданство и за искане на сравнения с данните в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането (преработен текст), COM(2016) 0272 окончателен, 4 май 2016 г., член 2, параграф 1.

900 *Пак там*, член 2, параграф 2.

901 Европейски парламент, *Доклад относно предложението за регламент на Европейския парламент и на Съвета за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство, за идентифициране на незаконно пребиваващ гражданин на трета държава или лице без гражданство и за искане на сравнения с данните в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането (преработен текст),* PE 597.620v03-00, 9 юни 2017 г.

изготвяне на наръчника обсъжданията по предложението в Парламента и в Съвета все още продължаваха.

Eurosur

Европейската система за наблюдение на границите (Eurosur)[902] е създадена с цел засилване на контрола на външните граници на Шенгенското пространство чрез разкриване, предотвратяване и борба с незаконната имиграция и трансграничната престъпност. Нейната функция е засилване на информационния обмен и оперативното сътрудничество между националните координационни центрове и Frontex — агенцията на ЕС, отговорна за разработване и прилагане на новото понятие „интегрирано управление на границите“[903]. Основните цели на системата са:

- намаляване на броя на незаконните имигранти, които успяват да влязат в ЕС, без да бъдат разкрити;
- намаляване на броя на смъртните случаи с незаконни мигранти чрез спасяване на повече човешки животи по море;
- повишаване на вътрешната сигурност в ЕС като цяло чрез подпомагане на предотвратяването на трансграничната престъпност[904].

Eurosur започна да функционира на 2 декември 2013 г. във всички държави членки с външни граници и на 1 декември 2014 г. в другите държави членки. Регламентът се прилага по отношение на наблюдението на външните сухоземни и морски граници и въздушните граници на държавите членки.

902 Регламент (ЕС) № 1052/2013 на Европейския парламент и на Съвета от 22 октомври 2013 г. за създаване на Европейската система за наблюдение на границите (Eurosur), ОВ L 295, 6.11.2013 г.

903 Регламент (ЕС) 2016/1624 на Европейския парламент и на Съвета от 14 септември 2016 г. за европейската гранична и брегова охрана, за изменение на Регламент (ЕС) 2016/399 на Европейския парламент и на Съвета и за отмяна на Регламент (ЕО) № 863/2007 на Европейския парламент и на Съвета, Регламент (ЕО) № 2007/2004 на Съвета и Решение 2005/267/ЕО на Съвета, ОВ L 251.

904 Вж. още: Европейска комисия (2008 г.), *Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите — Относно проучване на създаването на Европейска система за наблюдение на границите (Eurosur)*, COM(2008) 68 окончателен, Брюксел, 13 февруари 2008 г.; Европейска комисия (2011 г.), *Оценка на въздействието, придружаваща предложението за регламент на Европейския парламент и на Съвета за създаване на Европейската система за наблюдение на границите (Eurosur)*, Работен документ на службите на Комисията, SEC(2011) 1536 окончателен, Брюксел,12 декември 2011 г., стр. 18.

В рамките на Eurosur лични данни се обменят и обработват в много ограничена степен, тъй като държавите членки и Frontex имат право да обменят единствено идентификационни номера на кораби. В системата се обменя оперативна информация, като например местоположението на патрулите и инцидентите, и като общо правило обменяната информация не включва лични данни[905]. В изключителни случаи, когато в рамките на Eurosur се обменят лични данни, регламентът предвижда, че се прилага в пълна степен общата правна рамка на ЕС за защита на данните[906].

Следователно Eurosur гарантира правото на защита на данните, а именно като се предвижда, че обменът на лични данни трябва да е съобразен с критериите и гаранциите, определени от Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, и Общия регламент относно защитата на данните[907].

Митническа информационна система

Друга важна митническа система, създадена на равнище ЕС, е митническата информационна система (МИС)[908]. В процеса на установяване на вътрешен пазар всички проверки и формалности по отношение на стоки, които се движат в рамките на територията на ЕС, бяха отменени, което доведе до повишен риск от измами. Този риск беше неутрализиран чрез засилено сътрудничество между митническите администрации на държавите членки. Целта на МИС е да подпомогне държавите членки при предотвратяването, разследването и наказателното преследване на сериозни нарушения на правото на ЕС в областта на митниците и селското стопанство. МИС беше създадена чрез два правни акта, приети на различни правни основания. Регламент (ЕО) № 515/97 на Съвета се отнася до сътрудничеството между различните национални административни органи за борба с измамите в контекста

905 Европейска комисия, *EUROSUR: Защита на външните граници на Шенгенското пространство — защита на живота на мигрантите. EUROSUR накратко*, 29 ноември 2013 г.

906 Регламент (ЕС) № 1052/2013, съображение 13 и член 13.

907 *Пак там*, съображение 13 и член 13.

908 Съвет на Европейския съюз (1995 г.), Акт на Съвета от 26 юли 1995 г. за съставяне на Конвенцията за използване на информационните технологии за митнически цели, ОВ C 316, 27.11.1995 г., изменен от Съвета на ЕС през 2009 г., Регламент № 515/97 от 13 март 1997 г. относно взаимната помощ между административните органи на страните членки и сътрудничеството между тях и Комисията за осигуряване на правилното прилагане на митническото и селскостопанско законодателство, Решение 2009/917/ПВР на Съвета от 30 ноември 2009 г. относно използването на информационни технологии за митнически цели, ОВ L 323, 10.12.2009 г. (Решение за МИС).

на митническия съюз и общата селскостопанска политика, а Решение 2009/917/ПВР на Съвета има за цел системата да оказва съдействие при предотвратяване, разследване и преследване на тежки нарушения на митническото законодателство. Това означава, че МИС не се отнася само до правоприлагането.

Информацията, която се съдържа в МИС, включва лични данни във връзка със стоки, транспортни средства, стопански дейности, лица, стоки и парични средства, които са задържани, иззети или конфискувани. Категориите данни, които може да бъдат обработвани, са ясно определени и включват имената, гражданството, пола, мястото и датата на раждане на съответните лица, причината за въвеждане на техните данни в системата и регистрационния номер на превозното средство[909]. Тази информация може да се използва единствено за целите на наблюдението, докладването или извършването на конкретни проверки или за стратегически или оперативен анализ относно лица, за които има подозрение, че нарушават митническите разпоредби.

Достъп до МИС се предоставя на националните митнически, данъчни, селскостопански органи, органи по обществено здравеопазване и полицейски органи, както и Европол и Евроюст.

Обработването на лични данни трябва да бъде извършвано в съответствие със специфичните правила, установени в Регламент № 515/97 и Решение 2009/917/ПВР на Съвета, както и в съответствие с разпоредбите на Общия регламент относно защитата на данните, Регламента относно защитата на данните при обработването им от институции на ЕС, модернизираната Конвенция № 108 и Препоръката за сектора на полицията. ЕНОЗД е отговорен за упражняване на надзора по съответствието на МИС с Регламент (ЕО) № 45/2001. Той организира заседание поне веднъж в годината с всички национални надзорни органи за защита на данните, компетентни по надзорните дейности във връзка с МИС.

909 Вж. Решението за МИС, членове 24, 25 и 28.

Оперативна съвместимост между информационните системи на ЕС

Управлението на миграцията, интегрираното управление на границите по отношение на външните граници на ЕС и борбата срещу тероризма и трансграничната престъпност представляват важни предизвикателства и стават все по-сложни в глобализиращия се свят. През последните години ЕС работи върху нов всеобхватен подход за опазване и поддържане на сигурността, без да се засягат ценностите и основните свободи в ЕС. В тези усилия ефективният обмен на информация между националните правоприлагащи органи и между държавите членки и съответните агенции на ЕС е от ключово значение[910]. Съществуващите в ЕС информационни системи за управлението на границите и вътрешната сигурност имат своите съответни цели, институционална структура, субекти на данни и потребители. ЕС полага усилия да преодолее недостатъците във функционалните характеристики на управлението на данни в ЕС, фрагментирано между различните информационни системи, като ШИС II, ВИС и Евродак, като проучва възможностите за оперативна съвместимост[911]. Главната цел е да се гарантира, че компетентните полицейски, митнически и съдебни органи разполагат систематично с необходимата информация, за да изпълняват своите задължения, като същевременно се поддържа баланс по отношение на правата на неприкосновеност на личния живот, защита на данните и другите основни права.

910 Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент и Съвета: По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността, COM(2016) 205 окончателен, Брюксел, 6 април 2016 г., Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент, Европейския съвет и Съвета: Повишаване на сигурността в свят на мобилност: подобряване на информационния обмен в борбата срещу тероризма и по-сигурни външни граници, COM(2016) 602 окончателен, Брюксел, 14 септември 2016 г., Европейска комисия (2016 г.), Предложение за регламент на Европейския парламент и на Съвета относно използването на Шенгенската информационна система за връщането на незаконно пребиваващи граждани на трети държави. Вж. също Съобщение на Комисията до Европейския парламент, Европейския съвет и Съвета: Седми доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, COM(2017) 261 окончателен, Брюксел, 16 май 2017 г.

911 Съвет на Европейския съюз (2005 г.), Хагската програма: укрепване на свободата, сигурността и правосъдието в Европейския съюз, ОВ C 53, 2005 г., Европейска комисия (2010 г.), Съобщение на Комисията до Европейския парламент и до Съвета: Преглед на управлението на информацията в областта на свободата, сигурността и правосъдието, COM(2010) 385 окончателен, Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент и Съвета: По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността, COM(2016) 205 окончателен, Брюксел, 6 април 2016 г., Европейска комисия (2016 г.), Решение на Комисията от 17 юни 2016 година за създаване на Експертна група на високо равнище по въпросите на информационните системи и оперативната съвместимост, ОВ C 257, 15.7.2016 г.

Оперативната съвместимост представлява „способността на информационните системи да обменят данни и да дават възможност за споделяне на информация“[912]. Този обмен не трябва да засяга задължително строгите правила относно достъпа до и използването на данни, гарантирани от Общия регламент относно защитата на данните, Директивата за защита на данните, обработвани от полицейските и наказателноправните органи, Хартата на основните права на ЕС и всички други свързани правила. Нито едно интегрирано решение за управление на данните не трябва да засяга принципите на ограничение на целите, защита на данните на етапа на проектирането и защита на данните по подразбиране[913].

В допълнение към подобряването на функционалните характеристики на трите основни информационни системи — ШИС II, ВИС и Евродак, Комисията предложи да бъде създадена четвърта централизирана система за управление на границите, насочена към гражданите на трети държави: Система за влизане/излизане[914], която се очаква да бъде въведена до 2020 г.[915] Комисията публикува и предложение за създаване на Система на ЕС за информация за пътуванията и разрешаването им (ETIAS)[916] — система, в която ще се събира информация за лицата, които пътуват без виза в ЕС, така че да се осигури възможност за предварителни проверки за незаконна миграция и проверки за сигурност.

912 Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент и Съвета: По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността, COM(2016) 205 окончателен, Брюксел, 6 април 2016 г., стр. 14.

913 *Пак там*, стр. 4—5.

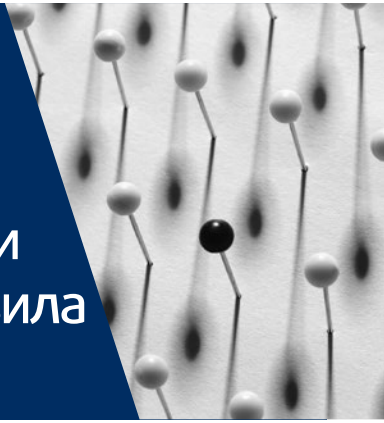
914 Европейска комисия (2016 г.), Предложение за регламент на Европейския парламент и на Съвета за създаване на Система за влизане/излизане с цел регистриране на данните относно влизането и излизането и данните относно отказа за влизане на граждани на трети държави, преминаващи външните граници на държавите членки на Европейския съюз, за определяне на условията за достъп до Системата за влизане/излизане за целите на правоприлагането и за изменение на Регламент (ЕО) № 767/2008 и Регламент (ЕС) № 1077/2011, COM(2016) 194 окончателен, Брюксел, 6 април 2016 г.

915 Европейска комисия (2016 г.), Съобщение на Комисията до Европейския парламент и Съвета: По-надеждни и по-интелигентни информационни системи в областта на границите и сигурността, COM(2016) 205 окончателен, Брюксел, 6 април 2016 г., стр. 5.

916 Европейска комисия (2016 г.), Предложение за регламент на Европейския парламент и на Съвета за създаване на Система на ЕС за информация за пътуванията и разрешаването им (ETIAS) и за изменение на регламенти (ЕС) № 515/2014, (ЕС) 2016/399, (ЕС) 2016/794 и (ЕС) 2016/1624, COM(2016) 731 окончателен, 16 ноември 2016 г.

9

Специални видове данни и техните съответни правила за защита на данните



ЕС	Обхванати въпроси	СЕ
Общ регламент относно защитата на данните Директива за правото на неприкосновеност на личния живот и електронни комуникации	**Електронни комуникации**	Модернизирана Конвенция № 108 Препоръка относно телекомуникационните услуги
Общ регламент относно защитата на данните, член 89	**Трудови правоотношения**	Модернизирана Конвенция № 108 Препоръка относно трудовите правоотношения ЕСПЧ, *Copland/ Обединеното кралство*, № 62617/00, 2007 г.
Общ регламент относно защитата на данните, член 9, параграф 2, букви з) и и)	**Медицински данни**	Модернизирана Конвенция № 108 Препоръка относно медицинските данни ЕСПЧ, *Z/Финландия*, № 22009/93, 1997 г.
Регламент относно клиничните изпитвания	**Клинични изпитвания**	
Общ регламент относно защитата на данните, член 6, параграф 4 и член 89	**Статистика**	Модернизирана Конвенция № 108 Препоръка относно статистическите данни

ЕС	Обхванати въпроси	СЕ
Регламент (ЕО) № 223/2009 относно европейската статистика Съд на ЕС, C-524/06, *Huber/Bundesrepublik Deutschland* [голям състав], 2008 г.	**Официална статистика**	Модернизирана Конвенция № 108 Препоръка относно статистическите данни
Директива 2014/65/ЕО относно пазарите на финансови инструменти Регламент (ЕС) № 648/2012 относно извънборсовите деривати, централните контрагенти и регистрите на транзакции Регламент (ЕО) № 1060/2009 относно агенциите за кредитен рейтинг Директива 2007/64/ЕО относно платежните услуги във вътрешния пазар	**Финансови данни**	Модернизирана Конвенция № 108 Препоръка № 90 (19) относно защитата на личните данни, използвани за платежни и други свързани с това операции ЕСПЧ, *Michaud/Франция*, № 12323/11, 2012 г.

В няколко случая на европейско равнище са били приети специални правни инструменти, чрез които общите правила на модернизираната Конвенция № 108 или на Директивата за защита на личните данни се прилагат по-подробно за конкретни ситуации.

9.1 Електронни комуникации

Ключови въпроси

- В препоръката на Съвета на Европа от 1995 г. се съдържат специални правила относно защитата на личните данни в областта на телекомуникационните услуги, и по-специално телефонните услуги.
- В ЕС обработването на лични данни, отнасящи се до предоставянето на комуникационни услуги, е уредено в Директивата за правото на неприкосновеност на личния живот и електронни комуникации.
- Поверителността на електронните комуникации се отнася не само до съдържанието на съобщението, но и до метаданните, като информация за това с кого и кога е осъществена комуникацията и с каква продължителност е била тя, и данни за местонахождението, например откъде е осъществена комуникацията.

При комуникационните мрежи съществува по-висок риск от необоснована намеса в личния живот на потребителите, тъй като мрежите предоставят

сериозни технически възможности за подслушване и наблюдение на комуникациите, осъществявани по тях. Логично е било счетено, че са необходими специални правила за защита на данните, за да се отговори на особените рискове за потребителите на комуникационни услуги.

През 1995 г. **Съветът на Европа** издаде Препоръка относно защита на личните данни в областта на телекомуникационните услуги, и по-специално телефонните услуги[917]. В съответствие с тази препоръка целите, за които се събират и обработват лични данни в контекста на телекомуникационните услуги, следва да се ограничават до свързването на потребителя с мрежата, предоставянето на самата телекомуникационна услуга, изготвянето на сметки, проверката, осигуряването на оптимално техническо функциониране и развитието на мрежата и услугите.

Специално внимание беше отделено също така на използването на комуникационните мрежи за изпращане на съобщения за директен маркетинг. Като общо правило не може да се изпращат съобщения за директен маркетинг на абонат, който изрично е отказал да получава рекламни съобщения. Автоматизирани повикващи устройства за предаване на предварително записани рекламни съобщения могат да се използват само ако абонатът е дал изрично съгласие. Националното законодателство трябва да предвижда подробни правила в тази област.

Що се касае до **правната рамка на ЕС**, след първи опит през 1997 г., през 2002 г. беше приета Директивата за правото на неприкосновеност на личния живот и електронни комуникации, изменена през 2009 г. Това беше направено с цел допълване и конкретизиране на разпоредбите на Директивата за защита на личните данни за сектора на телекомуникациите[918].

917 Съвет на Европа, Комитет на министрите (1995 г.), Препоръка Rec(95)4 до държавите членки относно защитата на личните данни в областта на телекомуникационните услуги, и по-специално телефонните услуги, 7 февруари 1995 г.

918 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, ОВ L 201, 31.7.2002 г. (Директива за правото на неприкосновеност на личния живот и електронни комуникации), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г.

Приложението на Директивата за правото на неприкосновеност на личния живот и електронни комуникации е ограничено до комуникационните услуги в обществените електронни мрежи.

В Директивата за правото на неприкосновеност на личния живот и електронни комуникации се разграничават три основни категории данни, създавани в процеса на комуникацията:

- данни, представляващи съдържанието на съобщенията, изпратени по време на комуникацията; тези данни са строго поверителни;

- данни, необходими за установяването и поддържането на комуникация, т. нар. метаданни, наричани данни за трафика в директивата, като информация за участниците в комуникацията, време и продължителност на комуникацията;

- в рамките на метаданните има данни, които се отнасят конкретно до местоположението на комуникационното устройство, т.нар. данни за местонахождението; тези данни същевременно са данни за местонахождението на потребителите на комуникационните устройства, по-специално що се отнася до потребителите на мобилни комуникационни устройства.

Данните за трафика могат да се използват от доставчика на услуги само с цел изготвяне на сметка и за техническо предоставяне на услугата. Със съгласието на субекта на данни обаче тези данни могат да бъдат разкривани на други администратори на данни, които предлагат услуги с добавена стойност, като предоставяне на свързана с местонахождението на потребителя информация за най-близката станция на метрото или аптека или прогнозата за времето за това място.

Съгласно член 15 от Директивата за електронната неприкосновеност, за друг достъп до данни за комуникациите в електронните мрежи трябва да са спазени изискванията за обоснована намеса в правото на защита на личните данни, както са заложени в член 8, параграф 2 от ЕКПЧ и потвърдени от Хартата на основните права на Европейския съюз в нейните членове 8 и 52. Подобен достъп може да бъде достъпът за целите на разследане на престъпления.

С измененията от 2009 г. в Директивата за правото на неприкосновеност на личния живот и електронни комуникации[919] се въведе следното:

- Ограниченията за изпращането на електронна поща за целите на директния маркетинг се разпростират върху кратките съобщения (SMS), мултимедийните услуги (MMS) и други видове подобни приложения; изпращането на електронна поща за целите на маркетинга е забранено, освен ако не е получено предварително съгласие. Без такова съгласие електронна поща за целите на маркетинга може да се адресира само до предишни клиенти, ако те са предоставили адреса на своята електронна поща и не възразяват на това.

- На държавите членки се възлага задължението да предвидят средства за правна защита срещу нарушения на забраната за изпращане на нежелани съобщения[920].

- Инсталирането на „бисквитки" на компютъра — софтуер, който наблюдава и записва действията на използващия го, вече не е позволено без неговото съгласие. Националното законодателство следва да регламентира по-подробно начините, по които следва да се изрази и получи съгласието, за да предложи достатъчна защита[921].

Ако настъпи нарушение на сигурността на данните в резултат на неразрешен достъп, загуба или унищожаване на лични данни, компетентният надзорен орган трябва да бъде уведомен незабавно. Абонатите трябва да бъдат информирани, ако е възможно да понесат щети като последица от нарушаването на сигурността на данните[922].

---

919 Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите, ОВ L 337, 18.12.2009 г.

920 Вж. изменената директива, член 13.

921 Вж. *пак там*, член 5; вж. също Работна група по член 29 (2012 г.), *Становище 04/2012 относно освобождаването от изискването за съгласие за някои бисквитки*, WP 194, Брюксел, 7 юни 2012 г.

922 Вж. също така Работна група по член 29 (2011 г.), *Работен документ № 01/2011 относно действащата нормативна уредба на ЕС в областта на нарушения по отношение на личните данни и препоръки за бъдещи развития на политиката*, WP 184, Брюксел, 5 април 2011 г.

Директивата за запазване на лични данни[923] задължаваше доставчиците на съобщителни услуги да запазват метаданни. Тази директива обаче беше отменена от Съда на ЕС (за повече информация вж. раздел 8.3).

Перспективи

През януари 2017 г. Европейската комисия прие ново предложение за Регламент за неприкосновеността на личния живот и електронните съобщения, който да замени старата Директива за неприкосновеността на личния живот и електронни комуникации. Целта продължава да бъде защитата на „основните права и свободи на физическите и юридическите лица при предоставянето и използването на електронни съобщителни услуги, и по-специално правата на зачитане на личния живот и тайната на съобщенията и защитата на физическите и юридическите лица при обработката на лични данни". В същото време новото предложение би трябвало да гарантира свободното движение на данни от електронни съобщения и електронни съобщителни услуги в рамките на Съюза[924]. Докато Общият регламент относно защитата на данните се отнася предимно до член 8 от Хартата на основните права на ЕС, предложеният регламент има за цел да включи член 7 от Хартата във вторичното законодателство на ЕС.

Регламентът ще адаптира разпоредбите на предишната директива към новите технологии и пазарната реалност и ще установи всеобхватна и последователна рамка с Общия регламент относно защитата на данните. В този смисъл Регламентът за неприкосновеността на личния живот и електронните съобщения ще бъде *lex specialis* пред Общия регламент относно защитата на данните, адаптирайки го към данните от електронни съобщения, които представляват лични данни. Новият регламент обхваща обработването на „данни от електронни съобщения", включително съдържанието и метаданните на електронните съобщения, които не са задължително лични данни. Териториалният обхват е ограничен до ЕС, включително когато данните, получени в ЕС, се обработват извън него, като са обхванати доставчиците на съобщителни

923 Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени във връзка с предоставянето на общественодостъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.4.2006 г.

924 Предложение за регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения), (COM(2017) 10 окончателен), член 1.

услуги *over the top*. Това са доставчиците на услуги, които доставят съдържание, услуги или приложения по интернет, без пряко участие на мрежов оператор или доставчик на интернет услуги. Примери за такива доставчици са Skype (гласови и видеообаждания), WhatsApp (съобщения), Google (търсене), Spotify (музика) или Netflix (видеосъдържание). За новия регламент ще са приложими механизмите за прилагане на Общия регламент относно защитата на данните.

Регламентът за неприкосновеността на личния живот и електронните съобщения се планира да бъде приет преди 25 май 2018 г., а дотогава във всички 28 държави членки ще е приложим Общият регламент относно защитата на данните. Това все пак зависи от споразумението между Европейския парламент и Съвета[925].

9.2 Данни за заетостта

Ключови въпроси

- Специални правила за защита на данните при трудови правоотношения се съдържат в Препоръката на Съвета относно данните за заетостта.
- В Общия регламент относно защитата на данните трудовите правоотношения се посочват конкретно само в контекста на обработването на чувствителни данни.
- Валидността на съгласието, което трябва да е било изразено свободно, като правно основание за обработването на данни може да е съмнителна, като се има предвид икономическата неравнопоставеност между работодателя и служителите. Обстоятелствата, при които е дадено съгласието, трябва да бъдат внимателно оценени.

Обработването на данните в контекста на трудовите правоотношения се подчинява на общото законодателство на ЕС в областта на защитата на личните данни. Един от регламентите[926] обаче се занимава конкретно със защитата

925 За повече информация вж. Европейска комисия (2017 г.), „Комисията предлага стриктни правила във връзка с неприкосновеността на личния живот при всички електронни комуникации и актуализира правилата за защита на данните за институциите на ЕС", Съобщение за медиите, 10 януари 2017 г.

926 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни, ОВ L 8, 12.1.2001 г.

на лицата при обработването на лични данни от европейските институции в контекста на трудовите правоотношения (наред с други неща). В Общия регламент относно защитата на данните трудовоправните отношения са изрично посочени в член 9, параграф 2, който предвижда, че лични данни може да бъдат обработвани за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право.

Съгласно Общия регламент относно защитата на данните служителят следва да може да отличава ясно данните, за които дава свободно съгласието си да бъдат обработвани/съхранявани, както и целите, за които се съхраняват неговите данни. Служителите следва също така да бъдат информирани за своите права и за периода, за който данните ще бъдат съхранявани, преди да дадат съгласието си. При нарушение на сигурността на личните данни, което може да доведе до висок риск за правата и свободите на физическите лица, работодателят трябва да уведоми служителя за това нарушение. Член 88 от регламента позволява на държавите членки да предвидят по-конкретни правила, за да гарантират защитата на правата и свободите по отношение на личните данни на наетите лица по трудово или служебно правоотношение.

Пример: В дело *Worten*[927] данните включват регистър на работното време, съдържащ ежедневното работно време и почивки, които съставляват лични данни. Националното законодателство може да изисква от работодателя да предоставя на компетентния национален орган за контрол на условията на труд достъп до регистъра на работното време. Това ще позволи незабавен достъп до съответните лични данни. Достъпът до личните данни обаче е необходим за целите на осъществяване от националния орган на контрол на правната уредба в областта на условията на труд[928].

Що се отнася до **Съвета на Европа** — Препоръката относно данните за заетостта е издадена през 1989 г. и е актуализирана през 2015 г.[929] Препоръката обхваща обработването на лични данни за целите на трудовите

927 Съд на ЕС, C-342/12, *Worten — Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, 30 май 2013 г., параграф 19.

928 *Пак там*, параграф 43.

929 Съвет на Европа, Комитет на министрите (2015 г.), Препоръка Rec(2015)5 до държавите членки относно обработването на лични данни в контекста на трудовите правоотношения, април 2015 г.

правоотношения както в частния, така и в публичния сектор. Обработването трябва да отговаря на определени принципи и ограничения, като например принципа на прозрачност и консултации с представители на работниците преди въвеждането на системи за следене на комуникациите на работното място. В препоръката също така се посочва, че работодателите следва да прилагат превантивни мерки, като например филтри, вместо да следят използването на интернет от работниците.

В работен документ на Работната група по член 29 е включено проучване на най-често срещаните проблеми, свързани със защитата на данните, характерни за областта на трудовите правоотношения[930]. Работната група е анализирала значението на съгласието като правно основание за обработването на данни за заетостта[931]. Тя констатира, че икономическата неравнопоставеност между работодателя, търсещ съгласие, и служителя, който дава такова, често поражда съмнения дали съгласието е било изразено свободно или не. Следователно обстоятелствата, при които се използва съгласие като правно основание за обработването на данни, следва да бъдат внимателно разгледани при оценяването на валидността на съгласието в контекста на трудовите правоотношения.

Често срещан проблем със защитата на данните в днешната типична работна среда е доколко е законосъобразно следенето на електронните комуникации на служителите на работното място. Често се твърди, че този проблем може лесно да бъде решен, като се забрани използването по време на работа на средствата за комуникация за лични цели. Подобна обща забрана обаче може да бъде несъразмерна и нереалистична. От особен интерес в този контекст са съдебните решения на ЕСПЧ по дело *Copland/Обединеното кралство* и дело *Bărbulescu/Румъния*.

Пример: По делото *Copland/Обединеното кралство*[932] използването на телефона, електронната поща и интернет от страна на служителка на колеж е било следено тайно, за да се установи дали прекалява

930 Работна група по член 29 (2017 г.), *Становище 2/2017 относно обработването на данни на работното място*, WP 249, Брюксел, 8 юни 2017 г.

931 Работна група по член 29 (2005 г.), *Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.*, WP 114, Брюксел, 25 ноември 2005 г.

932 ЕСПЧ, *Copland/Обединеното кралство*, № 62617/00, 3 април 2007 г.

с използването на оборудването на колежа за лични цели. ЕСПЧ постановява, че обажданията по телефона от служебното място се обхващат от понятията личен живот и лична кореспонденция. Следователно подобни обаждания и електронни съобщения, изпратени от работното място, както и информацията, произтичаща от следенето на личното използване на интернет, са защитени по силата на член 8 от ЕКПЧ. В случая на жалбоподателката не са били налице никакви разпоредби, уреждащи обстоятелствата, при които работодателите могат да следят използването на телефона, електронната поща и интернет от страна на служителите. Следователно намесата не е била в съответствие със закона. Съдът заключава, че е налице нарушение на член 8 от ЕКПЧ.

Пример: В дело *Bărbulescu/Румъния*[933] жалбоподателят е бил уволнен, защото е използвал интернет на работното място през работно време в нарушение на вътрешните правила. Неговият работодател е следял комуникациите му. Записите, които показват съобщения от изцяло личен характер, са представени по време на националното производство. Като се произнася, че член 8 е приложим, ЕСПЧ оставя открит въпроса дали ограничителните правила на работодателя са оставили в жалбоподателя разумно очакване за неприкосновеност на личния живот, но постановява, че указанията на работодателя не може да сведат личния социален живот на работното място до нула.

Що се отнася до въпросите по същество, на договарящите се страни е трябвало да се предостави широка свобода на преценка при оценяването на необходимостта от установяване на правна рамка, уреждаща условията, при които работодателят може да регулира електронните или други съобщения от непрофесионален характер на своите служители на работното място. Все пак националните органи е трябвало да гарантират, че въвеждането от страна на работодателя на мерки за следене на кореспонденцията и другите съобщения, независимо от обхвата и продължителността на тези мерки, е придружено от подходящи и достатъчни гаранции срещу злоупотреби. Пропорционалността и процедурните гаранции срещу всякакви форми на произвол са важни и ЕСПЧ определи редица фактори, които са от значение при дадените обстоятелства. Те включват, наред с другото, обхвата на следенето от страна на работодателя и степента на

933 ЕСПЧ, *Bărbulescu/Румъния* [голям състав], № 61496/08, 5 септември 2017 г., параграф 121.

навлизане в личния живот на служителя, последствията за служителя и дали са предвидени подходящи гаранции. Освен това националните органи е трябвало да гарантират, че служителят, чиито съобщения са били следени, има достъп до правни средства за защита пред съдебен орган, който разполага с компетентност да се произнася, поне по същество, дали са спазени определените критерии и дали са законосъобразни оспорваните мерки.

В този случай ЕСПЧ констатира нарушение на член 8, тъй като националните органи не са осигурили подходяща защита на правото на жалбоподателя на зачитане на личния живот и кореспонденцията и следователно не са успели да постигнат справедлив баланс между различните засегнати интереси.

Съгласно Препоръката на Съвета на Европа за данните за заетостта, личните данни, събирани за целите на трудовите правоотношения, следва да бъдат получавани пряко от самия служител.

Личните данни, събирани с цел наемане на работа, трябва да се ограничават до информацията, необходима за оценка на пригодността на кандидатите и техния потенциал за професионално развитие.

В препоръката специално се споменава за данните, събирани с цел оценка на работата или потенциала на отделните служители. Данните от тази субективна преценка трябва да се основават на добросъвестни и безпристрастни оценки и начинът, по който са формулирани, не трябва да е оскърбителен. Това се изисква в съответствие с принципите за добросъвестно обработване и за точност на данните.

Особен аспект на правото за защита на данните при взаимоотношенията работодател — служител е ролята на представителите на служителите. Тези представители може да получават лични данни на служителите само доколкото това е необходимо, за да бъдат представени интересите на служителите, или ако тези данни са необходими за изпълнението или упражняването на контрол на задълженията, предвидени в колективните трудови договори.

Чувствителните лични данни, събирани за целите на трудовите правоотношения, могат да бъдат обработвани само в определени случаи и при спазване на гаранциите, залегнали в националното право. Работодателите могат да искат

от служителите или кандидатите за работа информация за здравословното им състояние или да ги подлагат на медицински изследвания само ако това е необходимо. Това може да е: за определяне на пригодността им за съответната работа; за изпълняване на изискванията на профилактичната медицина; за защита на жизненоважните интереси на субекта на данните или на други служители и лица; за целите на отпускане на социални обезщетения или за отговаряне на искания на съдебни органи. Данни за здравето не може да се събират от източници, различни от съответния служител, освен ако не бъде получено изрично и информирано съгласие или когато това се предвижда от националното законодателство.

Съгласно Препоръката относно данните за заетостта служителите следва да бъдат информирани за целите на обработването на личните им данни, вида на събираните лични данни, субектите, на които редовно се предават данните, целите на подобно оповестяване и правното му основание. Електронните комуникации на работното място са достъпни единствено на основание, свързано със сигурността, или по други основателни причини, като такъв достъп се разрешава само след информиране на служителите, че работодателят може да има достъп до този вид комуникации.

Служителите трябва да имат право на достъп до своите данни за заетостта, както и право на коригиране или изтриване. Освен това служителите трябва да имат право да оспорват извършена преценка на тяхната работа, направена въз основа на обработване на лични данни. Тези права обаче могат да бъдат временно ограничавани за целите на вътрешни разследвания. Ако на служител бъде отказан достъп, коригиране или изтриване на лични данни за заетостта, националното право трябва да предвижда подходящи процедури за оспорване на този отказ.

9.3 Здравни данни

Ключов въпрос

- Медицинските данни са чувствителни данни и следователно са обект на специална защита.

Личните данни, отнасящи се до здравословното състояние на съответния субект на данни, се определят като чувствителни данни съгласно член 9, параграф 1 от Общия регламент относно защитата на данните и член 6 от модернизираната Конвенция № 108. Свързаните със здравето данни, съответно, подлежат на по-строг режим на обработване от нечувствителните данни. Общият регламент относно защитата на данните забранява обработването на „лични данни за здравословното състояние" (под което се разбира „всички данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или психическото здравословно състояние на субекта на данните в миналото, настоящето или бъдещето")[934], както и на генетични данни и на биометрични данни, освен ако това не е разрешено съгласно член 9, параграф 2. И двата вида данни са добавени в списъка на „специални категории данни"[935].

Пример: *В дело Z./Финландия*[936] бившият съпруг на жалбоподателката, заразен с ХИВ, е извършил редица сексуални престъпления. Впоследствие той е осъден за убийство по непредпазливост на основание на това, че умишлено е изложил своите жертви на опасност от заразяване с ХИВ. Националният съд определя пълното съдебно решение и документите по делото да останат поверителни за срок от 10 години въпреки молбите на жалбоподателката за по-дълъг период на поверителност. Тези молби са отхвърлени от апелативния съд и неговото решение съдържа пълните имена както на жалбоподателката, така и на бившия ѝ съпруг. ЕСПЧ постановява, че

934 Общ регламент относно защитата на данните, съображение 35.

935 *Пак там*, член 2.

936 ЕСПЧ, *Z/Финландия*, № 22009/93, 25 февруари 1997 г., параграфи 94 и 112; вж. също ЕСПЧ, *M.S./Швеция*, № 20837/92, 27 август 1997 г.; ЕСПЧ, *L.L./Франция*, № 7508/02, 10 октомври 2006 г.; ЕСПЧ, *I/Финландия*, № 20511/03, 17 юли 2008 г.; ЕСПЧ, *K.H. и други/Словакия,* № 32881/04, 28 април 2009 г.; ЕСПЧ, *Szuluk/Обединеното кралство,* № 36936/05, 2 юни 2009 г.

намесата не се счита за необходима в едно демократично общество, тъй като защитата на медицинските данни е от първостепенно значение за упражняване на правото на зачитане на личния и семейния живот, по-специално по отношение на информацията за заразяване с ХИВ, като се има предвид заклеймяването на това заболяване в много общества. Ето защо съдът заключава, че предоставянето на достъп до решението на апелативния съд, в което са описани самоличността и медицинското състояние на жалбоподателката, само 10 години след произнасянето на решението е в нарушение на член 8 от ЕКПЧ.

Съгласно **правото на ЕС** в член 9, параграф 2, буква з) от Общия регламент относно защитата на данните се позволява обработването на медицински данни, когато то е необходимо за целите на превантивната медицина, медицинската диагноза, осигуряването на грижи или лечение или за целите на управлението на услугите и системите за здравеопазване. Обработването е допустимо обаче само когато се извършва от медицинско лице, което е длъжно да спазва професионална тайна, или от друго лице, което е също обвързано с равностойно задължение.

Съгласно **правото на Съвета на Европа** в Препоръката относно медицинските данни на Съвета на Европа от 1997 г. се прилагат по-подробно принципите на Конвенция № 108 за обработването на данни от медицинско естество[937]. Предложените правила са в съответствие с тези от Общия регламент относно защитата на данните по отношение на законосъобразните цели на обработването на медицински данни, необходимите задължения за опазване на професионална тайна от страна на лицата, служещи си със здравните данни, и правата на съответните физически лица за прозрачност и достъп, коригиране и заличаване. Освен това медицинските данни, обработвани законосъобразно от здравни специалисти, не могат да бъдат предавани на правоприлагащи органи, освен ако не бъдат предоставени „достатъчни гаранции за предотвратяване на разкриване, несъвместимо със зачитането на [...] личния живот, гарантиран съгласно член 8 от ЕКПЧ“[938]. Националният закон трябва също така

937 Съвет на Европа, Комитет на министрите (1997 г.), Препоръка Rec(97)5 до държавите членки относно защитата на медицински данни, 13 февруари 1997 г. Обърнете внимание, че тази Препоръка е в процес на ревизиране.

938 ЕСПЧ, *Avilkina и други/Русия*, № 1585/09, 6 юни 2013 г., параграф 53. Виж също ЕСПЧ, *Biriuk/Литва,* № 23373/03, 25 ноември 2008 г.

да е „формулиран с достатъчно точност и да предлага подходяща правна защита срещу произволна намеса“[939].

Също така в Препоръката относно медицинските данни се съдържат специални разпоредби относно медицинските данни на неродени деца и недееспособни лица и относно обработването на генетични данни. Научните изследвания се признават изрично като основание за по-дългосрочно от необходимото съхранение на данните, въпреки че това обикновено изисква анонимизация. В член 12 от Препоръката относно медицинските данни се предлагат подробни разпоредби за случаи, при които изследователите се нуждаят от лични данни и анонимизираните данни са недостатъчни.

Използването на псевдоним може да бъде подходящ начин за задоволяване на нуждите на науката и същевременно за защита на интересите на съответните пациенти. Концепцията за използването на псевдоним в контекста на защитата на данните е обяснена по-подробно в раздел 2.1.1.

Препоръката на Съвета на Европа от 2016 г. относно данните, получени в резултат на генетични тестове, се отнася и до обработването на данни от медицинско естество[940]. Тази препоръка е от голямо значение за електронното здравеопазване, където ИКТ се използват за улесняване на медицинските грижи. Пример за това е изпращането на резултатите от тест за бащинство на пациента от един доставчик на здравни услуги към друг. Тази препоръка има за цел да защити правата на лицата, чиито лични данни се обработват за застрахователни цели, за да бъдат застраховани срещу рискове, свързани със здравето, физическата неприкосновеност, възрастта или смъртта на лицето. Застрахователите трябва да обосноват обработването на свързани със здравето данни, като то следва да е пропорционална на естеството и значението на съответния риск. За обработването на този вид данни е необходимо съгласието на субекта. Застрахователите следва също така да са въвели предпазни мерки за съхранението на свързаните със здравето данни.

Клиничните изпитвания, които включват оценка на ефектите на нови лекарства върху пациентите в документирана изследователска среда, имат

939 ЕСПЧ, *L.H./Латвия*, № 52019/07, 29 април 2014 г., параграф 59.

940 Съвет на Европа, Комитет на министрите (2016 г.), Препоръка Rec(2016)8 до държавите членки относно обработването за застрахователни цели на лични данни, свързани със здравето, включително данни, получени в резултат на генетични тестове, 26 октомври 2016 г.

значително отражение върху защитата на данните. Клиничните изпитвания на лекарствени продукти за хуманна употреба са уредени с Регламент (ЕС) № 536/2014 на Европейския парламент и на Съвета от 16 април 2014 г. относно клиничните изпитвания на лекарствени продукти за хуманна употреба, и за отмяна на Директива 2001/20/ЕО (Регламент за клиничните изпитвания)[941]. Основните елементи на Регламента за клиничните изпитвания са:

- оптимизирана процедура за подаване на заявление чрез портала на ЕС[942];
- срокове за оценяване на заявлението за клинични изпитвания[943];
- комисия по етика, която е част от процеса на оценяване, в съответствие с правото на държавите членки (и европейското законодателство, в което се определят съответните срокове)[944];
- повишена прозрачност на клиничните изпитвания и техните резултати[945].

В Общия регламент относно защитата на данните се посочва, че за целите на даване на съгласие за участие в научноизследователска дейност при клинични изпитвания се прилага Регламент (ЕС) № 536/2014[946].

На равнището на ЕС все още предстои да бъдат приети много други законодателни и други инициативи относно личните данни в сектора на здравеопазването[947].

Електронни здравни досиета

Електронното здравно досие се определя като „обстоен медицински запис или подобна документация за миналото и сегашното физическо и душевно

941 Регламент (ЕС) № 536/2014 на Европейския парламент и на Съвета от 16 април 2014 г. относно клиничните изпитвания на лекарствени продукти за хуманна употреба, и за отмяна на Директива 2001/20/ЕО (Регламент за клиничните изпитвания), ОВ L 158, 27.5.2014 г.

942 Регламент за клиничните изпитвания, член 5, параграф 1.

943 *Пак там*, член 5, параграфи 2—5.

944 *Пак там*, член 2, параграф 11.

945 *Пак там*, член 9, параграф 1 и съображение 67.

946 Общ регламент относно защитата на данните, съображения 156 и 161.

947 ЕНОЗД (2013 г.), *Становище на Европейския надзорен орган по защита на данните относно съобщението на Комисията „План за действие за електронно здравеопазване за периода 2012—2020 година — иновационно здравно обслужване през 21-ви век“*, Брюксел, 27 март 2013 г.

състояние на здравето на дадено лице в електронна форма, обезпечаващо бърз достъп на тези данни за медицинско лечение или други тясно свързани цели“[948]. Електронните здравни досиета са електронни версии на медицинската история на пациентите и може да включват клинични данни, свързани с тези лица, като например история на заболяванията, проблемите и здравословното състояние, лекарствата и лечениятa, както и резултатите и докладите от прегледи и лабораторни изследвания. До тези електронни файлове, които може да варират от досието в неговата цялост до откъси от него или негово резюме, имат достъп общопрактикуващият лекар, фармацевтът и други здравни специалисти. Концепцията за „електронното здравеопазване“ също е свързана с тези здравни досиета.

Пример: Г-н А е сключил застрахователна полица с дружество Б, застрахователя. Дружеството ще събере известна свързана със здравето информация от А, като например текущи здравословни проблеми или заболявания. Застрахователят следва да съхранява личните данни, свързани със здравето, на А отделно от останалите данни. Застрахователят също така трябва да съхранява личните данни, свързани със здравето, отделно от останалите лични данни. Това означава, че само лицето, което се занимава със случая на А, ще има достъп до свързаните със здравето данни на А.

Въпреки това електронните здравни досиета повдигат определени въпроси, свързани със защитата на данните, като например тяхната достъпност, правилно съхранение и достъп от страна на субекта на данните.

В допълнение към електронните здравни досиета на 10 април 2014 г. Европейската комисия публикува Зелена книга относно мобилното здравеопазване, като взе предвид, че мобилното здравеопазване е нова и бързо развиваща се област, която има потенциал да трансформира здравното обслужване и да повиши неговата ефикасност и качеството му. Терминът обхваща медицинските и обществените практики в областта на здравеопазването, осъществявани с помощта на мобилни устройства, като например мобилни телефони, устройства за наблюдение на здравното състояние на пациента, цифрови персонални помощници и други безжични устройства, както и приложения (например за подобряване на благосъстоянието), които

948 Препоръка на Комисията от 2 юли 2008 г. относно трансграничната оперативна съвместимост на системите за електронни здравни досиета, параграф 3, буква в).

могат да се свързват с медицински изделия или датчици[949]. В документа се подчертават рисковете за правото на защита на личните данни, до които прилагането на мобилното здравеопазване би могло да доведе, и се предвижда, че предвид чувствителния характер на здравните данни техническите решения в областта на мобилното здравеопазване следва да включват специални, подходящи за целта механизми за сигурност на данните на пациентите, като например криптиране, и съответни механизми за удостоверяване на пациента, за да се намалят рисковете за сигурността. Спазването на правилата за защита на личните данни, включително задължението за предоставяне на информация на субекта на данните, сигурността на данните и принципа за законна обработка на личните данни, е от изключително значение за изграждането на доверие в решенията за мобилното здравеопазване[950]. За тази цел отрасълът е изготвил кодекс за поведение въз основа на информация от широк кръг заинтересовани страни, включващи представители с експертни познания в областта на защитата на данните, саморегулирането и съвместното регулиране, ИКТ и здравеопазването[951]. Към момента на изготвяне на наръчника проектът на кодекс за поведение беше представен за коментари на Работната група за защита на личните данни по член 29, в очакване да бъде официално одобрен.

9.4 Обработване на данни за научноизследователски и статистически цели

Ключови въпроси

- Данните, събирани за статистически цели, не могат да се използват за каквито и да било други цели.
- Данните, събирани законно с каквато и да било цел, може да се използват в бъдещи периоди за статистически цели и за целите на научни или исторически проучвания, при условие че са въведени адекватни гаранции. За тази цел анонимизацията или псевдонимизацията преди предаването на данните на трети страни може да осигурят тези гаранции.

949 Европейска комисия (2014 г.), *Зелена книга относно мобилното здравеопазване*, COM(2014) 219 окончателен, Брюксел, 10 април 2014 г.

950 *Пак там,* стр. 8.

951 Проект на кодекс за поведение относно неприкосновеността на личния живот във връзка с мобилните здравни приложения, 7 юни 2016 г.

Правото на ЕС позволява обработването на данни за статистически цели или за целите на научни или исторически изследвания, при условие че са въведени подходящи гаранции за правата и свободите на субектите на данни. Те може да включват псевдонимизация[952]. Правото на ЕС или националното право може да предвижда определени дерогации от правата на субектите на данни, ако има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на легитимната цел на изследванията[953]. Може да бъдат въведени дерогации от правото на достъп на субекта на данни, правото на коригиране на данни, правото на ограничаване на обработването и правото на възражение.

Въпреки че данните, които са били законосъобразно събрани от администратор за някаква цел, може да бъдат повторно използвани от този администратор за негови собствени статистически цели или за целите на научни или исторически изследвания, данните би трябвало да бъдат анонимизирани или да бъдат обект на мерки, като псевдонимизация, в зависимост от контекста, преди предаването им на трета страна за статистически цели или за целите на научни или исторически изследвания, освен когато субектът на данни се е съгласил с това или това е изрично предвидено в националното законодателство. За разлика от анонимизираните данни, данните, които са обект на псевдонимизация, остават обект на Общия регламент относно защитата на данните[954].

По този начин регламентът прави изследванията обект на специално третиране по отношение на общите правила за защита на данните с цел избягване на ограниченията за развитието на научните изследвания и съобразяване с целта за постигане на европейско научноизследователско пространство, както е предвидено в член 179 от ДФЕС. Той предвижда широко тълкуване на обработването на лични данни за научноизследователски цели, в т.ч. технологичното развитие и демонстрационни дейности, фундаменталните научни изследвания, приложните научни изследвания и частно финансираните научни изследвания. В него се признава и значението на събирането на данни в регистри за научноизследователски цели и възможните трудности при пълното идентифициране на последващата цел на обработването на лични данни за научноизследователски цели към момента на събиране на данните[955]. По

952 Общ регламент относно защитата на данните, член 89, параграф 1.

953 *Пак там*, член 89, параграф 2.

954 *Пак там*, съображение 26.

955 *Пак там*, съображения 33, 157 и 159.

тази причина регламентът позволява обработването на данни за тези цели без съгласието на субектите на данни, при условие че са въведени подходящи гаранции.

Важен пример за използването на данни за статистически цели са официалните статистически данни, получавани от националните статистически бюра и статистическите бюра на ЕС въз основа на националните закони и разпоредбите на ЕС относно официалната статистика. Според тези закони и разпоредби гражданите и предприятията обикновено са задължени да разкриват данните на съответните статистически органи. Длъжностните лица, които работят в статистическите бюра, са обвързани от специални задължения за опазване на професионална тайна, които трябва да се спазват стриктно, тъй като са от съществено значение за високото ниво на доверие в гражданите, което е необходимо, ако данните ще се предоставят на статистическите органи[956].

Регламент (ЕО) № 223/2009 относно европейската статистика (Регламент относно европейската статистика) съдържа съществени правила за защитата на данните в контекста на извършването на официални статистически изследвания и по тази причина може също така да бъде считан за приложим, що се отнася до разпоредбите относно официалните статистически изследвания на национално равнище[957]. В регламента се поддържа принципът, че е необходимо достатъчно ясно правно основание за извършването на официални статистически дейности[958].

956 *Пак там*, член 90.

957 Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета от 11 март 2009 г. относно европейската статистика и за отмяна на Регламент (ЕО, Евратом) № 1101/2008 за предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности, на Регламент (ЕО) № 322/97 на Съвета относно статистиката на Общността и на Решение 89/382/ЕИО, Евратом на Съвета за създаване на Статистически програмен комитет на Европейските общности, ОВ L 87, 31.3.2009 г., изменен с Регламент (ЕС) 2015/759 на Европейския парламент и на Съвета от 29 април 2015 г. за изменение на Регламент (ЕО) № 223/2009 относно европейската статистика, ОВ L 123, 19.5.2015 г.

958 Този принцип трябва да бъде по-подробно описан в Кодекса на европейската статистическа практика, който в съответствие с член 11 от Регламента относно европейската статистика предоставя етични насоки относно това как да се извършват официалните статистически изследвания, включително и относно внимателното използване на лични данни.

Пример: В делото *Huber/Bundesrepublik Deutschland*[959] австрийски бизнесмен, който се е преместил в Германия, се оплаква, че събирането и съхранението на лични данни на чуждестранни граждани от германските органи в централен регистър (AZR) също и за статистически цели е нарушило правата му по Директивата за защита на личните данни. Предвид факта, че целта на Директива 95/46 е да се осигури еднаква степен на защита на данните във всички държави членки, Съдът на ЕС постановява, че за да се гарантира висока степен на защита в ЕС, понятието за необходимост в член 7, буква д) не може да има различно съдържание в зависимост от държавите членки. Следователно става въпрос за самостоятелно понятие на правото на ЕС, на което трябва да се направи тълкуване, отговарящо в пълна степен на предмета на Директива 95/46. Като отбелязва, че за статистически цели следва да е необходима единствено анонимна информация, Съдът на ЕС постановява, че германският регистър не е съвместим с изискването за необходимост по член 7, буква д).

В контекста на **Съвета на Европа** по-нататъшно обработване на данни за научни, исторически или статистически цели може да се извършва, когато това е в обществен интерес, и трябва да подлежи на подходящи гаранции[960]. Правата на субектите на данни може да бъдат ограничени и при обработването на данни за статистически цели, при условие че не съществува очевиден риск от нарушаване на техните права и свободи[961].

Препоръката относно статистическите данни, публикувана през 1997 г., обхваща извършването на статистически изследвания в публичния и частния сектор[962].

Данните, събирани от администратор за статистически цели, не може да се използват за каквито и да било други цели. Данните, които не са събирани за статистически изследвания, може да бъдат използвани по-нататък за такава цел. Препоръката относно статистическите данни също така дава възможност

959 Съд на ЕС, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г.; вж. по-специално параграф 68.

960 Модернизирана Конвенция № 108, член 5, параграф 4, буква б).

961 *Пак там*, член 11, параграф 2.

962 Съвет на Европа, Комитет на министрите (1997 г.), Препоръка Rec(97)18 до държавите членки относно защитата на лични данни, събирани и обработвани за статистически цели, 30 септември 1997 г.

за съобщаване на данни на трети страни, ако това се извършва само за статистически цели. В такива случаи страните следва да се договорят и писмено да определят обхвата на по-нататъшното законно използване на данните за статистически цели. Тъй като това не може да замени съгласието на субекта на данни, ако такова съгласие е необходимо, в националното законодателство трябва да са предвидени подходящи гаранции, за да се сведат до минимум рисковете от злоупотреба с лични данни, като например задължение за анонимизация или псевдонимизация на данните преди тяхното разкриване.

Хората, които професионално се занимават със статистически изследвания, трябва да бъдат обвързани със специални задължения за опазване на професионална тайна — каквато е обичайната практика в сферата на официалната статистика — съгласно националното законодателство. Това задължение трябва да бъде разширено също и до анкетьорите и другите събиращи лични данни, ако те се занимават със събиране на данни от субектите на данни или от други лица.

Ако статистическо проучване, в което се използват лични данни, не е разрешено от закона, съответните субекти на данни може да е необходимо да дадат съгласието си за използването на техните данни, за да стане то законно, или на тях може да е необходимо да им да се даде възможност да изразят възражение. Ако личните данни се събират за статистически цели чрез анкетьори, тези лица трябва да бъдат ясно информирани за това дали предоставянето на данните е задължително съгласно националното законодателство или не.

Когато дадено статистическо проучване не може да бъде извършено чрез използването на анонимизирани данни и наличието на лични данни е необходимо, събраните за тази цел данни следва да бъдат анонимизирани възможно най-скоро. Резултатите от статистическото проучване не трябва да дават ни най-малка възможност за идентифициране на съответните субекти на данни, освен ако това очевидно не би породило никакъв риск.

След приключването на статистическия анализ използваните лични данни следва да бъдат заличени или анонимизирани. В тези случаи в Препоръката относно статистическите данни се предлага идентификационните данни да бъдат съхранявани отделно от другите лични данни. Това означава например, че ключът за шифроване или списъкът с идентификационните синоними трябва да се съхранява отделно от другите данни.

9.5 Финансови данни

Ключови въпроси

- Въпреки че финансовите данни не се считат за чувствителни данни съгласно модернизираната Конвенция № 108 или Общия регламент относно защитата на данните, тяхното обработване изисква особени гаранции за осигуряване на точност и сигурност на данните.
- По-специално електронните платежни системи е нужно да разполагат с вградена защита на данните — така наречената защита на неприкосновеността на личния живот или на данните още на етапа на проектирането и по подразбиране.
- В тази област може да възникнат особени проблеми със защитата на данните поради нуждата от наличието на подходящи механизми за автентификация.

Пример: В дело *Michaud/Франция*[963] жалбоподателят, френски адвокат, е оспорил задължението си по силата на френското законодателство да съобщава, ако има подозрения за възможни дейности на негови клиенти, свързани с изпиране на пари. ЕСПЧ отбелязва, че изискването адвокати да съобщават на административните органи информация относно друго лице, която е станала тяхно достояние вследствие на професионални контакти с това лице, е намеса в правото на адвоката да се зачитат неговата кореспонденция и личният му живот по силата на член 8 от ЕКПЧ, тъй като тази концепция обхваща дейности от професионално или служебно естество. Намесата обаче е била законосъобразна и е преследвала законна цел, а именно предотвратяването на безредици и престъпления. Предвид факта, че адвокатите са задължени да съобщават за подозрителни дейности само при много ограничени обстоятелства, ЕСПЧ постановява, че това задължение е било пропорционално. Той заключава, че не е налице нарушение на член 8.

963 ЕСПЧ, *Michaud/Франция*, № 12323/11, 6 декември 2012 г. Вж. също ЕСПЧ, *Niemietz/Германия*, № 13710/88, 16 декември 1992 г., параграф 29; и ЕСПЧ, *Halford/Обединеното кралство*, № 20605/92, 25 юни 1997 г., параграф 42.

Пример: В делото *M.N. и други/Сан Марино*[964] жалбоподателят, който е италиански гражданин, е сключил споразумение за доверително управление с дружество, срещу което се води разследване. Това означава, че дружеството е било обект на претърсване и изземане на копия на документи (в електронен формат). Жалбоподателят е подал жалба пред съда на Сан Марино, твърдейки, че липсва каквато и да било връзка между него и предполагаемите престъпления. Съдът обаче обявява жалбата му за недопустима, тъй като той не е „заинтересована страна". ЕСПЧ постановява, че жалбоподателят е бил поставен в по-неизгодна позиция по отношение на съдебната защита в сравнение със „заинтересованите страни" и все пак неговите данни са били предмет на операциите по претърсване и изземване. Поради това Съдът постановява, че е налице нарушение на член 8.

Пример: В делото *G.S.B./Швейцария*[965] данни за банковата сметка на жалбоподателя са били изпратени на американските данъчни органи въз основа на споразумение за административно сътрудничество между Швейцария и САЩ. ЕСПЧ постановява, че това предаване на данни не е в нарушение на член 8 от ЕКПЧ, тъй като намесата в правото на неприкосновеност на личния живот на жалбоподателя е предвидена от закона, преследва легитимна цел и е пропорционална на засегнатия обществен интерес.

Прилагането на общата правна рамка за защита на данните по отношение на плащанията, така както се съдържа в Конвенция № 108, е развито от **Съвета на Европа** в Препоръка Rec(90)19 от 1990 г.[966] В нея се изяснява обхватът на законосъобразното събиране и използване на данни за плащанията, по-специално чрез разплащателни карти. Също така на националните законодатели се предлагат подробни препоръки за правилата за разкриване на трети страни на данни за плащанията, за сроковете за запазване на данните, за прозрачността, сигурността на данните и трансграничното предоставяне на данни, както и за надзора и средствата за правна защита. Съветът на Европа

964 ЕСПЧ, *M.N. и други/Сан Марино*, № 28005/12, 7 юли 2015 г.

965 ЕСПЧ, *G.S.B./Швейцария*, № 28601/11, 22 декември 2015 г.

966 Съвет на Европа, Комитет на министрите (1990 г.), Препоръка № R(90)19 относно защитата на личните данни, използвани за платежни и други свързани с това операции, 13 септември 1990 г.

разработи и Становище относно прехвърлянето на данъчни данни[967], в което са представени препоръки и въпроси, които трябва да бъдат взети предвид при разглеждането на прехвърлянето на данъчни данни.

ЕСПЧ позволява предаването на финансови данни — по-конкретно данните за банковата сметка на физическо лице — съгласно член 8 от ЕКПЧ, ако това е предвидено от закона, преследва легитимна цел и е пропорционално на засегнатия обществен интерес[968].

Що се отнася до **правото на ЕС**, електронните платежни системи, които включват обработване на лични данни, трябва да отговарят на изискванията на Общия регламент относно защитата на данните. Следователно тези системи трябва да гарантират защита на данните още на етапа на проектирането и по подразбиране. Защитата на данните още на етапа на проектирането задължава администратора да въведе подходящи технически и организационни мерки с оглед на прилагането на принципите на защита на данните. Защита на данните по подразбиране означава, че администраторът трябва да гарантира, че единствено личните данни, които са необходими за конкретна цел, може да бъдат обработвани по подразбиране (вж. раздел 4.4). По отношение на финансовите данни Съдът на ЕС е постановил, че прехвърлените данъчни данни може да представляват лични данни[969]. В тази връзка Работната група за защита на личните данни по член 29 издаде насоки за държавите членки, в които бяха включени критерии за гарантиране на спазването на правилата за защита на данните при автоматичен обмен на лични данни за данъчни цели по автоматизиран начин[970]. Освен това влязоха в сила редица правни инструменти за регулиране на финансовите пазари и дейностите на

967 Съвет на Европа, Консултативен комитет на Конвенция № 108 (2014 г.), Становище относно последиците за защитата на данните от механизмите за автоматичен обмен между държавите на данни за административни и данъчни цели, 4 юни 2014 г.

968 ЕСПЧ, *G.S.B./Швейцария*, № 28601/11, 22 декември 2015 г.

969 Съд на ЕС, C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 1 октомври 2015 г., параграф 29.

970 Работна група за защита на личните данни по член 29 (2015 г.), Изявление на Работната група по член 29 относно автоматичния обмен между държавите на данни за административни и данъчни цели, 14/EN WP 230.

кредитните институции и инвестиционните посредници[971]. Други правни инструменти подпомагат борбата със злоупотребата с вътрешна информация и с манипулирането на пазарите[972]. Основните области, оказващи въздействие върху защитата на данните, са:

- запазването на документацията за финансовите сделки;
- предаването на лични данни на трети държави;
- записването на телефонни разговори или електронни съобщения, включително правомощията на компетентните органи да изискват телефонни записи и сведения за преноса на данни;
- разкриването на лична информация, включително публикуването на санкции;
- надзорните и разследващите правомощия на компетентните органи, включително проверки на място и навлизане в частни обекти за изземване на документи;
- механизмите за докладване за нарушения, т.е. схеми за подаване на сигнали за нарушения; и
- сътрудничеството между компетентните органи на държавите членки и Европейския орган за ценни книжа и пазари (ESMA).

В тези области има и други въпроси, на които е обърнато специално внимание, включително събирането на данни за финансовото състояние на

971 Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 година относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС, ОВ L 173, 12.6.2014 г.; Регламент (ЕС) № 600/2014 на Европейския парламент и на Съвета от 15 май 2014 година относно пазарите на финансови инструменти и за изменение на Регламент (ЕС) № 648/2012, ОВ L 173, 12.6.2014 г.; Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 година относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО, ОВ L 176, 27.6.2013 г.

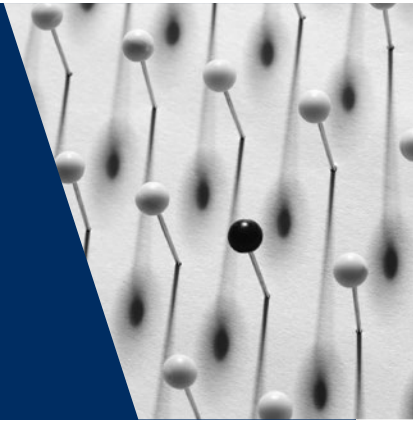
972 Регламент (ЕС) № 596/2014 на Европейския парламент и на Съвета от 16 април 2014 година относно пазарната злоупотреба (Регламент относно пазарната злоупотреба) и за отмяна на Директива 2003/6/ЕО на Европейския парламент и на Съвета и директиви 2003/124/ЕО, 2003/125/ЕО и 2004/72/ЕО на Комисията, ОВ L 173, 12.6.2014 г.

съответните субекти на данните[973] или трансграничното плащане чрез банкови преводи, което неизбежно води до движение на лични данни[974].

973 Регламент (ЕО) № 1060/2009 на Европейския парламент и на Съвета от 16 септември 2009 г. относно агенциите за кредитен рейтинг, ОВ L 302, 17.11.2009 г., последно изменен с Директива 2014/51/ЕС на Европейския парламент и на Съвета от 16 април 2014 година за изменение на Директива 2003/71/ЕО, Директива 2009/138/ЕО, Регламент (ЕО) № 1060/2009, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010 във връзка с правомощията на Европейския надзорен орган (Европейския орган за застраховане и професионално пенсионно осигуряване) и на Европейския надзорен орган (Европейския орган за ценни книжа и пазари), ОВ L 153, 22.5.2014 г.; Регламент (ЕС) № 462/2013 на Европейския парламент и на Съвета от 21 май 2013 година за изменение на Регламент (ЕО) № 1060/2009 относно агенциите за кредитен рейтинг, ОВ L 146, 2013 г.

974 Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 ноември 2007 г. относно платежните услуги във вътрешния пазар, за изменение на директиви 97/7/ЕО, 2002/65/ЕО, 2005/60/ЕО и 2006/48/ЕО и за отмяна на Директива 97/5/ЕО, ОВ L 319, 5.12.2007 г., изменена с Директива 2009/111/ЕО на Европейския парламент и на Съвета от 16 септември 2009 година за изменение на директиви 2006/48/ЕО, 2006/49/ЕО и 2007/64/ЕО по отношение на банки — филиали на централни институции, определени елементи на собствения капитал, големи експозиции, надзорна уредба и управление при кризи, ОВ L 302, 17.11.2009 г.

10 Съвременните предизвикателства в областта на защитата на личните данни



Цифровата ера или ерата на информационните технологии се характеризира с широко използване на компютрите, интернет и цифровите технологии. Това включва събирането и обработването на големи обеми от данни, включително лични данни. Събирането и обработването на лични данни в една глобализирана икономика означава нарастване на броя на трансграничните потоци от данни. Това обработване може да доведе до значителни и видими ползи в ежедневието: интернет търсачките улесняват достъпа до значителни обеми информация и знания, услугите за социални мрежи дават възможност на хората в целия свят да общуват, да изразяват мнението си и да мобилизират подкрепа за социални, екологични и политически каузи, а дружествата и потребителите се възползват от ефективни и ефикасни маркетингови техники, които стимулират икономиката. Технологиите и обработването на лични данни също така представляват незаменими инструменти за държавните органи в борбата им срещу престъпността и тероризма. По същия начин големите информационни масиви – събирането, съхранението и анализът на големи обеми информация с цел определяне на модели и прогнозиране на поведението – „могат да бъдат източник на значителна стойност за обществото, като подобряват производителността, резултатите от работата на публичния сектор и социалното участие“[975].

Въпреки своите многобройни ползи цифровата ера създава и предизвикателства пред неприкосновеността на личния живот и защитата на данните, тъй като огромни количества лична информация се събират и обработват по

975 Съвет на Европа, Консутативен комитет на Конвенция № 108, *Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви*, T-PD(2017)01, Страсбург, 23 януари 2017 г.

все по-сложни и непрозрачни начини. Развитието на технологиите доведе до разработването на масивни набори от данни, които могат лесно да бъдат съпоставени и анализирани допълнително с цел търсене на модели или приемане на решения, основаващи се на алгоритми, които могат да предоставят безпрецедентен поглед върху човешкото поведение и личния живот[976].

Новите технологии са мощни инструменти и могат да бъдат особено опасни, ако попаднат в неподходящи ръце. Държавните органи, които извършват дейности по масово наблюдение и които могат да използват тези технологии, са пример за значителното въздействие, което тези технологии могат да окажат върху правата на физическите лица. През 2013 г. разкритията на Едуард Сноудън относно функционирането на мащабни програми за следене на интернет и телефонните разговори от страна на разузнавателните служби в някои държави предизвикаха сериозни опасения относно опасностите от дейностите по следене за неприкосновеността на личния живот, демократичното управление и свободата на изразяване. Масовото наблюдение и технологиите, които дават възможност за глобализирано съхранение и обработване на лична информация и достъп до всички данни едновременно, може да засегнат самата същност на правото на неприкосновеност на личния живот[977]. Освен това те могат да окажат отрицателно въздействие върху политическата култура и да имат възпиращ ефект върху демокрацията, творчеството и иновациите[978]. Самите опасения, че държавата може постоянно да следи и анализира поведението и действията на гражданите, могат да ги обезкуражат да изразяват мнението си по определени въпроси и водят до недоверие и предпазливо отношение[979]. Тези предизвикателства накараха редица публични органи, изследователски центрове и организации на гражданското общество да анализират потенциалните въздействия на новите технологии върху обществото. През 2015 г. Европейският надзорен орган по защита

976 Европейски парламент (2017 г.), Резолюция относно последиците за основните права, породени от големи информационни масиви: неприкосновеност на личния живот, защита на личните данни, недопускане на дискриминация, сигурност и правоприлагане (P8_TA-PROV(2017)0076), Страсбург, 14 март 2017 г.

977 Вж. ООН, Генерална асамблея, *Доклад на специалния докладчик на ООН за насърчаване и защита на правата на човека и основните свободи в борбата с тероризма*, Ben Emmerson, A/69/397, 23 септември 2014 г., параграф 59. Вж. също ЕСПЧ, *Информационен бюлетин относно масовото наблюдение,* юли 2017 г.

978 ЕНОЗД (2015 г.), *„Посрещане на предизвикателствата на големите информационни масиви“*, Становище 7/2015, Брюксел, 19 ноември 2015 г.

979 Вж. по-специално Съд на ЕС, съединени дела C-293/12 и C-594/12, *Digital Rights Ireland Ltd/ Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г., параграф 37.

на данните стартира няколко инициативи с цел оценяване на въздействието на големите информационни масиви и интернет на предметите върху морала. По-специално той учреди етична консултативна група, която цели да насърчава „отворена, информирана дискусия относно етиката в областта на цифровите технологии, която да позволи на ЕС да реализира ползите от технологиите за обществото и икономиката и същевременно да затвърди правата и свободите на хората, особено правото на личен живот и защита на данните“[980].

Обработването на лични данни също така е мощен инструмент в ръцете на корпорациите. Днес то може да разкрие подробна информация за здравето или финансовото положение на дадено лице — информация, която след това корпорациите използват, за да вземат важни решения за лицата, като например за здравните застрахователни премии, които да се прилагат за тях, или за тяхната кредитоспособност. Техниките за обработване на данни може да окажат въздействие и върху демократичните процеси, когато се използват от политици или корпорации за оказване на влияние върху изборите, например чрез „микротаргетиране“ на комуникациите на гласоподавателите. С други думи, въпреки че първоначално неприкосновеността на личния живот се възприемаше като право на защита на лицата срещу необоснована намеса от страна на публичните органи, в съвременната епоха тя може да бъде застрашена и от правомощията на частни субекти. Това повдига въпроси относно използването на технологии и прогнозни анализи в решенията, които засягат ежедневието на лицата, и засилва необходимостта да се гарантира спазването на изискванията в областта на основните права при всяко обработване на лични данни.

Защитата на данните е неразделно свързана с технологичните, социалните и политическите промени. Ето защо би било невъзможно да се направи изчерпателен списък на бъдещите предизвикателства. В настоящата глава се разглеждат избрани области във връзка с големите информационни масиви, социалните мрежи в интернет и цифровия единен пазар на ЕС. В нея не се прави изчерпателна оценка на тези области от гледна точка на защитата на данните, а се изтъкват множеството възможни взаимодействия между новите или променените човешки дейности и защитата на данните.

980 ЕНОЗД, Решение от 3 декември 2015 г. за учредяване на външна консултативна група по етичните измерения на защитата на данните („Етичната консултативна група“).

10.1 Големи информационни масиви, алгоритми и изкуствен интелект

Ключови въпроси

- Революционните иновации в сферата на ИКТ формират нов начин на живот, където социалните отношения, стопанската дейност, частните и публичните услуги са взаимосвързани в цифрово отношение, като по този начин се създава все по-голям обем данни, много от които са лични данни.
- Правителствата, предприятията и гражданите все повече работят в основана на данни икономика, в която самите данни се превърнаха в ценни активи.
- Понятието „големи информационни масиви“ се отнася едновременно до самите данни и до техния анализ.
- Личните данни, обработвани чрез анализ на големи информационни масиви, попадат в обхвата на законодателството на ЕС и на Съвета на Европа.
- Дерогациите от правилата за защита на данните и правата в тази област са ограничени до избрани права и до конкретни ситуации, при които прилагането на дадено право би било невъзможно или би изисквало непропорционални усилия от страна на администраторите на данни.
- Изцяло автоматизираното вземане на решения като цяло е забранено, освен в специални случаи.
- Осведомеността сред лицата и упражняването на контрол от тяхна страна са от ключово значение за гарантиране на прилагането на правата.

В нашия все по-цифровизиран свят всяка дейност оставя цифрова следа, която може да бъде събрана, обработена и оценена или анализирана. С новите информационни и комуникационни технологии се събират и записват все повече данни[981]. До неотдавна нито една технология не беше в състояние да анализира или да оцени информационните масиви или да извлече полезни заключения. Данните просто бяха прекалено многобройни, за да бъдат оценени, и твърде сложни, зле структурирани и бързо развиващи се, за да бъдат установени определени тенденции и навици.

981 Европейска комисия, Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Към просперираща икономика, основана на данни“, COM(2014) 442 окончателен, Брюксел, 2 юли 2014 г.

10.1.1 Определяне на големите информационни масиви, алгоритмите и изкуствения интелект

Големи информационни масиви

„Големи информационни масиви“ е модерен термин, който може да се отнася до няколко понятия в зависимост от контекста. Той най-общо включва „нарастващата технологична способност за събиране, обработване и извличане на нова и прогнозна информация от голям обем, скорост и разнообразие от данни“[982]. Следователно понятието „големи информационни масиви“ обхваща едновременно самите данни и анализа на данните.

Източниците на данните са най-различни по вид и включват хора и техни лични данни, машини или датчици, информация за климата, спътникови изображения, цифрови снимки и видеоматериали или GPS сигнали. Голяма част от данните и информацията обаче са лични данни – име, снимка, електронен адрес, номер на банкова сметка, проследяване на данните от GPS, публикации в уебсайтове на социални мрежи, медицинска информация или IP адрес на компютър[983].

Терминът „големи информационни масиви“ се отнася и до **обработването**, анализа и оценката на масивите от данни и налична информация, т.е. за придобиването на полезна информация за целите на анализа на големи информационни масиви. Това означава, че събраните данни и информация може да бъдат използвани за цели, различни от първоначално предвидените, например определяне на статистически тенденции, или за по-персонализирани услуги, като например реклама. Всъщност когато наистина съществуват

982 Съвет на Европа, Консултативен комитет към Конвенция № 108, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., на стр. 2; Европейска комисия, Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Към просперираща икономика, основана на данни“, COM(2014) 442 окончателен, Брюксел, 2 юли 2014 г., на стр. 4; Международен съюз по далекосъобщения (2015 г.), Препоръка Y.3600 „Големи информационни масиви — изисквания и капацитет въз основа на изчисления в облак“.

983 Европейска комисия, Информационен бюлетин „Реформата на ЕС в областта на защитата на данните и големите информационни масиви“; Съвет на Европа, Консултативен комитет към Конвенция № 108, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., стр. 2.

технологии за събиране, обработване и оценяване на големи информационни масиви, може да бъде комбинирана и подложена на повторна оценка всякакъв вид информация: финансови операции, кредитоспособност, медицинско лечение, частно потребление, професионална дейност, проследяване и избрани маршрути, използване на интернет, електронни карти и смартфони, видео- или комуникационно наблюдение. Анализът на големите информационни масиви дава ново количествено измерение на данните, което може да бъде оценено и използвано в реално време, например за предоставяне на персонализирани услуги на потребителите.

Алгоритми и изкуствен интелект

Изкуственият интелект (ИИ) се отнася до интелигентността на машини, които действат като „интелигентни агенти". Като интелигентни агенти някои устройства могат, с помощта на софтуер, да усещат средата около себе си и да предприемат действия съгласно алгоритми. Терминът ИИ се прилага, когато машина имитира „когнитивни" функции, например обучение и разрешаване на проблеми, които обикновено се свързват с хората[984]. За да имитират процеса на вземане на решения, съвременните технологии и софтуер използват алгоритми, чрез които устройствата вземат „автоматизирани решения". Алгоритъмът може да се опише най-добре като поетапна процедура за изчисляване, обработване на данни, оценка и автоматизирано мислене и вземане на решения.

Подобно на анализа на големи информационни масиви, ИИ и създаваните от него автоматизирани решения изискват да се компилират и обработват големи обеми от данни. Тези данни може да идват от самото устройство (загряване на спирачките, гориво и др.) или от заобикалящата го среда. Профилирането например е процес, който може да разчита на автоматизирано вземане на решения в съответствие с предварително определени модели или фактори.

Пример: Профилиране и целева реклама

Профилирането въз основа на големи информационни масиви включва търсенето на модели, които отразяват „характеристиките на тип личност" – например когато дружества за онлайн пазаруване предлагат

984 Russel, Stuart и Norvig, Peter, *Artificial Intelligence: A Modern Approach (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, pp. 27, 32–58, 968–972; Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed.),* 2009, Upper Saddle River, New Jersey: Prentice Hall, p. 2.

продукти, които „и вие може да харесате“, въз основа на информацията, събрана от продуктите, които преди това са били поставени в кошницата на клиента. Колкото повече са данните, толкова по-ясна е картината. Смартфонът например е мощен въпросник, който лицата попълват с всяко използване, съзнателно и несъзнателно.

Съвременната психография — науката за изучаване на личностните характеристики — използва метода OCEAN, въз основа на който определя видовете разглеждани характери. „Големите пет“ личностни черти са: откритост (колко отворени сте за нови преживявания?), добросъвестност (до каква степен сте перфекционист?), екстровертност (колко общителен сте?), приемливост (колко внимателен и отзивчив сте към сътрудничество?) и невротизъм (лесно ли се разстройвате?). Тази информация профилира въпросното лице, неговите нужди и страхове, начина му на действие и т.н. След това тя се допълва с другата информация за лицето, събрана от всички налични източници – от посредниците на данни, социалните мрежи (включително „харесванията“ на публикации и публикуваните снимки) до слушаната онлайн музика или данните от GPS и проследяване.

Масивите на профилите, които са създадени чрез техники за анализ на големи информационни масиви, впоследствие се сравняват, за да се установят сходни модели и да се определят групите от личности. Следователно посоката на потока от информация относно поведението и нагласите на определени личности е обърната. С достъпа до големи информационни масиви и тяхното използване тестът за личностните характеристики действа в обратен ред, като информацията за поведението и нагласите днес се използва за определяне на личността на съответното лице. Комбинираната информация за „харесванията“ в социалните мрежи, данните от проследяването, слушаната музика или гледаните филми дава възможност да се изгради ясна картина на личността на дадено лице, позволявайки на предприятията да публикуват целеви реклами и/или информация в съответствие с „личността“ на това лице. Преди всичко тази информация може да се обработва в реално време[985].

985 Техниките и новият софтуер за обработване оценяват в реално време информацията за това какво харесва дадено лице, какво разглежда то, когато пазарува онлайн, или какво слага в кошницата с покупки онлайн и могат да предложат „продукти“, които може да представляват интерес въз основа на събраната информация.

10.1.2 Балансиране на ползите и рисковете, свързани с големите информационни масиви

Съвременните техники за обработване на данни са в състояние да обхванат големи масиви от данни, да импортират бързо нови данни, да осигуряват обработване в реално време на информацията при кратки срокове за реагиране (дори в случай на сложни искания) и да предоставят възможност за множество и едновременни искания, като могат да анализират различни видове информация (снимки, текстове или номера). Тези технологични иновации дават възможност да се структурират, обработват и оценяват в реално време масиви от данни и информация[986]. Чрез експоненциално увеличаване на обема на наличните и анализирани данни вече могат да се постигнат резултати, които биха били невъзможни при анализ в по-дребни мащаби. Големите информационни масиви спомогнаха за развитието на нова сфера на стопанска дейност, в която може да се появят нови услуги както за предприятията, така и за потребителите. Стойността на личните данни на гражданите на ЕС може да нарасне до почти 1 трилион евро годишно до 2020 г.[987] Следователно големите информационни масиви могат да предложат нови **възможности**, произтичащи от оценката на масивите от данни, за нови социални, икономически или научни познания, които могат да бъдат от полза както за физическите лица, така и за предприятията и правителствата[988].

986 Разработването на софтуер за обработването на големи информационни масиви все още е на ранен етап. Все пак неотдавна бяха разработени програми за анализ, по-специално за анализ на масиви от данни и информация в реално време, свързани с дейностите на физическите лица. Възможността за анализ и обработване на големи информационни масиви по структуриран начин осигури нови средства за профилиране и целева реклама. Европейска комисия, Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Към просперираща икономика, основана на данни", COM(2014) 442 окончателен, Брюксел, 2 юли 2014 г.; Европейска комисия, Информационен бюлетин „Реформата на ЕС в областта на защитата на данните и големите информационни масиви", и Съвет на Европа, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., на стр. 2.

987 Европейска комисия, Информационен бюлетин „Реформата на ЕС в областта на защитата на данните и големите информационни масиви".

988 Международна конференция на комисарите по неприкосновеността на личния живот и защитата на данните (2014 г.), Резолюция относно големите информационни масиви, и Европейска комисия, Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Към просперираща икономика, основана на данни", COM(2014) 442 окончателен, Брюксел, 2 юли 2014 г., на стр. 2; Европейска комисия, Информационен бюлетин „Реформата на ЕС в областта на защитата на данните и големите информационни масиви", и Съвет на Европа, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., на стр. 1.

Анализът на големи информационни масиви може да разкрие закономерности между различните източници и масиви от данни, давайки възможност за осигуряване на полезна информация в области като науката и медицината. Такъв е случаят например в области като здравеопазването, безопасността на храните, интелигентните транспортни системи, енергийната ефективност и градоустройството. Този анализ на информацията в реално време може да бъде използван за подобряване на въведените системи. В научноизследователската дейност нови знания може да се получат чрез комбиниране на големи количества данни и статистически оценки, особено в дисциплините, в които оценката на голяма част от данните до момента се извършва само ръчно. Може да бъдат разработени нови видове лечение, адаптирани към отделните пациенти, въз основа на сравнения с масивите от налична информация. Дружествата се надяват, че анализът на големи информационни масиви ще им позволи да придобият конкурентно предимство, да реализират потенциални икономии и да създадат нови бизнес области чрез пряко, индивидуализирано обслужване на потребителите. Държавните агенции се надяват да постигнат подобрения в областта на наказателното правосъдие. Стратегията на Комисията за цифров единен пазар за Европа отбелязва потенциала на основаните на данни технологии и услуги и на големите информационни масиви да послужат като катализатор на икономически растеж, нововъведения и цифровизация в ЕС[989].

Големите информационни масиви обаче носят и **рискове**, които обикновено са свързани с три техни характеристики: обем, скорост и разнообразие на обработваните данни. Обемът се отнася до количеството обработвани данни, разнообразието — до броя и многообразието на видовете данни, а скоростта — до бързината на обработване на данните. Специфични съображения за защита на данните възникват най-вече когато анализът въз основа на големи информационни масиви се използва върху големи масиви от данни, за да се извлече нова и прогнозна информация с цел вземане на решения, отнасящи се до отделни лица и/или групи[990]. Рисковете за защитата на данните и неприкосновеността на личния живот, свързани с големите информационни масиви, бяха подчертани в становища на ЕНОЗД и на Работната група по

989 Резолюция на Европейския парламент от 14 март 2017 г. относно последиците за основните права, породени от големи информационни масиви: неприкосновеност на личния живот, защита на личните данни, недопускане на дискриминация, сигурност и правоприлагане (2016/2225(INI).

990 Съвет на Европа, Консултативен комитет към Конвенция № 108, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., стр. 2.

член 29, в резолюции на Европейския парламент и в документи по политиката на Съвета на Европа[991].

Рисковете може да включват неправомерна употреба на големите информационни масиви от лица с достъп до масивите от информация посредством манипулиране, дискриминация или потискане на отделни лица или на конкретни групи в обществото[992]. Когато се събират, обработват и оценяват масиви от лични данни или информация за поведението, тяхното използване може да доведе до значителни нарушения на основните права и свободи, които надхвърлят правото на неприкосновеност на личния живот. Степента, в която може да бъде засегната неприкосновеността на личния живот и личните данни, е невъзможно да се измери точно. Според Европейския парламент няма методология за основана на обективни данни оценка на цялостното въздействие на големите информационни масиви, но има данни, че анализът въз основа на големи информационни масиви може да окаже значително хоризонтално въздействие в целия частен и публичен сектор[993].

Общият регламент относно защитата на данните включва разпоредби относно правото на субекта да не бъде обект на автоматизирано вземане на решения, включително профилиране[994]. Въпросът относно неприкосновеността на личния живот възниква, когато упражняването на правото на възражение изисква човешка намеса, позволяваща на субектите на данни да изразят гледната си точка и да оспорят решението[995]. Това може да породи затруднения при осигуряването на адекватно ниво на защита на личните данни, ако например човешка намеса не е възможна или когато алгоритмите са прекалено сложни

991 Вж. например ЕНОЗД (2015 г.), *„Посрещане на предизвикателствата на големите информационни масиви“*, Становище 7/2015, 19 ноември 2015 г.; ЕНОЗД (2016 г.), *„Съгласуваното осигуряване на спазването на основните права в ерата на големите информационни масиви“*, Становище 8/2016, 23 септември 2016 г.; Европейски парламент (2016 г.), Резолюция относно последиците за основните права, породени от големи информационни масиви: неприкосновеност на личния живот, защита на личните данни, недопускане на дискриминация, сигурност и правоприлагане, P8_TA(2017)0076, Страсбург, 14 март 2017 г.; Съвет на Европа, Консултативен комитет на Конвенция № 108, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, T-PD(2017)01, Страсбург, 23 януари 2017 г.

992 Международна конференция на комисарите по неприкосновеността на личния живот и защитата на данните (2014 г.), Резолюция относно големите информационни масиви.

993 Резолюция на Европейския парламент от 14 март 2017 г. относно последиците за основните права, породени от големи информационни масиви: неприкосновеност на личния живот, защита на личните данни, недопускане на дискриминация, сигурност и правоприлагане (2016/2225(INI).

994 Общ регламент относно защитата на данните, член 22.

995 *Пак там*, член 22, параграф 3.

и обемът на съответните данни е твърде голям, за да се предостави на лицата обосновка за определени решения и/или предварителна информация с цел получаване на тяхното съгласие. Пример за използването на ИИ и автоматизирано вземане на решения са неотдавнашните промени в исканията за ипотечен кредит или при набирането на персонал. Исканията се отхвърлят или получават отказ въз основа на факта, че кандидатите не отговарят на предварително зададени параметри или фактори.

10.1.3 Проблеми, свързани със защитата на данните

От гледна точка на защитата на данните основните проблеми са свързани, от една страна, с обема и разнообразието на обработваните лични данни, и от друга страна, със самото обработване и резултатите от него. Въвеждането на сложни алгоритми и софтуер за трансформиране на информационни масиви в ресурс за целите на вземането на решения засяга по-специално отделните лица и групи, най-вече в случаите на профилиране или класифициране, и в крайна сметка повдига много въпроси, свързани със защитата на данните[996].

Идентифициране на администраторите и обработващите лични данни и тяхната отговорност

Големите информационни масиви и изкуственият интелект повдигат редица въпроси относно идентифицирането на администраторите и обработващите лични данни, както и относно тяхната отговорност: кой е собственикът на данните, когато се събира и обработва такова голямо количество данни? Кой е администраторът, когато данните се обработват от машини и софтуер? Какви са конкретните отговорности на всяко действащо лице при обработването? И за какви цели могат да се използват големите информационни масиви?

Въпросът за отговорността в контекста на ИИ ще стане още по-сложен, когато ИИ вземе решение въз основа на обработка на данни, разработена от самия него. Общият регламент относно защитата на данните осигурява правна рамка за отговорността на администратора и на обработващия лични данни.

996 Съвет на Европа, Консултативен комитет към Конвенция № 108, Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви, 23 януари 2017 г., стр. 2.

Неправомерното обработване на лични данни поражда задължение за администратора на данни и за обработващия лични данни[997]. Изкуственият интелект и автоматизираното вземане на решения повдигат въпроси за това кой носи отговорност за нарушенията, които засягат неприкосновеността на личния живот на субекта на данните, когато сложността и обемът на обработваните данни не може да бъдат определени със сигурност. Ако ИИ и алгоритмите се считат за продукти, това поражда въпроси за разликата между личната отговорност, която е уредена в Общия регламент относно защитата на данните, и отговорността във връзка с продукт, която не е уредена в посочения регламент[998]. Това ще наложи необходимост от правила относно отговорността, за да се премахне несъответствието между личната отговорност и отговорността във връзка с продукт по отношение на роботиката и ИИ, включително например автоматизираното вземане на решения[999].

Въздействие върху принципите за защита на данните

Естеството, анализът и използването на големи информационни масиви, описани по-горе, поставят под въпрос прилагането на някои от традиционните, основни принципи на европейското право в областта на защитата на данните[1000]. Тези предизвикателства са свързани най-вече с принципите на законосъобразност, свеждане на данните до минимум, ограничение на целите и прозрачност.

Принципът на свеждане на данните до минимум изисква личните данни да бъдат адекватни, важни и ограничени до необходимото за целите, за които се обработват. Бизнес моделът на големите информационни масиви може да бъде пълна противоположност на принципа на свеждане на данните до минимум, тъй като изисква все повече данни, често за неустановени цели.

997 Общ регламент относно защитата на данните, членове 77—79 и член 82.

998 Европейски парламент, Европейските гражданскоправни норми за роботиката, Генерална дирекция „Вътрешни политики“, (октомври 2016 г.), стр. 14.

999 Реч на Роберто Виола на семинара за медиите относно Европейските гражданскоправни норми в областта на роботиката в Европейския парламент. (РЕЧ 16.2.2017 г.); Съобщение на Европейския парламент относно призива към Комисията да представи предложение за правила за гражданска отговорност в областта на роботиката и ИИ.

1000 Съвет на Европа, *Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви*, T-PD(2017)01, Страсбург, 23 януари 2017 г.

Същото важи за принципа на ограничение на целите, който изисква данните да се обработват за конкретни цели и да не може да се използват за цели, които са несъвместими с първоначалната цел на събирането, освен ако за такова обработване няма правно основание, като например, но не само, съгласие на субекта на данните (вж. раздел 4.1.1).

И накрая, големите информационни масиви поставят предизвикателство и пред принципа за точност на данните, тъй като свързаните с тях приложения обикновено събират данни от различни източници, без възможност да се проверява и/или поддържа точността на събираните данни[1001].

Специални правила и права

Запазва се основното правило, че обработването на лични данни чрез анализ на големи информационни масиви попада в обхвата на законодателството за защита на данните. В правото на ЕС и на Съвета на Европа обаче са въведени специални правила или дерогации за конкретни случаи във връзка с алгоритмичното комплексно обработване на данни.

В правото на Съвета на Европа модернизираната Конвенция № 108 предоставя нови права на субекта на данни с оглед постигането на по-ефективен контрол на неговите/нейните данни във времето на големите информационни масиви. Точно такъв е например случаят с член 9, параграф 1, букви а), в) и г) от модернизираната Конвенция относно правото на лицето да не продлежи на решение, което съществено ще го засегне, основано само на автоматична обработка на данни, без да се вземе предвид неговото/нейното мнение; правото да получи, при поискване, информация относно логиката, свързана с обработката на данни, когато резултатите от тази обработка го засягат, както и правото да възрази срещу обработката. Други разпоредби на модернизираната Конвенция № 108, най-вече относно прозрачността и допълнителните задължения, са допълващи елементи на механизма за защита, установен с модернизираната Конвениция № 108 за борба с предизвикателствата на дигиталната сфера.

В правото на ЕС, освен случаите, изброени в член 23 от ОРЗД, трябва да се осигури **прозрачност** на всички дейности по обработване на лични данни.

1001 ЕНОЗД (2016 г.), *Съгласувано прилагане на основните права в ерата на големите масиви от данни,* Становище 8/2016, 23 септември 2016 г., стр. 8.

Това е особено важно по отношение на интернет услугите и комплексното автоматизирано обработване на данни, като например използването на алгоритми за вземане на решения. Тук характеристиките на системите за обработване на данни трябва да позволяват на субектите на данните действително да разбират какво се случва с техните данни. За да се гарантира добросъвестно и прозрачно обработване, Общият регламент относно защитата на данните изисква администраторът да предоставя на субекта на данните съществена информация относно логиката, използвана при автоматизирано вземане на решения, включително профилирането[1002]. В своята Препоръка относно защитата и насърчаването на правото на свобода на изразяване на мнение и правото на неприкосновеност на личния живот, що се отнася до принципа за неутралност на мрежата, Комитетът на министрите на Съвета на Европа препоръчва доставчиците на интернет услуги „да предоставят на потребителите ясна, пълна и обществено достъпна информация по отношение на всички практики за управление на трафика, които могат да се отразят на достъпа на потребителите до съдържание, приложения или услуги, както и на разпространението на последните“[1003]. Докладите относно практиките за управление на интернет трафика, изготвяни от компетентните органи във всички държави членки, следва да се изготвят по открит и прозрачен начин и следва да се предоставят безплатно на обществеността[1004].

Администраторите на данни трябва да **предоставят** на субектите на данните — когато данните са получени от тях или когато не са получени от тях — не само конкретна информация за събраните данни и за предвиденото обработване (вж. раздел 6.1.1), но, когато е уместно, и за съществуването на процеси на автоматизирано вземане на решения, като им предоставят „съществена информация относно използваната логика“[1005], целите и евентуалните последствия от тези процеси. В Общия регламент относно защитата на данните също така се пояснява (само в случаите, когато личните данни не са получени от субекта на данните), че администраторът не е задължен да предостави тази информация на субекта на данните, когато „предоставянето на

1002 Общ регламент относно защитата на данните, член 13, параграф 2, буква е).

1003 Съвет на Европа, Комитет на министрите (2016 г.), Препоръка CM/Rec(2016)1 на Комитета на министрите до държавите членки относно защитата и насърчаването на правото на свобода на изразяване на мнение и правото на неприкосновеност на личния живот, що се отнася до принципа за неутралност на мрежата, 13 януари 2016 г., параграф 5.1.

1004 *Пак там*, параграф 5.2.

1005 Общ регламент относно защитата на данните, член 13, параграф 2, буква е) и член 14, параграф 2, буква ж).

такава информация се окаже невъзможно или изисква несъразмерно големи усилия“[1006]. Както обаче посочва Работната група по член 29 в своите *Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679,* сложността на обработването не следва сама по себе си да изключва възможността във формуляра на администратора на данни да се предоставят на субекта на данните ясни обяснения относно целите и анализа, използвани при обработването на данните[1007].

Правата на субектите на данните на **достъп до**, **коригиране** и **изтриване** на техните лични данни, както и тяхното право на **ограничаване** на обработването не включват такова изключение. Администраторът на данни може да бъде освободен от задължението да съобщава на субекта на данните за всяко извършено коригиране или изтриване на неговите лични данни (вж. раздел 6.1.4) и когато такова уведомяване „е невъзможно или изисква несъразмерно големи усилия“[1008].

Съгласно член 21 от ОРЗД субектите на данните имат също така право на **възражение** (вж. раздел 6.1.6) срещу обработването на негови лични данни, включително в случаите на анализ на големи информационни масиви. Макар и администраторите на данни да са освободени от това задължение, ако могат да докажат, че съществуват основни законни интереси, те не могат да се ползват от такова изключение при обработване за целите на директния маркетинг.

Администраторите на данни могат да ползват и специални дерогации по отношение на тези права, когато обработват лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели[1009].

Що се отнася до **профилирането и автоматизираното вземане на решения**, с ОРЗД са въведени специални правила: в член 22, параграф 1 се предвижда, че субектът на данните „има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, което поражда правни

1006 *Пак там*, член 14, параграф 5, буква б).

1007 Работна група по член 29, *Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679*, WP 251, 3 октомври 2017 г., стр. 14.

1008 Общ регламент относно защитата на данните, член 19.

1009 *Пак там*, член 89, параграфи 2 и 3.

последствия за субекта на данните“. Както се подчертава в насоките на Работната група по член 29, с този член се установява обща забрана за напълно автоматизирано вземане на решения[1010]. Администраторите на данни може да бъдат изключени от тази забрана само в три специални случая: когато решението 1) е необходимо за изпълнението на договор между субект на данни и администратор; 2) е разрешено от правото на ЕС или от национално право; или 3) се основава на изрично съгласие[1011].

Контрол от страна на лицата

Сложността и липсата на прозрачност по отношение на анализа на големи информационни масиви може да изисква преосмисляне на идеите за контрол на личните данни от страна на лицата. Това следва да стане съобразно конкретния социален и технологичен контекст, като се вземе предвид липсата на познания от страна на лицата. Ето защо за защитата на личните данни във връзка с големите информационни масиви следва да се възприеме по-обща идея за контрола върху използването на данните, съгласно която контролът от страна на лицата да се превърне в по-сложен процес на множество оценки на въздействието на рисковете, свързани с използването на данни[1012].

Доколко е добро приложението, свързано с големи информационни масиви, зависи от това доколко добре то може да предскаже желанията или поведението на изследваните лица (или потребители). Настоящите модели на прогнозиране, основаващи се на анализ на големи информационни масиви, се усъвършенстват непрекъснато. Последните промени в тази област включват не само използване на данните с цел категоризиране на личности (т.е. поведение и нагласи), но и анализиране на поведението чрез анализ на гласовите модели и скоростта на набиране на съобщенията или температурата на тялото. Цялата тази информация може да се използва в реално време, като се прави сравнение с познанията, придобити от оценките на големи информационни масиви, с цел например оценяване на кредитоспособността по време на среща с банков представител. Оценката се извършва не въз основа

1010 Работна група по член 29, *Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679*, WP 251, 3 октомври 2017 г., стр. 9.

1011 Общ регламент относно защитата на данните, член 22, параграф 2.

1012 Съвет на Европа, Консултативен комитет на Конвенция № 108, *Насоки относно защитата на лицата по отношение на обработването на лични данни в света на големи информационни масиви,* T-PD(2017)01, Страсбург, 23 януари 2017 г.

на качествата на лицето, кандидатстващо за кредит, а по-скоро въз основа на поведенческите характеристики, извлечени от анализ и оценка на големи информационни масиви, т.е. обстоятелството, че кандидатът говори със силен глас или ласкателно, неговия език на тялото или телесна температура.

Профилирането и целевата реклама може да не са непременно проблем, ако лицата са **наясно**, че са обект на персонализирани реклами. Профилирането се превръща в проблем, когато се използва за манипулиране на лицата, т.е. за търсене на определени личности или групи от хора за провеждането на политически кампании. Например към групите от гласоподаватели, които все още не са решили за кого да гласуват, може да бъдат насочени политически послания, съобразени с тяхната „личност" и нагласи. Друг проблем може да бъде използването на това профилиране за отказване на достъп на определени лица до стоки и услуги. Една предпазна мярка, която може да осигури защита срещу злоупотребата с големи информационни масиви и лична информация, е псевдонимизацията (вж. раздел 2.1.1)[1013]. Когато личните данни са наистина анонимизирани, т.е. липсва информация, която да оставя следи към субекта на данните, тези случаи попадат извън приложното поле на Общия регламент относно защитата на данните. Съгласието на субектите на данните и на лицата при обработването на големи информационни масиви също представлява предизвикателство за законодателството в областта на защитата на данните. Това включва съгласието на субектите/лицата да са предмет на персонализирани реклами и профилиране, което може да е обосновано с цел разбиране на „опита на клиентите", както и съгласието им за използването на масивите от лични данни за усъвършенстване и разработване на основани на информация аналитични инструменти. Осведомеността или липсата на осведоменост за обработването на големи информационни масиви повдига няколко въпроса по отношение на средствата, чрез които субектите на данните могат да упражняват правата си, като се има предвид, че при обработването на големи информационни масиви може да се разчита както на псевдонимизирана, така и на анонимизирана информация, като се използват алгоритми. Докато псевдонимизираните данни попадат в приложното поле на Общия регламент относно защитата на данните, регламентът не се прилага за анонимизираните данни. Контролът от страна на лицата върху обработването на техните лични данни и тяхната осведомеността по тези въпроси са от решаващо значение при анализа на големи информационни масиви: без това

1013 *Пак там,* стр. 2.

те няма да имат ясна представа кой е администраторът или обработващият лични данни и няма да могат да упражняват ефективно своите права.

10.2 Технологиите web 2.0 и 3.0: социални мрежи и интернет на предметите

Ключови въпроси

- Услугите за социални мрежи са онлайн комуникационни платформи, които дават възможност на отделните лица да се присъединят към или да създават мрежи от потребители със сходни интереси.
- Интернет на предметите означава свързването на различни предмети с интернет, както и взаимосвързаността на отделни предмети.
- Съгласието на субектите на данните е най-често използваното правно основание за законосъобразно обработване на данни от страна на администраторите на данни в социалните мрежи.
- Потребителите на социални мрежи по принцип са защитени от „изключението за обработване за напълно частни цели"; при определени обстоятелства обаче тази дерогация може да бъде отменена
- Доставчиците на социални мрежи не са защитени от „изключението за обработване за напълно частни цели".
- Правото на неприкосновеност на личния живот на етапа на проектирането и по подразбиране е от решаващо значение за гарантиране на сигурността на данните в тази област.

10.2.1 Определяне на технологиите web 2.0 и 3.0

Услуги за социални мрежи

Първоначално интернет беше замислен като мрежа за взаимно свързване на компютри и предаване на съобщения с ограничени възможности за обмен на данни, като уебсайтовете просто предлагаха възможност на лицата пасивно

да гледат тяхното съдържание[1014]. В ерата на Web 2.0 интернет се превърна във форум, в който потребителите си взаимодействат, сътрудничат и генерират данни. За този период са характерни забележителният успех и широкото използване на услугите за социални мрежи, които понастоящем са важна част от ежедневието на милиони хора.

Услугите за социални мрежи, или „социалните медии" може да бъдат най-общо определени като „онлайн комуникационни платформи, които дават възможност на отделните лица да се присъединят към или да създават мрежи от потребители със сходни интереси"[1015]. За да станат част от мрежа или да създадат нова, лицата се приканват да предоставят лични данни и да си създадат профил. Услугите за социални мрежи позволяват на потребителите да създават цифрово „съдържание", вариращо от снимки и видеоматериали до хипервръзки към вестници и лични публикации, чрез които да изразят своето мнение. Чрез тези онлайн комуникационни платформи, потребителите могат да взаимодействат и да общуват с няколко други потребители. Важно е, че повечето от популярните услуги за социални мрежи не изискват никакви такси за регистрация. Вместо да изискват от потребителите да плащат, за да се присъединят към мрежата, доставчиците на услуги за социални мрежи генерират по-голямата част от приходите си от целева реклама. Рекламодателите могат да извлекат голяма полза от личната информация, разкривана ежедневно в тези сайтове. Получаването на информация за възрастта, пола, местоположението и интересите на потребителя им дава възможност да достигнат до „правилните" хора с техните реклами.

Комитетът на министрите на Съвета на Европа прие Препоръка относно защитата на човешките права по отношение на услугите, които предоставят възможност за използване на социални мрежи[1016], която в специален раздел се занимава със защитата на данните и беше допълнена през 2018 г. от друга Препоръка относно ролята и отговорностите на интернет посредниците[1017].

1014 Европейска комисия (2016 г.), *Развитието на интернет на предметите в Европа*, SWD(2016) 110 окончателен.

1015 Работна група по член 29 (2009 г.), *Становище 5/2009 относно социалните мрежи онлайн*, WP 163, 12 юни 2009 г., стр. 4.

1016 Съвет на Европа, Комитет на министрите, Препоръка CM/Rec(2012)4 на Комитета на министрите до страните членки относно защитата на човешките права по отношение на услугите, които предоставят възможност за използване на социални мрежи, 4 април 2012 г.

1017 Съвет на Европа, Комитет на министрите, Препоръка CM/Rec(2018)2 на Комитета на министрите до страните членки относно ролята и отговорностите на интернет посредниците, 7 март 2018 г.

Пример: Нора е много щастлива, защото нейният партньор ѝ е предложил брак. Тя иска да сподели добрата новина с приятелите и семейството си и решава да напише емоционален постинг в социална мрежа, изразявайки радостта си, както и да промени статуса си на „сгодена“. През следващите дни, когато влиза в профила си, Нора вижда реклами на булчински рокли и цветарски магазини. Каква е причината за това?

При създаването на реклама във Facebook дружествата за булчински рокли и цветя са подбрали определени параметри, за да могат да достигнат до хора като Нора. Когато профилът на Нора показва, че тя е жена, сгодена, живее в Париж, близо до района, където са разположени магазините за булчински рокли и цветя, публикували рекламите, тя незабавно вижда тези реклами.

Интернет на предметите

Интернет на предметите е следващата стъпка в развитието на интернет: ерата на Web 3.0. Благодарение на интернет на предметите устройствата могат да бъдат свързани и да взаимодействат с други устройства чрез интернет. Това дава възможност на предмети и хора да бъдат свързани помежду си чрез комуникационни мрежи, да отчитат своето състояние и/или състоянието на заобикалящата среда[1018]. Интернет на предметите и свързаните устройства вече са реалност и през следващите няколко години се очаква да нараснат значително със създаването и по-нататъшното развитие на интелигентни устройства, които ще доведат до създаването на интелигентни градове, интелигентни домове и интелигентни предприятия.

Пример: Интернет на предметите може да бъде от особена полза за здравеопазването. Някои дружества вече са създали устройства, сензори и приложения, които позволяват да се следи здравето на пациента. Чрез използване на преносим алармен бутон и други безжични датчици, разположени на различни места в дома, е възможно да се следи ежедневният режим на възрастни хора, които живеят сами, и да се генерират сигнали, ако бъдат установени сериозни смущения

1018 Европейска комисия, Работен документ на службите на Комисията, *Развитието на интернет на предметите в Европа*, SWD(2016) 110, 19 април 2016 г.

в него. По-възрастните хора например използват широко сензори за долавяне на падане. Тези датчици могат да доловят падане съвсем точно и уведомяват лекаря и/или семейството на съответното лице, че то е паднало.

Пример: Барселона е един от най-известните примери за интелигентен град. От 2012 г. насам градът използва иновативни технологии с цел създаване на интелигентна система за обществен транспорт, управление на отпадъците, паркиране и улично осветление. Например за подобряване на управлението на отпадъците градът използва интелигентни контейнери. Това дава възможност да се следят нивата на отпадъците, така че да се оптимизират маршрутите за събиране. Когато контейнерите са почти пълни, те предават сигнали чрез мобилната комуникационна мрежа, които се изпращат до софтуерните приложения, използвани от дружеството за управление на отпадъците. По този начин дружеството може да планира най-добрия маршрут за събиране на отпадъците, като приоритизира и/или организира събирането само на контейнери, които действително трябва да бъдат изпразнени.

10.2.2 Балансиране на ползите и рисковете

Значителното разрастване и успехът на услугите за социални мрежи през последното десетилетие показват, че те носят **значителни ползи**. Например целевите реклами (както е описано в подчертания пример) са особено иновативен начин предприятията да достигнат до своята аудитория, като им предлагат по-специфичен пазар. Възможно е да е в интерес и на самите потребители да им бъдат представени реклами, които са съотносими в по-голяма степен и по-интересни. Нещо повече, услугите за социални мрежи и социалните медии могат да оказват положително въздействие върху обществото и върху въвеждането на промени. Те дават възможност на потребителите да общуват, да си взаимодействат, да организират групи и прояви по въпроси, които ги засягат.

Интернет на предметите се очаква също така да донесе значителни ползи за икономиката и е част от стратегията на ЕС за развитието на цифров единен пазар. Прогнозира се, че през 2020 г. броят на свързаните устройства в интернет на предметите ще се увеличи на шест милиарда в рамките на ЕС.

Това разрастване на свързаността се очаква да донесе важни икономически ползи чрез развитието на иновационни услуги и приложения, по-добро здравеопазване, по-добро разбиране на нуждите на потребителите и по-голяма ефективност.

В същото време, предвид огромния обем лична информация, генерирана от потребителите на социалните медии и впоследствие обработвана от операторите на услугата, разрастването на услугите за социални мрежи е съпътствано от **нарастваща загриженост** относно начините, по които могат да бъдат защитени неприкосновеността на личния живот и личните данни. Услугите за социални мрежи могат да застрашат правото на неприкосновеност на личния живот и правото на свобода на изразяване на мнение. Опасностите може да възникнат от: „липсата на правни и процедурни гаранции относно различните процеси, които могат да доведат до недопускане на потребители, недостатъчна защита на децата и младите хора срещу вредно съдържание или поведение, незачитане на правата на другите; отсъствие на удобни настройки по подразбиране за неприкосновеност на личния живот; непрозрачност по отношение на целите, за които се събират и обработват лични данни“[1019]. Европейското право в областта на защитата на данните се постара да отговори на предизвикателствата пред защитата на неприкосновеността на личния живот/данните, създадени от социалните медии. Такива принципи, като съгласието, защитата на неприкосновеността на личния живот/данните на етапа на проектирането и по подразбиране и правата на лицата, са от особено значение в контекста на социалните медии и услугите за социални мрежи.

В контекста на интернет на предметите големият обем лични данни, генерирани от различните взаимосвързани устройства, също поражда рискове за неприкосновеността на личния живот и защитата на данните. Въпреки че прозрачността е важен принцип на европейското право в областта на защитата на данните, поради множеството свързани устройства невинаги е ясно кой може да събира, да има достъп до и да използва данните, събрани от базираните на интернет на предметите устройства[1020]. Съгласно правото на ЕС и на Съвета на Европа обаче принципът на прозрачност създава задължение за администраторите да уведомяват на ясен и разбираем език субектите на данните за

1019 Съвет на Европа, Препоръка Rec(2012)4 до държавите членки относно защитата на човешките права по отношение на услугите, които предоставят възможност за използване на социални мрежи, 4 април 2012 г.

1020 Европейски надзорен орган по защита на данните (2017 г.), *Разбиране на интернет на предметите*.

начина, по който се използват техните данни. Рисковете, правилата, гаранциите и правата по отношение на обработването на техните лични данни трябва да бъдат изяснени на засегнатите лица. Свързаните чрез интернет на предметите устройства и множеството операции по обработване и засегнати данни също могат да бъдат предизвикателство за изискването за ясно и информирано съгласие за обработването на данни, когато това обработване се основава на съгласие. Хората често не разбират техническото функциониране на това обработване и следователно последиците от своето съгласие.

Друг важен повод за безпокойство е сигурността, като се има предвид, че свързаните устройства са особено уязвими към рисковете за сигурността. Свързаните устройства имат различни нива на сигурност. Тъй като функционират извън стандартната ИТ инфраструктура, те може да не разполагат с достатъчно мощност за обработка и капацитет за съхранение, за да имат софтуер за сигурност или да прилагат такива техники, като криптиране, псевдонимизация или анонимизация с цел защита на личните данни на потребителите.

Пример: В Германия регулаторните органи решиха да забранят детска играчка, свързана към интернет, след сериозни опасения относно въздействието на детската играчка върху зачитането на неприкосновеността на личния живот на децата. Регулаторните органи считат, че куклата Cayla, която е свързана към интернет, на практика представлява скрито устройство за шпиониране. Куклата функционира, като изпраща аудиовъпросите на играещото с нея дете към приложение на цифрово устройство, което ги превръща в текст и търси техния отговор в интернет. След това приложението изпраща отговора до куклата, която го казва на глас на детето. Чрез тази кукла разговорите на детето, както и тези на намиращите се наблизо възрастни могат да се записват и предават на приложението. Ако производителите на куклата не са приели адекватни мерки за сигурност, всеки човек е можело да я използва, за да слуша тези разговори.

10.2.3 Проблеми, свързани със защитата на данните

Съгласие

В Европа обработването на лични данни е законосъобразно само ако е позволено съгласно европейското право в областта на защитата на данните. За доставчиците на услуги за социални мрежи съгласието на субектите на данните обикновено представлява законно основание за обработването на данни. Съгласието трябва да е свободно изразено и да е конкретно, информирано и недвусмислено (вж. раздел 4.1.1)[1021]. „Свободно изразено" по същество означава, че субектите на данните трябва да имат възможност да упражняват действителен и реален избор. Съгласието е „конкретно" и „информирано", когато е разбираемо и се отнася ясно и точно до пълния обхват, цели и последствия от обработването на данни. В контекста на социалните медии може да се постави под въпрос дали съгласието е свободно изразено, конкретно и информирано за всички видове обработване, извършвано от оператора на услуги за социални мрежи и трети страни.

Пример: За да се присъединят към и да получат достъп до дадена услуга за социална мрежа, лицата често трябва да се съгласяват с различни видове обработване на техни лични данни, често без да им бъдат предоставяни необходимите спецификации или алтернативни варианти. Пример за това е необходимостта лицето да даде съгласие да получава поведенческа реклама, за да се регистрира в услуга за социална мрежа. Както Работната група по член 29 отбелязва в своето становище относно понятието за съгласие, „предвид значението, което някои социални мрежи са придобили, някои категории потребители (например подрастващите) ще се съгласят да получават поведенческа реклама, за да избегнат риска да бъдат частично изключени от социалните отношения. Потребителят следва да бъде поставен в положение да изрази свободно и конкретно съгласие да получава поведенческа реклама, независимо от неговия достъп до услуги за социални мрежи"[1022].

1021 Общ регламент относно защитата на данните, член 4 и член 7; модернизирана Конвенция № 108, член 5.

1022 Работна група по член 29 (2011 г.), *Становище 15/2011 относно понятието „съгласие"*, WP 187, 13 юли 2011 г., стр. 18.

Съгласно Общия регламент относно защитата на данните личните данни на децата под 16 години, по принцип, не може да се обработват въз основа на тяхното съгласие[1023]. Ако за обработването е необходимо съгласие, то трябва да бъде дадено от родителя или настойника на детето. На децата се полага специална защита, поради факта че те може да не познават достатъчно добре съответните рискове и последици, свързани с обработването на данни. Това е много важно в контекста на социалните медии, тъй като децата са по-уязвими към някои от евентуалните отрицателни последици от използването на тези медии, например кибер тормоз, онлайн преследване или кражба на самоличност.

Сигурност и защита на неприкосновеността на личния живот/данните на етапа на проектирането и по подразбиране

Обработването на лични данни по принцип е свързано с рискове за сигурността, като се има предвид постоянната възможност за нарушение на сигурността, което води до неволно или незаконно унищожаване или неволна загуба, промяна или неразрешен достъп до или разкриване на обработваните лични данни. Съгласно европейското право в областта на защитата на данните администраторите и обработващите данни трябва да прилагат подходящи технически и организационни мерки за предотвратяване на неразрешена намеса в операциите по обработване на данни. Доставчиците на услуги за социални мрежи, които попадат в обхвата на европейските правила в областта на защитата на данните, също трябва да спазват това задължение.

Принципите за защита на неприкосновеността на личния живот/данните на етапа на проектирането и по подразбиране изискват администраторите на данни да поддържат сигурността при проектирането на своите продукти и автоматично да прилагат подходящи настройки за защита на неприкосновеността на личния живот и данните. Това означава, че когато дадено лице реши да се присъедини към социална мрежа, доставчикът на услугата не може автоматично да направи цялата информация за новия потребител на услугата достъпна за всички свои потребители. При присъединяването към услуга настройките по подразбиране по отношение на защитата на неприкосновеността на личния живот и данните следва да бъдат такива, че информацията да е достъпна само за избраните контакти на съответното

1023 Вж. Общ регламент относно защитата на данните, член 8. Държавите членки могат да предвидят в правото си по-ниска възраст, при условие че тази по-ниска възраст не е под 13 години.

лице. Разширяването на достъпа до хора извън този списък следва да бъде възможно единствено след като потребителят е предприел действия за ръчна промяна на настройките по подразбиране по отношение на защитата на неприкосновеността на личния живот и данните. Това може да окаже въздействие и в случаите, когато въпреки въведените мерки за сигурност настъпи нарушение на сигурността на данните. В тези случаи доставчиците на услуги трябва да уведомят засегнатите потребители, ако съществува вероятност това да породи висок риск за правата и свободите на субекта на данните[1024].

Защитата на неприкосновеността на личния живот/данните на етапа на проектирането и по подразбиране е особено важна в контекста на услугите за социални мрежи, тъй като освен рисковете от неразрешен достъп, които съществуват при повечето видове обработване, споделянето на лична информация в социалните медии създава допълнителни рискове за сигурността. Те често се дължат на обстоятелството, че лицата често не разбират *кой* може да има достъп до тяхната информация и как тези хора могат да я използват. С широкото използване на социалните медии се увеличи броят на случаите на кражби на самоличност и на жертвите на такива кражби.

Пример: Кражбата на самоличност е явление, при което дадено лице получава информация, данни или документи, които принадлежат на друго лице (жертвата), и след това използва тази информация, за да се представя за жертвата и да получи стоки и услуги от името на жертвата. Да вземем например Пол, който има профил в уебсайта на една социална мрежа. Пол е учител и е активен член на своята общност, много дружелюбен и не особено загрижен за настройките по отношение на защитата на неприкосновеността на личния живот и данните на неговия профил в социалната медия. Неговият списък с контакти е голям и понякога включва хора, които той невинаги познава лично. Тъй като работи в голямо училище и е доста популярен, поради факта че тренира училищния отбор по футбол, той счита, че тези хора най-вероятно са родители или приятели на училището. В профила на Пол в социалните медии се показват неговите електронна поща и рождена дата. Освен това Пол редовно публикува снимки на своето куче Тоби, придружени от такива коментари като „Аз и Тоби по време

1024 *Пак там*, член 34.

на сутрешното ни тичане“. Пол не осъзнава, че един от най-популярните тайни въпроси за защитата на неговата електронна поща или мобилен телефон е „Как се казва вашият домашен любимец?“. Като използва наличната информация в профила на Пол в социалните медии, Ник лесно успява да пробие защитата на неговите профили.

Права на лицата

Доставчиците на услуги за социални медии трябва да зачитат правата на лицата (вж. раздел 6.1), включително правото им да бъдат информирани относно целта на обработването и как личните данни могат да се използват за целите на директния маркетинг. Лицата трябва също така да имат право на достъп до личните данни, които самите те са генерирали в платформата на социалните мрежи, и да поискат тяхното заличаване. Дори когато лицата са дали съгласието си за обработването на лични данни и са качили информация в интернет, те следва да могат да поискат да „бъдат забравени“, ако вече не желаят да получават услугите на социалната мрежа. Освен това правото на преносимост на данните дава възможност на потребителите да получат копие от личните данни, които са предоставили на доставчика на услуги за социални мрежи, в структуриран, широко използван и пригоден за машинно четене формат, както и да прехвърлят техните данни от един доставчик на услуги за социални мрежи на друг[1025].

Администратори на данни

Един труден въпрос, който често възниква в контекста на социалните медии, е въпросът кой точно е администраторът, тоест кое лице има задължението и отговорността да спазва правилата за защита на данните. Доставчиците на услуги за социални мрежи се считат за администратори по европейското право в областта на защитата на данните. Това е очевидно, като се има предвид широкото определение на „администратор“, както и фактът, че тези доставчици на услуги определят целта и средствата за обработването на личните данни, споделени от лицата. Съгласно правото на ЕС, ако предлагат услуги на субекти на данни в ЕС, администраторите трябва да спазват разпоредбите на Общия регламент относно защитата на данните, дори и да не са установени в ЕС.

1025 Общ регламент относно защитата на данните, член 21.

Може ли обаче потребителите на услуги за социални мрежи също да се считат за администратори? Когато лицата обработват лични данни „в рамките на изцяло лична дейност или дейност в рамките на домакинството“, правилата за защита на данните не се прилагат. В европейското право в областта на защитата на данните това е познато като „изключение за обработване за напълно частни цели“. В някои случаи обаче потребителят на услуга за социални мрежи може да не е обхванат от изключението за обработване за напълно частни цели.

Потребителите доброволно споделят своята лична информация онлайн. Споделената онлайн информация обаче често включва лична информация на други лица.

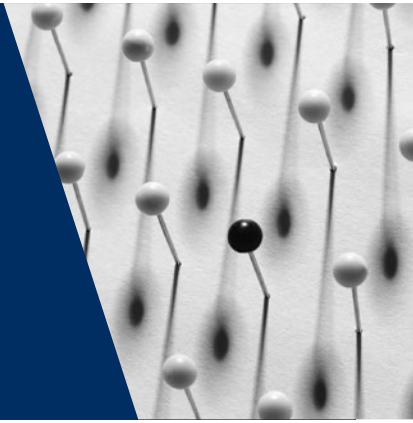
Пример: Пол има профил в много популярна платформа на социална мрежа. Пол се опитва да стане актьор и използва профила си, за да качва снимки, видеоматериали и публикации, в които обяснява своята страст към изкуството. Популярността е важна за неговото бъдеще и затова той е решил, че неговият профил следва да бъде достъпен не само за личните му контакти, но и за всички потребители на интернет, независимо дали те са членове на мрежата или не. Може ли Пол да публикува свои снимки и видеоматериали, на които присъства и неговата приятелка Сара, без нейно съгласие? Като учител в начално училище, Сара се опитва да държи своя работодател, своите ученици и техните родители настрана от своя личен живот. Да си представим случай, при който Сара, която не използва социални мрежи, разбира от техния общ приятел Ник, че има публикувана онлайн нейна снимка с Пол от едно празненство. В този случай обработването на данни от страна на Пол няма да попада в обхвата на правото на ЕС, тъй като е обхванато от „изключението за обработване за напълно частни цели“.

За потребителите обаче продължава да е от решаващо значение да знаят и да не забравят, че качването на информация за други лица без тяхното съгласие може да наруши правото на неприкосновеност на личния живот и на защита на личните данни на тези лица. Дори и да се прилага изключението за обработване за напълно частни цели — например ако даден потребител има профил, който е публичен само за избрани от него лица за контакт — публикуването на лична информация за други лица все пак може да доведе до това потребителят да носи отговорност. Въпреки че правилата за защита

на данните не се прилагат, ако се прилага изключението за обработване за напълно частни цели, отговорност може да възникне вследствие прилагането на други национални правила, например клевета или нарушаване на правата на личността. На последно място, от изключението за обработване за напълно частни цели са защитени само потребителите на услуги за социални мрежи: администраторите или обработващите лични данни, които осигуряват средствата за обработване на лични данни, попадат в обхвата на правото за защита на данните на ЕС[1026].

С реформата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации правилата за защитата на данните, неприкосновеността на личния живот и сигурността, които са приложими за доставчиците на далекосъобщителни услуги съгласно настоящата правна рамка, биха били приложими ще се прилагат и за услугите за комуникация „машина-машина" и електронни съобщителни услуги, включително например услуги „over the top".

1026 *Пак там*, съображение 18.



Допълнителна литература

Глава 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance", *International Data Privacy Law*, Vol. 6, No. 3, pp. 195–209.

EDRi, *An introduction to data protection*, Brussels.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. and Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, Vol. 26 (1), pp. 73–82.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. and Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Kokott, J. и Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, Vol. 3, No. 4, pp. 222—228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, Vol. 1, No. 1, pp. 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the „added-value" of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, Vol. 63, No. 3, pp. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?“, *Neue Juristische Wochenschrift*, No. 5, pp. 281—288.

Warren, S. и Brandeis, L. (1890), „The right to privacy“, *Harvard Law Review,* Vol. 4, No. 5, pp. 193—220.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Глава 2

Acquisty, A., and Gross R. (2009), „Predicting Social Security numbers from public data“, *Proceedings of the National Academy of Science*, 7 July 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, Vol. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, Vol. 57, No. 6, pp. 1701—1777.

Samarati, P. and Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression", Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy" *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, No. 5, pp. 557–570.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice.*

Глави 3–6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010 г.), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. и Kaye, J. (2010 г.), „Revoking consent: a „blind spot" in data protection law?", *Computer Law & Security Review*, Vol. 26, No. 3 pp. 273–283.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. and Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

De Hert, P. and Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, No. 2, pp. 130–142.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, Vol. 20, No. 2, pp. 473–506.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. and Saxby, S. (2011), „30 years on — The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, Vol. 27, No 3, pp. 223—231.

Simitis, S. (2011 г.), *Bundesdatenschutzgesetz*, Баден-Баден, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Глава 7

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Европейски надзорен орган по защита на данните (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Работна група по член 29 (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 [Работен документ за общо тълкуване на член 26, параграф 1 от Директива 95/46/ЕО от 24 октомври 1995 г.]*

Глава 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. and Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

Drewer, D. and Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, Vol. 13, No. 3, pp. 381–395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Глава 9

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, Vol. 36, No. 5, pp. 722–776.

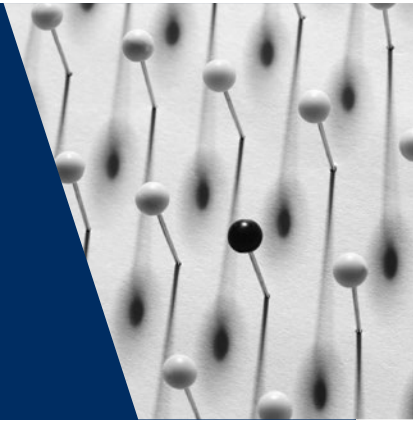
Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Глава 10

El Emam, K. and Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, Vol. 5, No. 1, pp. 73–87.

Mayer-Schönberger, V and Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, Vol. 3, No. 2, pp. 67–73.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, Vol. 3, No. 2, pp. 74–87.



Съдебна практика

Избрана съдебна практика на Европейския съд по правата на човека

Достъп до лични данни
Gaskin/Обединеното кралство, № 10454/83, 7 юли 1989 г.
Godelli/Италия, № 33783/09, 25 септември 2012 г.
K.H. и други/Словакия, № 32881/04, 28 април 2009 г.
Leander/Швеция, № 9248/81, 26 март 1987 г.
M.K./Франция, № 19522/09, 18 април 2013 г.
Odièvre/Франция [голям състав], № 42326/98, 13 февруари 2003 г.

Балансиране на защитата на данните със свободата на изразяване на мнение и правото на информация

Axel Springer AG/Германия [голям състав], № 39954/08, 7 февруари 2012 г.
Bohlen/Германия, № 53495/09, 19 февруари 2015 г.
Coudec и Hachette Filipacchi Associés/Франция [голям състав], № 40454/07, 10 ноември 2015 г.
Magyar Helsinki Bizottság/Унгария [голям състав], № 18030/11, 8 ноември 2016 г.
Müller и други/Швейцария, № 10737/84, 24 май 1988 г.
Vereinigung bildender Künstler/Австрия, № 68354/01, 25 януари 2007 г.
Von Hannover/Германия (№ 2) [голям състав], № 40660/08 и № 60641/08, 7 февруари 2012 г.

Satakunnan Markkinapörssi Oy и Satamedia Oy/Финландия [голям състав], № 931/13, 27 юни 2017 г.

Балансиране на защитата на данните със свободата на религията
Sinan Işık/Турция, № 21924/05, 2 февруари 2010 г.

Предизвикателства в областта на защитата на данните онлайн
K.U./Финландия, № 2872/02, 2 декември 2008 г.

Съгласие на субекта на данни
Elberte/Латвия, № 61243/08, 13 януари 2015 г.
Sinan Işık/Турция, № 21924/05, 2 февруари 2010 г.
Y/Турция, № 648/10, 17 февруари 2015 г.

Кореспонденция
Amann/Швейцария [голям състав], № 27798/95, 16 февруари 2000 г.
Bernh Larsen Holding AS и други/Норвегия, № 24117/08, 14 март 2013 г.
Cemalettin Canli/Турция, № 22427/04, 18 ноември 2008 г.
Dalea/Франция, № 964/07, 2 февруари 2010 г.
Gaskin/Обединеното кралство, № 10454/83, 7 юли 1989 г.
Haralambie/Румъния, № 21737/03, 27 октомври 2009 г.
Khelili/Швейцария, № 16188/07, 18 октомври 2011 г.
Leander/Швеция, № 9248/81, 26 март 1987 г.
Malone/Обединеното кралство, № 8691/79, 2 август 1984 г.
Rotaru/Румъния [голям състав], № 28341/95, 4 май 2000 г.
S. и Marper/Обединеното кралство [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г.
Shimovolos/Русия, № 30194/09, 21 юни 2011 г.
Silver и други/Обединеното кралство, № 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 март 1983 г.
The Sunday Times/Обединеното кралство, № 6538/74, 26 април 1979 г.

Асоциация за Европейска интеграция и права на човека и Екимджиев/България, № 62540/00, 28 юни 2007 г.
Д.Л/България, № 7472/14, 19 май 2016 г.

Бази данни на регистрите за съдимост
Aycaguer/Франция, № 8806/12, 22 юни 2017 г.
B.B./Франция, № 5335/06, 17 декември 2009 г.
Brunet/Франция, № 21010/10, 18 септември 2014 г.
M.K./Франция, № 19522/09, 18 април 2013 г.
M.M./Обединеното кралство, № 24029/07, 13 ноември 2012 г.

Сигурност на данните
Haralambie/Румъния, № 21737/03, 27 октомври 2009 г.
K.H. и други/Словакия, № 32881/04, 28 април 2009 г.

Бази данни с ДНК
S. и Marper/Обединеното кралство [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г.

Данни от GPS
Uzun/Германия, № 35623/05, 2 септември 2010 г.

Здравни данни
Avilkina и други/Русия, № 1585/09, 6 юни 2013 г.
Biriuk/Литва, № 23373/03, 25 ноември 2008 г.
I/Финландия, № 20511/03, 17 юли 2008 г.
L.H./Латвия, № 52019/07, 29 април 2014 г.
L.L./Франция, № 7508/02, 10 октомври 2006 г.
M.S./Швеция, № 20837/92, 27 август 1997 г.
Szuluk/Обединеното кралство, № 36936/05, 2 юни 2009 г.
Y/Турция, № 648/10, 17 февруари 2015 г.
Z/Финландия, № 22009/93, 25 февруари 1997 г.

Самоличност
Ciubotaru/Молдова, № 27138/04, 27 април 2010 г.
Godelli/Италия, № 33783/09, 25 септември 2012 г.
Odièvre/Франция [голям състав], № 42326/98, 13 февруари 2003 г.

Информация относно професионалните дейности
G.S.B./Швейцария, № 28601/11, 22 декември 2015 г.

M.N. и други/Сан Марино, № 28005/12, 7 юли 2015 г.
Michaud/Франция, № 12323/11, 6 декември 2012 г.
Niemietz/Германия, № 13710/88, 16 декември 1992 г.

Прихващане на комуникации
Amann/Швейцария [голям състав], № 27798/95, 16 февруари 2000 г.
Brito Ferrinho Bexiga Villa-Nova/Португалия, № 69436/10, 1 декември 2015 г.
Copland/Обединеното кралство, № 62617/00, 3 април 2007 г.
Halford/Обединеното кралство, № 20605/92, 25 юни 1997 г.
Iordachi и други/Молдова, № 25198/02, 10 февруари 2009 г.
Kopp/Швейцария, № 23224/94, 25 март 1998 г.
Liberty и други/Обединеното кралство, № 58243/00, 1 юли 2008 г.
Malone/Обединеното кралство, № 8691/79, 2 август 1984 г.
Mustafa Sezgin Tanrıkulu/Турция, № 27473/06, 18 юли 2017 г.
Pruteanu/Румъния, № 30181/05, 3 февруари 2015 г.
Szuluk/Обединеното кралство, № 36936/05, 2 юни 2009 г.

Задължения на лицата, които носят отговорност
B.B./Франция, № 5335/06, 17 декември 2009 г.
I/Финландия, № 20511/03, 17 юли 2008 г.
Mosley/Обединеното кралство, № 48009/08, 10 май 2011 г.

Лични данни
Amann/Швейцария [голям състав], № 27798/95, 16 февруари 2000 г.
Bernh Larsen Holding AS и други/Норвегия, № 24117/08, 14 март 2013 г.
Uzun/Германия, № 35623/05, 2 септември 2010 г.

Снимки
Sciacca/Италия, № 50774/99, 11 януари 2005 г.
Von Hannover/Германия, № 59320/00, 24 юни 2004 г.

Право „да бъдеш забравен“
Satakunnan Markkinapörssi Oy и Satamedia Oy/Финландия [голям състав], № 931/13, 27 юни 2017 г.
Segerstedt-Wiberg и други/Швеция, № 62332/00, 6 юни 2006 г.

Право на възражение
Leander/Швеция, № 9248/81, 26 март 1987 г.
M.S./Швеция, № 20837/92, 27 август 1997 г.
Mosley/Обединеното кралство, № 48009/08, 10 май 2011 г.
Rotaru/Румъния [голям състав], № 28341/95, 4 май 2000 г.
Sinan Işık/Турция, № 21924/05, 2 февруари 2010 г.

Чувствителни категории данни
Brunet/Франция, № 21010/10, 18 септември 2014 г.
I/Финландия, № 20511/03, 17 юли 2008 г.
Michaud/Франция, № 12323/11, 6 декември 2012 г.
S. и Marper/Обединеното кралство [голям състав], № 30562/04 и № 30566/04, 4 декември 2008 г.

Надзор и правоприлагане (роля на различните участници, включително на надзорните органи)

I/Финландия, № 20511/03, 17 юли 2008 г.
K.U./Финландия, № 2872/02, 2 декември 2008 г.
Von Hannover/Германия, № 59320/00, 24 юни 2004 г.
Von Hannover/Германия (№ 2) [голям състав], № 40660/08 и № 60641/08, 7 февруари 2012 г.

Методи за наблюдение
Allan/Обединеното кралство, № 48539/99, 5 ноември 2002 г.
Bărbulescu/Румъния [голям състав], № 61496/08, 5 септември 2017 г.
Dragojević/Хърватия, № 68955/11, 15 януари 2015 г.
Karabeyoğlu/Турция, № 30083/10, 7 юни 2016 г.
Klass и други/Германия, № 5029/71, 6 септември 1978 г.
Roman Zakharov/Русия [голям състав], № 47143/06, 4 декември 2015 г.
Rotaru/Румъния [голям състав], № 28341/95, 4 май 2000 г.
Szabó и Vissy/Унгария, № 37138/14, 12 януари 2016 г.
Taylor-Sabori/Обединеното кралство, № 47114/99, 22 октомври 2002 г.
Uzun/Германия, № 35623/05, 2 септември 2010 г.
Versini-Campinchi и Crasnianski/Франция, № 49176/11, 16 юни 2016 г.
Vetter/Франция, № 59842/00, 31 май 2005 г.
Vukota-Bojić/Швейцария, № 61838/10, 18 октомври 2016 г.

Асоциация за Европейска интеграция и права на човека и Екимджиев/България, № 62540/00, 28 юни 2007 г.
Д.Л/България, № 7472/14, 19 май 2016 г.

Видеонаблюдение
Köpke/Германия, № 420/07, 5 октомври 2010 г.
Peck/Обединеното кралство, № 44647/98, 28 януари 2003 г.

Гласови образци
P.G. и J.H./Обединеното кралство, № 44787/98, 25 септември 2001 г.
Wisse/Франция, № 71611/01, 20 декември 2005 г.

Избрана съдебна практика на Съда на Европейския съюз

Съдебна практика, свързана с Директивата за защита на личните данни

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 май 2017 г.

[Принцип на законосъобразно обработване: законен интерес, преследван от трета страна]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9 март 2017 г.

[Право на изтриване на личните данни; право на възражение срещу обработването]

Съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], 21 декември 2016 г.

[Поверителност на електронните съобщения; доставчици на електронни съобщителни услуги; задължение за общо и неизбирателно запазване на данни за трафика и на данни за местонахождението; липса на предварителен контрол от юрисдикция или независим административен орган; Харта на основните права на Европейския съюз; съвместимост с правото на ЕС]

C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19 октомври 2016 г.

[Понятие за лични данни; адреси по интернет протокол; съхраняване на данни от доставчик на онлайн медийни услуги; национално законодателство, което не допуска отчитане на законния интерес, преследван от администратора на лични данни]

C-362/14, *Maximillian Schrems/Data Protection Commissioner* [голям състав], 6 октомври 2015 г.

[Принцип на законосъобразно обработване; основни права; невалидност на Решението относно „сферата на неприкосновеност на личния живот"; правомощия на независимите надзорни органи]

C-230/14, *Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 октомври 2015 г.
[Правомощия на националните надзорни органи]

C-201/14, *Smaranda Bara и други/Casa Națională de Asigurări de Sănătate и други*, 1 октомври 2015 г.
[Право на лицето да бъде информирано относно обработването на лични данни]

C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 декември 2014 г.
[Понятията „обработване на данни" и „администратор"]

C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert и други*, 7 ноември 2013 г.
[Право на лицето да бъде информирано относно обработването на лични данни]

T-462/12 R, *Pilkington Group Ltd/Европейска комисия*, Определение на председателя на Общия съд от 11 март 2013 г.

C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, 30 май 2013 г.
[Понятие „лични данни"; регистър на работното време; принципи, отнасящи се до качеството на данните, и критерии за законосъобразност на обработването на данни; достъп на компетентния национален орган за контрол на условията на труд; задължение на работодателя да предостави на разположение регистъра на работното време, така че да позволи неговото незабавно консултиране]

Съединени дела C-293/12 и C-594/12 *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources и други и Kärntner Landesregierung и други* [голям състав], 8 април 2014 г.
[Нарушаване на първичното право на ЕС от Директивата за запазване на лични данни; законосъобразно обработване на лични данни; ограничение на целите и на съхраняването на данни]

C-288/12, *Европейска комисия/Унгария* [голям състав], 8 април 2014 г.
[Законност на отстраняването от длъжност на националния надзорен орган за защита на данните]

Съединени дела C-141/12 и C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel и Minister voor Immigratie, Integratie en Asiel/M u S*, 17 юли 2014 г.

[Обхват на правото на достъп на субекта на данни; защита на физическите лица при обработването на лични данни; понятие за лични данни; данни относно поискалото разрешение за пребиваване лице и правен анализ, съдържащи се в подготвителен административен документ, използван при изготвяне на решението; Харта на основните права на Европейския съюз]

C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [голям състав], 13 май 2014 г.

[Задължения на доставчиците на интернет търсачки да се въздържат, по искане на субекта на данни, от показване на лични данни в резултатите от търсенето; приложимост на Директивата за защита на личните данни, понятие за обработване на лични данни; значение на „администратори"; балансиране на защитата на данните със свободата на изразяване на мнение; правото „да бъдеш забравен"]

C-614/10, *Европейска комисия/Република Австрия* [голям състав], 16 октомври 2012 г.

[Независимост на национален надзорен орган]

Съединени дела C-468/10 и C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) u Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24 ноември 2011 г.

[Правилно прилагане на член 7, буква е) от Директивата за защита на личните данни – „законните интереси на други лица" — в националното законодателство]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16 февруари 2012 г.

[Задължение на доставчиците на платформи за социални мрежи да предотвратяват незаконосъобразното използване на музикални и аудиовизуални произведения от потребителите на мрежата]

C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 ноември 2011 г.

[Информационно общество; авторско право; интернет; софтуери „peer-to-peer"; доставчици на интернет услуги; въвеждане на система за филтриране на електронни съобщения, за да се възпрепятства обменът на файлове, който нарушава

авторските права; липса на общо задължение да се контролира пренасяната информация]

C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5 май 2011 г.
[Необходимост от подновено съгласие]

Съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke GbR u Hartmut Eifert/Land Hessen* [голям състав], 9 ноември 2010 г.
[Понятие „лични данни"; пропорционалност на правното задължение да се публикуват лични данни относно бенефициентите по определени земеделски фондове на ЕС]

C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer,* 7 май 2009 г.
[Право на достъп на субектите на данни]

C-518/07, *Европейска комисия/Федерална република Германия* [голям състав], 9 март 2010 г.
[Независимост на национален надзорен орган]

C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy u Satamedia Oy* [голям състав], 16 декември 2008 г.
[Понятие за „журналистическа дейност" по смисъла на член 9 от Директивата за защита на личните данни]

C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [голям състав], 16 декември 2008 г.
[Законност на съхранението на данни за чужденците в статистически регистър]

C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [голям състав], 29 януари 2008 г.
[Понятие „лични данни"; задължение на доставчиците на услуги за достъп до интернет да разкрият на сдружение за защита на интелектуалната собственост самоличността на потребителите на програми за споделяне на файлове KaZaA]

C-101/01, *Наказателно производство срещу Bodil Lindqvist*, 6 ноември 2003 г.
[Специални категории лични данни]

Съединени дела C-465/00, C-138/01 и C-139/01, *Rechnungshof/Österreichischer Rundfunk и други и Christa Neukomm и Jospeh Lauermann/Österreichischer Rundfunk*, 20 май 2003 г.

[Пропорционалност на правното задължение да се публикуват лични данни относно заплатите на служители в определени категории институции, свързани с публичния сектор]

C-434/16, *Peter Nowak/Data Protection Commissioner*, Заключение на генералния адвокат Kokott от 20 юли 2017 г.

[Понятие „лични данни"; достъп до собствена писмена изпитна работа; коментари на проверителя]

C-291/12, *Michael Schwarz/Stadt Bochum*, 17 октомври 2013 г.

[Преюдициално запитване; пространство на свобода, сигурност и правосъдие; биометричен паспорт; дактилоскопични отпечатъци; правно основание; пропорционалност]

Съдебна практика, свързана с Директива 2016/681

Становище 1/15 на Съда (голям състав), 26 юли 2017 г.

[Правно основание, проект на споразумение между Канада и Европейския съюз относно предаването и обработката на резервационни данни на пътниците; съвместимост на проекта на споразумение с член 16 ДФЕС, с членове 7 и 8 и член 52, параграф 1 от Хартата на основните права на Европейския съюз]

Съдебна практика, свързана с Регламента относно защитата на данните при обработването им от институции на ЕС

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Европейски орган за безопасност на храните (ЕОБХ), Европейска комисия,* 16 юли 2015 г.

[Достъп до документи]

C-28/08 P, *Европейска комисия/The Bavarian Lager Co. Ltd.* [голям състав], 29 юни 2010 г.

[Достъп до документи]

Съдебна практика, свързана с Директива 2002/58/ЕО

C-536/15, *Tele2 (Netherlands) BV и други/Autoriteit Consument en Markt (AMC)*, 15 март 2017 г.

[Принцип на недопускане на дискриминация; предоставяне на лични данни за абонатите с оглед осигуряването на общодостъпни телефонни справочни услуги и указатели; съгласие на абоната; разграничение в зависимост от държавата членка, в която се предлагат общодостъпните телефонни справочни услуги и указатели]

Съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen и Secretary of State for the Home Department/Tom Watson и други* [голям състав], 21 декември 2016 г.

[Поверителност на електронните съобщения; доставчици на електронни съобщителни услуги; задължение за общо и неизбирателно запазване на данни за трафика и на данни за местонахождението; липса на предварителен контрол от юрисдикция или независим административен орган; Харта на основните права на Европейския съюз; съвместимост с правото на ЕС]

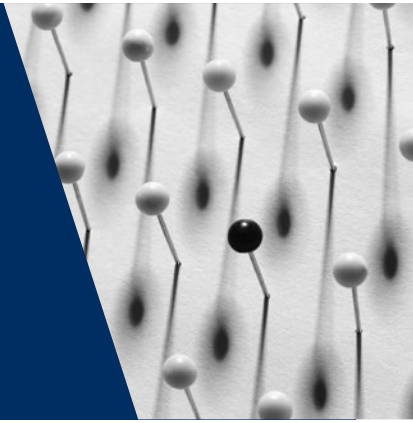
C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 ноември 2011 г.

[Информационно общество; авторско право; интернет; софтуери „peer-to-peer"; доставчици на интернет услуги; въвеждане на система за филтриране на електронни съобщения, за да се възпрепятства обменът на файлове, който нарушава авторските права; липса на общо задължение да се контролира пренасяната информация]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*, 19 април 2012 г.

[Авторско право и сродни права; обработване на данни в интернет; нарушаване на изключително право; аудиокниги, до които е предоставен достъп в интернет чрез FTP сървър на предоставен от интернет оператора IP адрес; разпореждане до интернет оператора да предостави името и адреса на ползвателя на IP адреса]

Списък на дела



Съдебна практика на Съда на Европейския съюз

Съдебна практика на Европейския съд по правата на човека

Съдебна практика на националните съдилища

Подробна информация за Агенцията на Европейския съюз за основните права (FRA) може да намерите в интернет. Тя е достъпна на интернет страницата на FRA: fra.europa.eu.

Допълнителна информация за юриспруденцията на Европейския съд по правата на човека може да се намери на уебсайта на Съда: echr.coe.int. Порталът за търсене HUDOC предоставя достъп до решенията на Съда на английски и/или френски език, както и преводи на други езици, обобщена информация по правни въпроси, съобщения за пресата и друга информация за работата на Съда (hudoc.echr.coe.int).

Как да се сдобием с публикациите на Съвета на Европа

Издателството на Съвета на Европа публикува трудове от всички сфери на дейността на организацията, включително правата на човека, правни науки, здравеопазване, етика, социално дело, околна среда, образование, култура, спорт, младеж и архитектурно наследство. Книги и електронни издания от пълния каталог можете да поръчате онлайн (http://book.coe.int).

Виртуална читалня дава възможност на потребителя да прегледа безплатно откъси от по-важните нови публикации, както и пълния текст на някои официални документи.

Информация за конвенциите на Съвета на Европа, както и пълният им текст може да се намери на интернет страницата на Отдела по договорите: http://conventions.coe.int/.

За контакт с представители на ЕС

Лично

В целия Европейския съюз съществуват стотици информационни центрове „Europe Direct". Адресът на най-близкия до Вас център ще намерите на уебсайта https://europa.eu/european-union/contact_bg.

По телефона или по електронна поща

Europe Direct е служба, която отговаря на въпроси за Европейския съюз. Можете да се свържете с тази служба:
- чрез безплатния телефонен номер 00 800 6 7 8 9 10 11 (някои оператори може да таксуват обаждането),
- или стационарен телефонен номер +32 22999696, или
- по електронна поща чрез формуляра на разположение на адрес https://europa.eu/european-union/contact_bg.

За да намерите информация за ЕС

Онлайн

Информация за Европейския съюз на всички официални езици на ЕС е на разположение на уебсайта Europa на адрес https://europa.eu/european-union/index_bg.

Публикации на ЕС

Можете да изтеглите или да поръчате безплатни и платени публикации на адрес https://publications.europa.eu/bg/publications. Редица безплатни публикации може да бъдат получени от службата Europe Direct или от Вашия местен информационен център (вж. https://europa.eu/european-union/contact_bg).

Право на ЕС и документи по темата

За достъп до правна информация от ЕС, включително цялото право на ЕС от 1952 г. насам на всички официални езици, посетете уебсайта EUR-Lex на адрес http://eur-lex.europa.eu.

Свободно достъпни данни от ЕС

Порталът на ЕС за свободно достъпни данни (http://data.europa.eu/euodp/bg) предоставя достъп до набори от данни от ЕС. Данните могат да бъдат изтеглени и използвани повторно безплатно, както за търговски, така и за нетърговски цели.

doi:10.2811/850556 TK-05-17-225-BG-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Бързото развитие на информационните технологии изостря необходимостта от стабилна защита на личните данни, правото на която е гарантирано както от актовете на Европейския съюз (ЕС), така и от тези на Съвета на Европа (СЕ). Гарантирането на това важно право поражда нови и значителни предизвикателства, тъй като технологичният напредък разширява границите на такива области, като наблюдението, прихващането на комуникациите и съхранението на данните. Настоящият наръчник е предназначен да запознае практикуващите юристи, които не са специализирани в областта на защитата на данните, с тази нововъзникваща област на правото. Той предоставя преглед на приложимите правни рамки на ЕС и на Съвета на Европа. В наръчника също така е обяснена ключова съдебна практика, като са представени обобщено най-важните решения на Съда на Европейския съюз и на Европейския съд по правата на човека. Освен това в него са представени хипотетични сценарии, които служат като практически примери за разнообразните проблеми, срещани в тази постоянно развиваща се област.

АГЕНЦИЯ НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА ОСНОВНИТЕ ПРАВА
Schwarzenbergplatz 11 — 1040 Виена — Австрия
Тел. +43 (1) 58030-0 — факс +43 (1) 58030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

ЕВРОПЕЙСКИ СЪД ПО ПРАВАТА НА ЧОВЕКА
СЪВЕТ НА ЕВРОПА
67075 Страсбург Cedex — Франция
Тел. +33 (0) 388412018 – факс +33 (0) 388412730
echr.coe.int — publishing@echr.coe.int

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ
Rue Wiertz 60 – 1047 Брюксел — Белгия
Тел. +32 22831900
www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

ISBN 978-92-871-9836-5 (CE)
ISBN 978-92-9474-293-3 (FRA)

Служба за публикации на Европейския съюз