Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

6 октомври 2020 година*

„Преюдициално запитване — Обработване на лични данни в сектора на електронните съобщения — Доставчици на електронни съобщителни услуги — Общо и неизбирателно предаване на данни за трафик и на данни за местонахождение — Защита на националната сигурност — Директива 2002/58/ЕО — Приложно поле — Член 1, параграф 3 и член 3 — Поверителност на електронните съобщения — Защита — Член 5 и член 15, параграф 1 — Харта на основните права на Европейския съюз — Членове 7, 8 и 11 и член 52, параграф 1 — Член 4, параграф 2 ДЕС“

По дело C-623/17,

с предмет преюдициално запитване, отправено на основание член 267 ДФЕС от Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство) с акт от 18 октомври 2017 г., постъпил в Съда на 31 октомври 2017 г., в рамките на производство по дело

Privacy International

срещу

Secretary of State for Foreign and Commonwealth Affairs,

Secretary of State for the Home Department,

Government Communications Headquarters,

Security Service,

Secret Intelligence Service,

СЪДЪТ (голям състав),

състоящ се от: K. Lenaerts, председател, R. Silva de Lapuerta, заместник-председател, J.-C. Bonichot, Ал. Арабаджиев, A. Prechal, M. Safjan, P. G. Xuereb и L. S. Rossi, председатели на състави, J. Malenovský, L. Bay Larsen, T. von Danwitz (докладчик), C. Toader, K. Jürimäe, C. Lycourgos и N. Piçarra, съдии,

генерален адвокат: M. Campos Sánchez-Bordona,

секретар: C. Strömholm, администратор,

* Език на производството: английски.

предвид изложеното в писмената фаза на производството и в съдебното заседание от 9 и 10 септември 2019 година,

като има предвид становищата, представени:

– за Privacy International, от B. Jaffey и T. de la Mare, QC, от D. Cashman, solicitor и от H. Roy, адвокат,

– за правителството на Обединеното кралство, от Z. Lavery, D. Guðmundsdóttir и S. Brandon, в качеството на представители, подпомагани от G. Facenna, D. Beard, QC, C. Knight и R. Palmer, barristers,

– за белгийското правителство, от P. Cottin и J.-C. Halleux, в качеството на представители, подпомагани от J. Vanpraet, advocaat, и E. de Lophem, адвокат,

– за чешкото правителство, от M. Smolek, J. Vláčil и O. Serdula, в качеството на представители,

– за германското правителство, първоначално от M. Hellmann, R. Kanitz, D. Klebs и T. Henze, а впоследствие от J. Möller, M. Hellmann, R. Kanitz и D. Klebs, в качеството на представители,

– за естонското правителство, от A. Kalbus, в качеството на представител,

– за ирландското правителство, от M. Browne, G. Hodge и A. Joyce, в качеството на представители, подпомагани от D. Fennelly, barrister,

– за испанското правителство, първоначално от L. Aguilera Ruiz и M. J. García-Valdecasas Dorrego, а впоследствие от L. Aguilera Ruiz, в качеството на представители,

– за френското правителство, първоначално от E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas и D. Dubois, а впоследствие от E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune и D. Dubois, в качеството на представители,

– за кипърското правителство, от E. Symeonidou и E. Neofytou, в качеството на представители,

– за литовското правителство, първоначално от V. Soņeca и I. Kucina, впоследствие от V. Soņeca, в качеството на представители,

– за унгарското правителство, първоначално от G. Koós, M. Z. Fehér, G. Tornyai и Z. Wagner, впоследствие от G. Koós и M. Z. Fehér, в качеството на представители,

– за нидерландското правителство, от C. S. Schillemans и M. K. Bulterman, в качеството на представители,

– за полското правителство, от B. Majczyna, J. Sawicka и M. Pawlicka, в качеството на представители,

– за португалското правителство, от L. Inez Fernandes, M. Figueiredo и F. Aragão Homem, в качеството на представители,

– за шведското правителство, първоначално от A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren и A. Alriksson, впоследствие от H. Shev, C. Meyer-Seitz, L. Zettergren и A. Alriksson, в качеството на представители,

– за норвежкото правителство, от T. B. Leming, M. Emberland и J. Vangsnes, в качеството на представители,

– за Европейската комисия, първоначално от H. Kranenborg, M. Wasmeier, D. Nardi и P. Costa de Oliveira, впоследствие от H. Kranenborg, M. Wasmeier и D. Nardi, в качеството на представители,

– за Европейския надзорен орган по защита на данните, от T. Zerdick и A. Buchta, в качеството на представители,

след като изслуша заключението на генералния адвокат, представено в съдебното заседание от 15 януари 2020 г.,

постанови настоящото

Решение

1 Преюдициалното запитване се отнася до тълкуването на член 1, параграф 3 и на член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63 и поправка в ОВ L 145, 8.6.2017 г., стр. 27), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (ОВ L 337, 2009 г., стр. 11 и поправка в ОВ L 241, 10.9.2013 г., стр. 9) (наричана по-нататък „Директива 2002/58“), във връзка с член 4, параграф 2 ДЕС и членове 7 и 8 и член 52, параграф 1 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“).

2 Запитването е отправено в рамките на спор между Privacy International, от една страна, и Secretary of State for Foreign and Commonwealth Affairs (министър на външните работи и на Общността на нациите, Обединено кралство), Secretary of State for the Home Departement (министър на вътрешните работи, Обединено кралство), Government Communications Headquarters (Централа за правителствените комуникации, Обединено кралство, наричана по-нататък „GCHQ“), Security Service (Служба за сигурност, Обединено кралство, наричана по-нататък „MI5“) и Secret Intelligence Service (Служба за тайно разузнаване, Обединено кралство, наричана по-нататък „MI6“), от друга страна, с предмет законосъобразността на правна уредба, позволяваща получаването и използването от службите за сигурност и разузнаване на масиви от данни за съобщения *(bulk communications data)*.

Правна уредба

Правото на Съюза

Директива 95/46

3 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10) е отменена, считано от 25 май 2018 г., с Регламент 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на

лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (ОВ L 119, 2016 г., стр. 1 и поправка в ОВ L 127, 23.5.2018 г., стр. 2). Член 3 от посочената директива, озаглавен „Приложно поле“, е имал следното съдържание:

„1. Настоящата директива се прилага към пълната или частична обработка на лични данни с автоматизирани средства, както и към обработката със средства, които не са автоматизирани, на лични данни, съставляващи част от файлова система, или които са предназначени да съставляват част от файлова система.

2. Настоящата директива не се прилага за обработването на лични данни:

– при извършване на дейности, извън приложното поле на правото на Общността, например дейностите, предвидени в дял V и дял VI от [ДЕС], и във всички случаи при дейности по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност (включително икономическото благосъстояние на държавата, когато процесът на обработка е свързан[…] с държавната сигурност) и при дейности на държавата в областта на наказателното право,

– когато се извършва от физическо лице в хода на предимно лични или домашни занимания“.

Директива 2002/58

4 Съображения 2, 6, 7, 11, 22, 26 и 30 от Директива 2002/58 гласят:

„(2) Настоящата директива се стреми да зачита основните права и да спазва признатите принципи, по-специално от [Хартата]. По-специално настоящата директива се стреми да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от [нея].

[…]

(6) Интернет преобръща традиционните пазарни структури, като осигурява обща глобална инфраструктура за доставка на широк обхват от електронни комуникационни услуги. Публично достъпните електронни комуникационни услуги чрез Интернет разкриват нови възможности за потребителите, но също нови рискове за техните лични данни и неприкосновеност на личния им живот.

(7) В случая на публични комуникационни мрежи, трябва да се изготвят специфични законови, подзаконови и технически разпоредби, за да се защитят основните права и свободи на физическите лица и легитимните интереси на юридическите лица, по-специално по отношение на увеличаващата се способност за автоматизирано съхранение и обработка на данни за абонати и потребители.

[…]

(11) Както Директива [95/46], настоящата директива не се отнася до въпросите за защита на основните права и свободи свързани с дейности, които не се управляват от законодателството на [Съюза]. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 15, параграф 1 от настоящата директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право. Следователно, настоящата директива не засяга възможността на

държавите членки да провеждат законно прихващане на електронни комуникации или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с Европейската конвенция за защита на човешките права и основните свободи [подписана в Рим на 4 ноември 1950 г.], съгласно тълкуването на решенията на Европейския съд за човешките права. Такива мерки трябва да бъдат уместни, строго пропорционални на предвидената цел и необходими в едно демократично общество, и следва да бъдат предмет на съответна защита в съответствие с Европейската конвенция за защита на човешките права и основните свободи.

[…]

(22) Забраната да се съхраняват съобщения и свързаните данни за трафик от лица, различни от потребителите, или без тяхното съгласие, не е насочено да забрани автоматично, междинно и временно съхранение на тази информация, доколкото това се прави с единствената цел осъществяване на предаване в електронни комуникационни мрежи и при условие че тази информация не се съхранява за период, по-дълъг от необходимия за предаване и за целите на ръководене на трафика, и че през периода на съхранение, конфиденциалният характер остава гарантиран. Когато това е необходимо за осъществяване на по-ефикасно продължаване на предаването на всякаква публично достъпна информация до други получатели на услугата по тяхно искане, настоящата директива не трябва да пречи такава информация да бъде допълнително съхранена, при условие че тази информация ще бъде при всички случаи без ограничение достъпна за обществото и че всякакви данни относно индивидуалните абонати или потребителите, поискали такава информация, ще бъдат изтрити.

[…]

(26) Данните отнасящи се до абонатите, обработвани в електронно комуникационни мрежи за осъществяване на връзки и предаване на информация, съдържат информация за личния живот на физически лица и засягат правото да се зачита тяхната кореспонденция или засягат легитимни интереси на юридически лица. Такива данни могат да бъдат съхранени само до степен, която е необходима за осигуряване на услугата с цел изготвяне на сметка и за плащания при взаимна връзка и за ограничено време. Всякаква по-нататъшна обработка на такива данни […] може да бъде позволена, само ако абонатът е дал съгласието си за това, на базата на точна и пълна информация, дадена от доставчика на публично достъпни електронни комуникационни услуги, за типа на по-нататъшната обработка, предвидена да се извърши и за правото на абоната да не даде или да оттегли неговото/нейното съгласие за такава обработка. Данни за трафика, използвани за търговия на комуникационни услуги […], трябва също да бъдат изтрити или да се направят анонимни […].

[…]

(30) Системите за обезпечаване на електронни комуникационни мрежи и услуги трябва да бъдат направени, така че да ограничават количеството на необходимите лични данни до точен минимум. […]“.

5 Член 1 от Директива 2002/58, озаглавен „Обхват и цел“, гласи:

„1. Настоящата директива предвижда да се хармонизират националните разпоредби, необходими за осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по

отношение на обработката на лични данни в електронно съобщителния сектор[,] и да се осигури свободно движение на такива данни и оборудване за електронни съобщения и услуги в [Европейския съюз].

2. Разпоредбите на настоящата директива конкретизират и допълват Директива [95/46] за целите, упоменати в параграф 1. Освен това те се грижат за защита на легитимните интереси на абонати, които са юридически лица.

3. Настоящата директива не се прилага за дейности, които попадат извън обхвата на Договора за създаване на Европейската общност, като тези обхванати от дялове V и VI от [ДФЕС], и във всички случаи за дейности, отнасящи се до обществената сигурност, отбраната, сигурността на държавата (включително икономическото благосъстояние на държавата, когато дейностите се отнасят до проблемите за сигурността на държавата) и дейностите на държавата в областта на наказателното право“.

6 Съгласно член 2 от тази директива, озаглавен „Дефиниции“:

„Освен ако не е предвидено друго, се прилагат дефинициите от Директива 95/46/ЕО и от Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно обща регулаторна структура за електронни комуникационни мрежи и услуги (Рамкова директива) [ОВ L 108, 2002 г., стр. 33; Специално издание на български език, 2007 г., глава 13, том 35, стр. 195)].

Прилагат се също следните дефиниции:

а) „потребител“ означава всяко физическо лице, използващо публично достъпни електронни комуникационни услуги за частни или бизнес цели, без да е необходимо да се е абонирал за тази услуга;

б) „данни за трафик“ означава всякакви данни, обработени с цел пренасяне на комуникация през електронни комуникационни мрежи или за изготвяне на сметка за това;

в) „данни за местонахождение“ означава всякакви данни, обработени в електронна съобщителна мрежа или чрез електронна съобщителна услуга, показващи географското местоположение на крайното оборудване на ползвателя на обществено достъпни електронни съобщителни услуги;

г) „комуникация“ означава всяка информация, обменена или пренесена между определен брой страни с помощта на публично достъпни електронни комуникационни услуги. Това не включва информация, пренасяна като част от услуга за публично радио-разпръскване през електронни комуникационни мрежи с изключение на информацията, която може да бъде свързана с идентифицируем абонат или потребител, получаващ информацията;

[…]“.

7 Член 3 от посочената директива, озаглавен „Обхванати услуги“, предвижда:

„Настоящата директива се прилага при обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в [Съюза], включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация“.

8 Съгласно член 5 от Директива 2002/58, озаглавен „Конфиденциалност на комуникациите“:

„1. Държавите членки гарантират конфиденциалност на съобщенията и свързани[те с тях данни за трафика] през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, чрез националното си законодателство. По-специално те забраняват слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители[,] без съгласието на заинтересованите потребители, с изключение на законно упълномощени да извършват това в съответствие с член 15[,] параграф 1. Настоящият параграф не пречи на техническото съхранение, което е необходимо за пренасяне на комуникация, без да противоречи на принципа за конфиденциалност.

[…]

3 Държавите членки гарантират, че съхраняването на информация или получаването на достъп до информация, вече съхранявана в крайното оборудване на абоната или ползвателя, е позволено само при условие че съответният абонат или ползвател е дал своето съгласие след получаване на предоставена ясна и изчерпателна информация в съответствие с Директива [95/46], inter alia, относно целите на обработката. Това не пречи на всякакво техническо съхранение или достъп с единствена цел осъществяване на предаването на съобщение по електронна съобщителна мрежа или доколкото е строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя“.

9 Член 6 от Директива 2002/58, озаглавен „Данни за трафик“, гласи:

„1. Данни за трафик, отнасящи се до абонати и потребители, обработени и съхранени от доставчика на публични комуникационни мрежи или публично достъпни електронни комуникационни услуги, трябва да бъдат изтрити или да се направят анонимни, когато не са необходими повече за целите на предаване на комуникация, без да се накърнява[т] параграф[и] 2, 3 и 5 от настоящия член и член 15, параграф 1.

2. Могат да бъдат обработени данни за трафик, необходими за целите на изготвяне на сметката на абоната и плащания при взаимна връзка. Такава обработка е допустима само до края на периода, през който сметката може законно да бъде оспорена или плащането търсено.

3. С цел маркетинг на електронни съобщителни услуги или за предоставянето на услуги с добавена стойност, доставчикът на обществено достъпна електронна съобщителна услуга може да обработва данните, упоменати в параграф 1, до степен и продължителност, необходими за такива услуги или маркетинг, ако абонатът или ползвателят, за когото се отнасят данните, е дал предварително съгласието си. На ползватели или абонати трябва да бъде дадена възможността да оттеглят по всяко време съгласието си за обработка на данни за трафика.

[…]

5. Обработка на данни за трафик, в съответствие с параграфи 1, 2, 3 и 4, трябва да бъде ограничена до лица, действащи под ръководството на доставчиците на публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, които отговарят за изготвянето на сметки или управлението на трафика, за запитванията на клиенти, за разкриването на измами, за търговията с електронни комуникационни услуги или за обезпечаването на услуга с добавена стойност и трябва да бъде ограничена до това, което е необходимо за целите на тези дейности“.

10 Член 9 от тази директива, озаглавен „Данни за местонахождение, различни от данни за трафик“, предвижда в параграф 1:

„Когато данни за местонахождение, различни от данни за трафик, отнасящи се до потребители или абонати на публични комуникационни мрежи или публично достъпни електронни комуникационни услуги, могат да бъдат обработени, такива данни могат да бъдат обработени, само когато се направят анонимни или със съгласието на потребители или абонати до степен и продължителност необходими за предоставяне на услуга с добавена стойност. Доставчикът на услуга трябва да информира потребители или абонати, преди да получи тяхното съгласие, за типа на данни за местонахождение, различни от данни за трафик, които ще бъдат обработени, за целите и за продължителността на обработката и дали данните ще бъдат предадени на трета страна с цел предоставяне на услуга с добавена стойност. […]“.

11 Член 15 от посочената директива, озаглавен „Приложение на някои разпоредби от Директива [95/46]“, предвижда в параграф 1:

„Държавите членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5, член 6, член 8, параграф[и] 1, 2, 3, и 4 и член 9 от настоящата директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на [престъпления] или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива [95/46]. В тази връзка, държавите членки могат, inter alia, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф. Всички мерки, упоменати в настоящия параграф, трябва да бъдат в съответствие с общите принципи на законодателството на [Съюза], включително онези, упоменати в член 6, параграф[и] 1 и 2 от Договора за Европейския съюз“.

Регламент 2016/679

12 Член 2 от Регламент 2016/679 предвижда:

„1. Настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

2. Настоящият регламент не се прилага за обработването на лични данни:

а) в хода на дейности, които са извън приложното поле на правото на Съюза;

б) от държавите членки, когато извършват дейности, които попадат в приложното поле на дял V, глава 2 от ДЕС;

[…]

г) от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност.

[…]“.

13 Член 4 от този регламент предвижда:

„За целите на настоящия регламент:

[…]

2) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

[…]“.

14 Съгласно член 23, параграф 1 от същия регламент:

„В правото на Съюза или правото на държава членка, което се прилага спрямо администратора или обработващия лични данни, чрез законодателна мярка може да се ограничи обхватът на задълженията и правата, предвидени в членове 12—22 и в член 34, както и в член 5, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 12—22, когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира:

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

г) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;

д) други важни цели от широк обществен интерес за Съюза или за държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;

е) защитата на независимостта на съдебната власт и съдебните производства;

ж) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

з) функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите, посочени в букви а)—д) и ж);

и) защитата на субекта на данните или на правата и свободите на други лица;

й) изпълнението по гражданскоправни искове“.

15 Съгласно 94, параграф 2, от Регламент 2016/679:

„Позоваванията на отменената директива се тълкуват като позовавания на настоящия регламент. Позоваванията на Работната група за защита на лицата при обработването на лични данни, създадена по силата на член 29 от Директива [95/46], се тълкуват като позовавания на Европейския комитет по защита на личните данни, създаден с настоящия регламент“.

Право на Обединеното кралство

16 Член 94 от Telecommunications Act 1984 [Закон за далекосъобщенията от 1984 г.] в редакцията му, приложима към фактите по главното производство (наричан по-нататък „Законът от 1984 г.“), озаглавен „Указания в интерес на националната сигурност и др.“, гласи:

„(1) Министърът може да даде на лице, за което се прилага настоящият член, след консултация с това лице, общи указания, ако прецени, че това е необходимо в интерес на националната сигурност или на отношенията с правителството на страна или територия извън Обединеното кралство.

(2) Министърът може да даде указания на лице, за което се прилага настоящият член, след консултация с това лице (в зависимост от обстоятелствата по случая) да извърши или да не извършва конкретно действие, посочено в указанията, ако прецени, че това е необходимо в интерес на националната сигурност или на отношенията с правителството на страна или територия извън Обединеното кралство.

(2A) Министърът може да даде указания по параграф 1 или 2 само ако прецени, че изискваното съгласно указанията действие е пропорционално на целта, която трябва да се постигне чрез него.

(3) Лицето, за което се прилага настоящият член, трябва да изпълни всички указания, дадени му от министъра съгласно настоящия член, независимо от всяко друго задължение, което му е наложено съгласно част 1 или част 2, глава 1 от Communications Act 2003 [Закон за съобщенията от 2003 г.], а доставчикът на обществена електронна съобщителна мрежа трябва да изпълни дадените му указания дори ако те се прилагат спрямо него поради качество, различно от това на доставчик на достъп до такава мрежа.

(4) Министърът изпраща на всяка от камарите на Парламента копие от всички указания, дадени въз основа на настоящия член, освен ако прецени, че оповестяването на тези указания е в противоречие с интересите на националната сигурност или с отношенията с правителството на страна или територия извън Обединеното кралство или на търговските интереси на друго лице.

(5) Никой не трябва да разкрива или не може да бъде задължен по силата на закон или по друга причина да разкрива каквато и да било информация относно предприетите съгласно настоящия член мерки, ако министърът го е уведомил, че по негова преценка оповестяването на тази информация е в противоречие с интересите на националната сигурност или с отношенията с правителството на страна или територия извън Обединеното кралство или с търговските интереси на друго лице.

[…]

(8) Настоящият член се прилага за [Office of communications (OFCOM)] и доставчиците на обществени електронни съобщителни мрежи“.

17 Член 21, параграфи 4 и 6 от Regulation of Investigatory Powers Act 2000 (Закон от 2000 г. за уреждане на правомощията по разследване, наричан по-нататък „RIPA“) гласи:

„(4) [„Д]анни за съобщения“ има едно от следните значения:

(a) всякакви данни за трафик, съдържащи се във или приложени към съобщение (от подателя или по друг начин) за целите на всякаква пощенска услуга или далекосъобщителна система, чрез която те се предават или могат да бъдат предадени;

(b) всякаква информация, която не включва никаква част от съдържанието на съобщението (освен информацията по буква а) и се отнася до използването от което и да е лице на:
(i) всякаква пощенска или далекосъобщителна услуга; или
(ii) всякаква част от далекосъобщителна система във връзка с предоставянето или използването от което и да е лице на всякаква далекосъобщителна услуга;

(c) всякаква информация извън тази по букви а) или b), която лице, предоставящо пощенска или далекосъобщителна услуга, притежава или получава във връзка с лицата, на които предоставя услугата.

[…]

(6) [„Д]анни за трафик“ (във връзка с всяко съобщение) означава:

(a) всякакви данни, които идентифицират или могат да идентифицират всяко лице, оборудване или местонахождение, до което или от което се предава или може да се предаде съобщение;

(b) всякакви данни, които идентифицират или определят, или които могат да идентифицират или определят оборудването, чрез което се предава или може да се предаде съобщението;

(c) всякакви данни, включващи сигнали за задействане на оборудването, използвано в далекосъобщителната система за целите на предаването на всякакви съобщения; и

(d) всякакви данни, които идентифицират данните, съдържащи се във или приложени към конкретно съобщение, или други данни като данни, съдържащи се във или приложени към конкретно съобщение.

[…]“.

18 Членове 65—69 от RIPA установяват правила, свързани с функционирането и правомощията на Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство). Съгласно член 65 от посочения закон този съд може да бъде сезиран, ако има причини да се смята, че определени данни са получени неправомерно.

Спорът в главното производство и преюдициалните въпроси

19 В началото на 2015 г. съществуването на практики за събиране и използване на масиви от данни за съобщения от различните служби за сигурност и разузнавателни служби на Обединеното кралство, а именно GCHQ, MI5 и MI6, е оповестено публично, по-специално в доклад на Intelligence and Security Committee of Parliament (Комисия по въпросите на разузнаването и сигурността към Парламента, Обединено кралство). На 5 юни 2015 г. Privacy International, неправителствена организация, сезира Investigatory Powers Tribunal (Съд за контрол върху

правомощията по разследване, Обединено кралство) с жалба срещу министъра на външните работи и на Общността на нациите, министъра на вътрешните работи и срещу тези служби за сигурност и разузнавателни служби, като оспорва законосъобразността на тези практики.

20 Запитващата юрисдикция разглежда законосъобразността на посочените практики с оглед най-напред на вътрешното право и разпоредбите на Европейската конвенция за защита на правата на човека и основните свободи, подписана в Рим на 4 ноември 1950 г. (наричана по-нататък „ЕКПЧ“), а след това и на правото на Съюза. В решение от 17 октомври 2016 г. тази юрисдикция установява, че ответниците в главното производство са признали, че посочените служби за сигурност и разузнавателни служби събират и използват в рамките на своята дейност масиви от данни, отнасящи се до частноправни субекти и попадащи в различни категории (*bulk personal data*), като биографични данни или данни, свързани с пътувания, сведения от финансово или търговско естество, данни, свързани със съобщения, които могат да съдържат чувствителни данни, попадащи в обхвата на професионалната тайна, или пък на поверителността на журналистическите източници. Тези данни, получени по различни — според случая, секретни — способи, били анализирани чрез съпоставяне и чрез автоматизирани средства и можели да бъдат разкрити на други лица и органи и споделени с чуждестранни партньори. В този контекст службите за сигурност и разузнавателните служби използвали също така масиви от данни за съобщения, събирани от доставчиците на обществени електронни съобщителни мрежи по силата, по-специално, на указания на министър, приети на основание член 94 от Закона от 1984 г. По този начин GCHQ и MI5 действали съответно от 2001 г. и от 2005 г.

21 Посочената юрисдикция приема, че тези мерки за събиране и използване на данни са в съответствие с националното право, а от 2015 г. — при все още неразгледани въпроси, които се отнасят до пропорционалността на посочените мерки и до предаването на данни на трети лица — с член 8 от ЕКПЧ. Във връзка с последното тя уточнява, че са ѝ били представени доказателства относно приложимите гаранции, по-специално що се отнася до процедурите за достъп и разкриване извън службите за сигурност и разузнавателните служби, условията и реда за запазване на данните и наличието на независим контрол.

22 Що се отнася до законосъобразността от гледна точка на правото на Съюза на разглежданите в главното производство мерки за събиране и използване, в решение от 8 септември 2017 г. запитващата юрисдикция извършва проверка дали тези мерки попадат в приложното поле на това право и ако това е така, дали са съвместими с него. Що се отнася до масивите от данни за съобщения, тази юрисдикция констатира, че доставчиците на електронни съобщителни мрежи са длъжни на основание член 94 от Закона от 1984 г., ако са налице указания в този смисъл от министър, да предоставят на службите за сигурност и разузнавателните служби събраните данни във връзка с икономическата им дейност, попадаща в обхвата на правото на Съюза. Случаят обаче не е такъв, що се отнася до събирането на други данни, получени от тези служби, без да се прибягва до такива обвързващи правомощия. Въз основа на тази констатация посочената юрисдикция счита за необходимо да отправи запитване до Съда, за да определи дали режим като този по член 94 попада в обхвата на правото на Съюза, и ако това е така, дали и по какъв начин изискванията, съдържащи се в съдебната практика, установена с решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, наричано по-нататък „решение Tele2“, EU:C:2016:970), се прилагат към този режим.

23 В това отношение в акта си за преюдициално запитване запитващата юрисдикция посочва, че съгласно въпросния член 94 министърът може да дава на доставчиците на електронни съобщителни услуги общи или конкретни указания, ако прецени, че това е необходимо в интерес на националната сигурност или на отношенията с чуждестранно правителство. Препращайки към определенията, съдържащи се в член 21, параграфи 4 и 6 от RIPA, тази юрисдикция уточнява, че разглежданите данни включват данни за трафик, както и информация за използваните услуги по смисъла на същата разпоредба, като е изключено само съдържанието

на съобщенията. Тези данни и информация се отнасят до това „кой, къде, кога и как“ осъществява комуникация. Посочените данни били предавани на службите за сигурност и разузнавателните служби и съхранявани от тях за целите на дейността им.

24 Според посочената юрисдикция разглежданият в главното производство режим се различава от произтичащия от Data Retention and Investigatory Powers Act 2014 (Закон за запазването на данните и правомощията по разследване от 2014 г.), предмет на делото, по което е постановено решение от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970), тъй като последният режим предвиждал запазването на данни от доставчиците на електронни съобщителни услуги и предоставянето им на разположение не само на службите за сигурност и разузнавателните служби в интерес на националната сигурност, но и на други публични органи, които имат необходимост от такива данни. Освен това посоченото решение се отнасяло до наказателно разследване, а не до националната сигурност.

25 Запитващата юрисдикция добавя, че базите данни, които се създават от службите за сигурност и разузнавателните служби, са предмет на масова обща автоматизирана обработка за разкриване на наличието на евентуални неизвестни заплахи. В това отношение тази юрисдикция посочва, че така образуваните масиви от метаданни трябвало да бъдат възможно най-пълни, с цел да се разполага с „купа сено“, в която да се намери „иглата“, която се крие в нея. Що се отнася до полезността на събирането на масиви от данни от посочените служби и техниките за извличане на информация от тези данни, посочената юрисдикция се позовава по-специално на заключенията в доклада, изготвен на 19 август 2016 г. от г-н David Anderson, QC, тогава United Kingdom Independent Reviewer of Terrorism Legislation (независим контрольор на Обединеното кралство относно законодателството в областта на тероризма), който при изготвянето на посочения доклад се е основал на проверка, извършена от екип от специалисти в областта на разузнаването, и на свидетелските показания на агенти от службите за сигурност и разузнавателните служби.

26 Запитващата юрисдикция уточнява също, че според Privacy International разглежданият в главното производство режим е незаконосъобразен от гледна точка на правото на Съюза, докато ответниците в главното производство считат, че предвиденото в този режим задължение за предаване на данни, достъпът до тези данни и тяхното използване не са от компетентността на Съюза в съответствие по-специално с член 4, параграф 2 ДЕС, съгласно който националната сигурност остава единствено в рамките на отговорността на всяка държава членка.

27 В това отношение въз основа на решение от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346, т. 56—59), което се отнася до предаването на PNR (*Passenger Name Record*) данни с цел защита на обществената сигурност, запитващата юрисдикция счита, че дейностите на търговските дружества, свързани с обработката и предаването на данни с цел защита на националната сигурност, изглежда, не попадат в приложното поле на правото на Съюза. Следвало да се провери не дали разглежданата дейност представлява обработване на данни, а само дали по своята същност и последици целта на такава дейност е да се подпомага съществена функция на държавата по смисъла на член 4, параграф 2 ДЕС посредством рамка, установена от публичните органи в областта на обществената сигурност.

28 В случай че разглежданите в главното производство мерки все пак попадат в приложното поле на правото на Съюза, запитващата юрисдикция счита, че изискванията, съдържащи се в точки 119—125 от решение от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970), изглеждат неподходящи в контекста на националната сигурност и биха могли поради естеството си да възпрепятстват способността на службите за сигурност и разузнавателните служби да овладеят определени заплахи за националната сигурност.

29 При тези обстоятелства Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство) решава да спре производството и да отправи до Съда следните преюдициални въпроси:

„В случай че:

а) възможностите на [службите за сигурност и разузнавателните служби] да използват предоставени им [масиви от данни за съобщения] са от съществено значение за защитата на националната сигурност на Обединеното кралство, включително в областта на борбата с тероризма, шпионажа и разпространението на ядрени оръжия;

б) [службите за сигурност и разузнавателните служби] използват [масивите от данни за съобщения] основно за разкриването на неизвестни до момента заплахи за националната сигурност чрез техники за нецелево събиране, разчитащи на натрупването на [масивите от данни за съобщения] на едно място. Главната полза от това е бързото идентифициране и разработка на обекта, както и осигуряването на основа за действие при наличието на непосредствена заплаха;

в) впоследствие (след изтичане на срока съгласно обичайните си търговски изисквания) доставчикът на електронна съобщителна мрежа не е длъжен да пази [масивите от данни за съобщения], които се запазват от самата държава ([службите за сигурност и разузнавателните служби]);

г) националната юрисдикция е приела (отчитайки някои резерви), че гаранциите, свързани с използването на [масивите от данни за съобщения] от [службите за сигурност и разузнавателните служби], съответстват на изискванията на ЕКПЧ; и

д) националната юрисдикция е приела, че налагането на изискванията, определени в точки 119—125 от решение [от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970)], доколкото са приложими, би осуетило вземаните от [службите за сигурност и разузнавателните служби] мерки за гарантиране на националната сигурност, като по този начин би изложило на опасност националната сигурност на Обединеното кралство;

1) Попада ли — предвид член 4 ДЕС и член 1, параграф 3 от Директива [2002/58] — в обхвата на правото на Съюза и на Директива [2002/58] изискване, което се съдържа в указание на министър до доставчик на електронна съобщителна мрежа и съгласно което последният трябва да предостави масив от данни за съобщения на службите за сигурност и разузнавателните служби на държава членка?

2) Ако отговорът на първия въпрос е утвърдителен, прилагат ли се по отношение на такова указание на министър някои от изискванията [приложими по отношение на съхраняваните масиви от данни за съобщения, определени в точки 119—125 от решение от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970) или някакви други изисквания, освен предвидените в ЕКПЧ? Ако това е така, как и до каква степен се прилагат тези изисквания, като се има предвид съществената необходимост [службите за сигурност и разузнавателните служби] да използват техники за събиране и автоматизирана обработка на масиви от данни с цел защита на националната сигурност, както и степента, в която тези иначе съответстващи на ЕКПЧ възможности могат да бъдат сериозно възпрепятствани от налагането на такива изисквания?“.

По преюдициалните въпроси

По първия въпрос

30 С първия си въпрос запитващата юрисдикция по същество иска да се установи дали член 1, параграф 3 от Директива 2002/58 във връзка с член 4, параграф 2 ДЕС трябва да се тълкува в смисъл, че национална правна уредба, която позволява на държавен орган да задължи доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби данни за трафик и данни за местонахождение с цел опазването на националната сигурност, попада в приложното поле на тази директива.

31 В това отношение Privacy International изтъква по същество, че с оглед на изводите, произтичащи от практиката на Съда относно приложното поле на Директива 2002/58, както събирането на данни от службите за сигурност и разузнавателните служби при тези доставчици по силата на член 94 от Закона от 1984 г., така и тяхното използване от посочените служби попадат в приложното поле на тази директива, независимо дали данните се събират чрез предаване, извършено в отложено във времето или в реално време. По-специално фактът, че целта за защита на националната сигурност е изрично посочена в член 15, параграф 1 от тази директива, не водел до нейната неприложимост към такива случаи, а член 4, параграф 2 ДЕС не засягал този извод.

32 Обратно, правителството на Обединеното кралство, чешкото и естонското правителство, Ирландия, френското, кипърското, унгарското, полското и шведското правителство по същество твърдят, че Директива 2002/58 не се прилага към разглежданата в главното производство национална правна уредба, доколкото тя има за цел опазването на националната сигурност. Дейностите на службите за сигурност и разузнаване спадали към съществените функции на държавите членки, свързани с поддържането на обществения ред и опазването на вътрешната сигурност и на териториалната цялост, и следователно били единствено от компетентността на последните, както свидетелствал по-специално член 4, параграф 2, трето изречение ДЕС.

33 Ето защо според тези правителства Директива 2002/58 не може да се тълкува в смисъл, че националните мерки за опазването на националната сигурност попадат в нейното приложно поле. Член 1, параграф 3 от тази директива ограничавал това приложно поле и изключвал, подобно на вече предвиденото в член 3, параграф 2, първо тире от Директива 95/46, дейностите, свързани с обществената сигурност, отбраната и държавната сигурност. Тези разпоредби отразявали разпределението на компетентностите, предвидени в член 4, параграф 2 ДЕС, и щели да бъдат лишени от полезно действие, ако мерките в областта на националната сигурност трябва да отговарят на изискванията на Директива 2002/58. Освен това практиката на Съда, установена с решение от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346) относно член 3, параграф 2, първо тире от Директива 95/46, била приложима към член 1, параграф 3 от Директива 2002/58.

34 В това отношение следва да се посочи, че съгласно член 1, параграф 1 от Директива 2002/58 тя предвижда по-специално хармонизиране на националните разпоредби, необходими за осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по отношение на обработката на лични данни в сектора на електронните съобщения.

35 Член 1, параграф 3 от тази директива изключва от приложното ѝ поле „дейностите на държавата“ в определени области, а именно дейностите в областта на наказателното право, както и тези, отнасящи се до обществената сигурност, отбраната, сигурността на държавата, включително икономическото благосъстояние на държавата, когато дейностите се отнасят до сигурността на държавата. Примерно посочените по този начин дейности във всички случаи са

присъщи на държавите или на държавните органи дейности, които са извън областите на дейност на частноправните субекти (решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 32 и цитираната съдебна практика).

36 Освен това член 3 от Директива 2002/58 предвижда, че тя се прилага при обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Съюза, включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация (наричани по-нататък „електронни съобщителни услуги“). Споменатата директива трябва следователно да се разглежда като уреждаща дейността на доставчиците на такива услуги (решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788,т. 33 и цитираната съдебна практика).

37 В този контекст член 15, параграф 1 от Директива 2002/58 допуска държавите членки, като спазват предвидените в него условия, да приемат „законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5, член 6, член 8, параграф[и] 1, 2, 3, и 4 и член 9 от [тази] директива“ (решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 71).

38 Член 15, параграф 1 от Директива 2002/58 обаче логично предполага, че посочените в нея национални законодателни мерки попадат в приложното ѝ поле, тъй като тя изрично допуска държавите членки да ги приемат само при спазване на предвидените в нея условия. Освен това подобни мерки регламентират — за посочените в същата разпоредба цели — дейността на доставчиците на електронни съобщителни услуги (решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 34 и цитираната съдебна практика).

39 Именно с оглед на тези съображения Съдът е приел, че член 15, параграф 1 от Директива 2002/58 във връзка с член 3 от нея трябва да се тълкува в смисъл, че в приложното поле на тази директива попада не само законодателна мярка, с която на доставчиците на електронни съобщителни услуги се налага задължение за запазване на данни за трафик и на данни за местонахождение, а и законодателна мярка, която ги задължава да предоставят на компетентните национални органи достъп до тези данни. Всъщност такива законодателни мерки по необходимост предполагат обработване на посочените данни от доставчиците и доколкото уреждат дейностите на същите доставчици, не могат да се приравнят на присъщи на държавите дейности, посочени в член 1, параграф 3 от тази директива (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 35 и 37 и цитираната съдебна практика).

40 Що се отнася до законодателна мярка като член 94 от Закона от 1984 г., въз основа на която компетентният орган може да дава на доставчиците на електронни съобщителни услуги указания да разкриват масиви от данни за съобщения чрез предаване на службите за сигурност и разузнавателните служби, следва да се отбележи, че съгласно определението в член 4, точка 2 от Регламент 2016/679, което е приложимо в съответствие с член 2 от Директива 2002/58, във връзка с член 94, параграф 2 от същия регламент, понятието „обработка на лични данни“ означава „всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, […] съхранение, […] консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни […]“.

41 От това следва, че разкриването на лични данни чрез предаване, както и съхранението на данни или друг начин, по който данните стават достъпни, представлява обработка по смисъла на член 3 от Директива 2002/58 и следователно попада в приложното поле на тази директива (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 45).

42 Освен това, предвид изложените в точка 38 от настоящото решение съображения и общата структура на Директива 2002/58, тълкуване на тази директива в смисъл, че законодателните мерки по член 15, параграф 1 от нея са изключени от приложното ѝ поле, тъй като целите, които трябва да се преследват с такива мерки, по същество съвпадат с целите, които се преследват с дейностите по член 1, параграф 3 от тази директива, би лишило от смисъл посочения член 15, параграф 1 (вж. в този смисъл решение от 21 декември 2016 г., Tele2., C-203/15 и C-698/15, EU:C:2016:970, т. 72 и 73).

43 Както по същество изтъква генералният адвокат в точка 75 от заключението си по съединени дела La Quadrature du Net и др. (C-511/18 и C-512/18, EU:C:2020:6), на което се позовава в точка 24 от заключението си по настоящото дело, понятието „дейности“, съдържащо се в член 1, параграф 3 от Директива 2002/58, следователно не може да се тълкува като включващо законодателните мерки по член 15, параграф 1 от тази директива.

44 Разпоредбите на член 4, параграф 2 ДЕС, на които се позовават посочените в точка 32 от настоящото решение правителства, не могат да оборят този извод. Всъщност съгласно постоянната практика на Съда, макар държавите членки да са тези, които определят основните интереси на своята сигурност и предприемат подходящи мерки, за да гарантират вътрешната и външната си сигурност, единствено фактът, че национална мярка е приета за защита на националната сигурност, не може да доведе до изключване на приложимостта на правото на Съюза и да освободи държавите членки от необходимостта от спазване на това право (вж. в този смисъл решения от 4 юни 2013 г., ZZ, C-300/11, EU:C:2013:363, т. 38 и цитираната съдебна практика, от 20 март 2018 г., Комисия/Австрия (Държавна печатница), C-187/16, EU:C:2018:194, т. 75 и 76 и от 2 април 2020 г., Комисия/Полша, Унгария и Чешка република (Схема за временно преместване на кандидати за международна закрила), C-715/17, C-718/17 и C-719/17, EU:C:2020:257, т. 143 и170).

45 Наистина, в решение от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346, т. 56—59) Съдът е постановил, че предаването на лични данни от авиокомпании на публични органи на трета държава с цел предотвратяване и борба с тероризма и други тежки престъпления не попада съгласно член 3, параграф 2, първо тире от Директива 95/46 в приложното поле на тази директива, тъй като такова предаване се вписва в установените от публичноправните органи рамки, насочени към запазване на обществената сигурност.

46 С оглед обаче на съображенията, изложени в точки 36, 38 и 39 от настоящото решение, тази съдебна практика не може да се приложи към тълкуването на член 1, параграф 3 от Директива 2002/58. Всъщност, както по същество отбелязва генералният адвокат в точки 70—72 от заключението си по съединени дела La Quadrature du Net и др. (C-511/18 и C-512/18, EU:C:2020:6), член 3, параграф 2, първо тире от Директива 95/46, към който се отнася посочената съдебна практика, оставя извън приложното поле на тази директива по общ начин „обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност“, без да въвежда разграничение, свързано със субекта, осъществяващ обработването на съответните данни. За сметка на това при тълкуването на член 1, параграф 3 от Директива 2002/58 такова разграничение се оказва необходимо. Всъщност, както следва от точки 37—39 и точка 42 от настоящото решение, всички видове обработване на лични данни, извършвано от доставчиците на електронни съобщителни услуги, попадат в приложното поле на посочената директива, включително обработването, което произтича от наложени им от публичните органи задължения, като последното обработване може евентуално да попада в приложното поле на изключението, предвидено в член 3, параграф 2, първо тире от Директива 95/46, като се има предвид по-широката формулировка на тази разпоредба, която се отнася до всеки вид обработване на данни, независимо от лицето, което го извършва, свързани с обществената сигурност, отбраната или държавната сигурност.

47 Освен това следва да се отбележи, че съгласно член 94, параграф 1 от Регламент 2016/679 Директива 95/46, която е предмет на делото, по което е постановено решение от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346), е отменена и заменена с този регламент, считано от 25 май 2018 г. Макар в член 2, параграф 2, буква г) от посочения регламент да се уточнява, че той не се прилага към обработването, извършвано „от компетентните органи“ за целите по-специално на предотвратяването и разкриването на престъпления, включително предпазването от и предотвратяването на заплахи за обществената сигурност, от член 23, параграф 1, букви г) и з) от същия регламент следва, че обработването на лични данни, извършвано от частноправни субекти за същите цели, попада в приложното му поле. От това следва, че изложеното по-горе тълкуване на член 1, параграф 3, член 3 и член 15, параграф 1 от Директива 2002/58 е в съответствие с очертаването на приложното поле на Регламент 2016/679, което тази директива допълва и уточнява.

48 Обратно, когато държавите членки прилагат пряко мерки, които въвеждат изключение от поверителността на електронните съобщения, без да налагат на доставчиците на услуги задължения за обработване на такива съобщения, защитата на данните на засегнатите лица се урежда не от Директива 2002/58, а единствено от националното право, без да се накърнява прилагането на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 2016 г., стр. 89) така, че въпросните мерки трябва да зачитат по-специално националното право с конституционен ранг и изискванията на ЕКПЧ.

49 С оглед на изложените по-горе съображения на първия въпрос следва да се отговори, че член 1, параграф 3, член 3 и член 15, параграф 1 от Директива 2002/58 във връзка с член 4, параграф 2 ДЕС трябва да се тълкуват в смисъл, че национална правна уредба, която позволява на държавен орган да задължи доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби данни за трафик и данни за местонахождение с цел опазването на националната сигурност, попада в приложното поле на тази директива.

По втория въпрос

50 С втория си въпрос запитващата юрисдикция по същество иска да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с член 4, параграф 2 ДЕС, членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която позволява на държавен орган с цел опазването на националната сигурност да наложи на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно предаване на данни за трафик и на данни за местонахождение на службите за сигурност и разузнавателните служби.

51 В самото начало следва да се припомни, че съгласно сведенията, съдържащи се в акта за преюдициално запитване, член 94 от Закона от 1984 г. дава право на министъра, ако прецени, че това е необходимо в интерес на националната сигурност или на отношенията с чуждестранно правителство, да задължава чрез указания доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби масиви от данни за съобщения, като тези данни включват данни за трафик и данни за местонахождение, както и информация за използваните услуги по смисъла на член 21, параграфи 4 и 6 от RIPA. Последната разпоредба обхваща по-специално данните, необходими, за да се идентифицира източникът на съобщението и неговото местоназначение, да се определят датата, времето, продължителността и видът на съобщението, да се идентифицира използваното оборудване, както и да се установи местонахождението на крайните устройства и на осъществяване на съобщенията, данни, сред

които по-специално са името и адресът на ползвателя, телефонният номер на викащата страна и номерът на виканата страна, IP адресите на източника и на получателя на съобщението, както и адресите на посетените уебсайтове.

52 Това разкриване чрез предаване на данни се отнася до всички ползватели на електронни съобщителни средства, без да се уточнява дали предаването трябва да се извършва в реално време или отложено във времето. Съгласно сведенията, съдържащи се в акта за преюдициално запитване, след предаването им тези данни се съхраняват от службите за сигурност и разузнавателните служби и остават на разположение на последните за целите на тяхната дейност, подобно на другите бази данни, държани от тези служби. По-специално събраните по този начин данни, които подлежат на масово и автоматизирано обработване и анализи, могат да бъдат съпоставени с други бази данни, съдържащи различни категории масиви от лични данни, или да бъдат разкрити извън тези служби, както и на трети държави. На последно място, за тези действия не е необходимо предварително разрешение от юрисдикция или независим административен орган и не се предоставя никаква информация на съответните лица.

53 Както следва по-специално от съображения 6 и 7 от Директива 2002/58, тя има за цел да се защитят потребителите на електронни съобщителни услуги срещу рискове за техните лични данни и неприкосновеност на личния им живот в резултат на новите технологии, и по-специално по отношение на увеличаващата се способност за автоматизирано съхранение и обработка на данни. По-специално, както се посочва в съображение 2 от тази директива, тя се стреми да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от Хартата. В това отношение от обяснителния меморандум към предложението за директива на Европейския парламент и на Съвета относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (COM(2000) 385 окончателен), въз основа на което предложение е приета Директива 2002/58, следва, че законодателят на Съюза е искал „да направи така, че да продължи гарантирането на високо равнище на защита на личните данни и на личния живот за всички електронни съобщителни услуги, независимо от използваната технология“. [неофициален превод]

54 За тази цел член 5, параграф 1 от Директива 2002/58 предвижда, че „[д]ържавите членки гарантират конфиденциалност на съобщенията и свързани[те с тях данни за трафика] през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, чрез националното си законодателство“. В същата разпоредба се подчертава и че „[п]о-специално [държавите членки] забраняват слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители[,] без съгласието на заинтересованите потребители, с изключение на законно упълномощени да извършват това в съответствие с член 15[,] параграф 1“ и се уточнява, че „[този] параграф не пречи на техническото съхранение, което е необходимо за пренасяне на комуникация, без да противоречи на принципа за конфиденциалност“.

55 Така член 5, параграф 1 закрепва принципа на поверителност както на електронните съобщения, така и на свързаните с тях данни за трафик и предполага по-специално забрана за всяко лице, различно от ползвателите, да съхранява без тяхното съгласие тези съобщения и данни. Предвид общия характер на текста ѝ тази разпоредба по необходимост обхваща всяко действие, което позволява на трети лица да се запознаят със съобщенията и свързаните с тях данни за цели, различни от пренасянето на съобщение.

56 Следователно съдържащата се в член 5, параграф 1 от Директива 2002/58 забрана за записване на съобщенията и свързаните с тях данни обхваща всеки начин на предоставяне от доставчиците на електронни съобщителни услуги на данни за трафик и на данни за местонахождение на публични органи като служби за сигурност и разузнавателни служби, както и запазването на посочените данни от тези органи, независимо от последващото им използване.

57 По този начин с приемането на тази директива законодателят на Съюза конкретизира правата, признати в членове 7 и 8 от Хартата, така че ползвателите на електронни съобщителни средства по принцип имат право да очакват, че техните съобщения и свързаните с тях данни, без тяхно съгласие, остават анонимни и няма да могат да бъдат записвани (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 109).

58 Член 15, параграф 1 от Директива 2002/58 обаче позволява на държавите членки да въвеждат изключения от установеното в член 5, параграф 1 от нея принципно задължение да гарантират поверителността на личните данни, както и от свързаните с него задължения, посочени по-специално в членове 6 и 9 от въпросната директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност, отбраната, обществената безопасност и да осигури превенцията, разследването, разкриването и преследването на престъпления или неразрешено използване на електронна съобщителна система. В тази връзка държавите членки могат, inter alia, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, когато това е оправдано с едно от тези основания.

59 При това положение възможността за дерогиране от правата и задълженията, предвидени в членове 5, 6 и 9 от Директива 2002/58, не би могла да послужи като основание допускането на изключение от принципното задължение да се гарантира поверителността на електронните съобщения и на свързаните с тях данни, и по-специално на изрично предвидената в член 5 от тази директива забрана за съхраняване на тези данни, да се превърне в правило (вж. в този смисъл решения от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 89 и 104 и от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 111).

60 Освен това от член 15, параграф 1, трето изречение от Директива 2002/58 следва, че на държавите членки се разрешава да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, посочени в членове 5, 6 и 9 от тази директива, само при зачитане на общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и на основните права, гарантирани от Хартата. В това отношение Съдът вече е постановил, че задължението, наложено на доставчиците на електронни съобщителни услуги с национална правна уредба, за запазване на данни за трафик с цел да може, когато се налага, да се предоставя достъп до тях на компетентните национални органи, повдига въпроси относно зачитането не само на членове 7 и 8 от Хартата, отнасящи се съответно до защитата на личния живот и до защитата на личните данни, но и на член 11 от Хартата, отнасящ се до свободата на изразяване на мнение (вж. в този смисъл решения от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 25 и 70 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 91 и 92 и цитираната съдебна практика).

61 Същите тези въпроси се поставят и за други видове обработване на данни, като предаването им на лица, различни от потребителите или достъп до тези данни с оглед използването им (вж. по аналогия становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 122 и 123 и цитираната съдебна практика).

62 В този смисъл при тълкуването на член 15, параграф 1 от Директива 2002/58 трябва да се вземе предвид подчертаната в практиката на Съда важност както на правото на зачитане на личния живот, гарантирано с член 7 от Хартата, така и на правото на защита на личните данни, гарантирано с член 8 от нея, и свободата на изразяване на мнение — основно право, гарантирано с член 11 от Хартата, което представлява един от основните стълбове на демократичното и плуралистичното общество, отразяващо ценностите, на които се основава Съюзът в съответствие с член 2 ДЕС (вж. в този смисъл решения от 6 март 2001 г., Connolly/Комисия, C-274/99 P, EU:C:2001:127, т. 39 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 93 и цитираната съдебна практика).

63 При все това правата, признати в членове 7, 8 и 11 от Хартата, не са абсолютни, а трябва да се разглеждат във връзка с тяхната социална функция (вж. в този смисъл решение от 16 юли 2020 г., Facebook Ireland и Schrems, C-311/18, EU:C:2020:559, т. 172 и цитираната съдебна практика).

64 Всъщност, както следва от член 52, параграф 1 от Хартата, тя допуска ограничения на упражняването на тези права, стига тези ограничения да са предвидени в закон, да зачитат основното съдържание на посочените права и при спазване на принципа на пропорционалност да са необходими и действително да отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

65 Следва да се добави, че изискването всяко ограничение на упражняването на основни права да бъде предвидено в закон, означава, че самото правно основание, позволяващо намеса в тези права, трябва да определя обхвата на ограничението при упражняване на съответното право (решение от 16 юли 2020 г., Facebook Ireland и Schrems, C-311/18, EU:C:2020:559, т. 175 и цитираната съдебна практика).

66 Що се отнася до спазването на принципа на пропорционалност, член 15, параграф 1, първо изречение от Директива 2002/58 гласи, че държавите членки могат да приемат мярка, с които да дерогират принципа на поверителност на съобщенията и на свързаните с тях данни за трафик, когато това представлява „необходима, подходяща и пропорционална мярка в рамките на демократично общество“ с оглед на посочените в същата разпоредба цели. В съображение 11 от тази директива пък се уточнява, че такава мярка трябва да бъде „строго“ пропорционална на предвидената цел.

67 В това отношение следва да се припомни, че съгласно постоянната практика на Съда защитата на основното право на зачитане на личния живот изисква дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото. Освен това целта от общ интерес не може да бъде преследвана, без да се отчете фактът, че тя трябва да бъде съгласувана с основните права, които се засягат от мярката, при това като се извърши балансирано претегляне между целите и интересите и разглежданите права (вж. в този смисъл решения от 16 декември 2008 г., Satakunnan Markkinapörssi и Satamedia, C-73/07, EU:C:2008:727, т. 56, от 9 ноември 2010 г., Volker und Markus Schecke и Eifert, C-92/09 и C-93/09, EU:C:2010:662, т. 76, 77 и 86 и от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 52 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 140).

68 За да изпълни изискването за пропорционалност, правната уредба трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито данни са засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на тези лични данни срещу рискове от злоупотреби. Тази уредба трябва да е задължителна по вътрешното право, и в частност да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни, като по този начин гарантира ограничаване на намесата до строго необходимото Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматизирано обработване по-специално когато съществува значителен риск от неправомерен достъп до тези данни. Тези съображения важат най-вече когато става дума за защита на чувствителни данни, които са особената категория лични данни (вж. в този смисъл решения от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 54 и 55 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 117 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 141).

69 Що се отнася до въпроса дали национална правна уредба като разглежданата в главното производство отговаря на изискванията по член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, следва да се отбележи, че предаването на данни за трафик и на данни за местонахождение на лица, различни от ползвателите, каквито са службите за сигурност и разузнавателните служби, е дерогация от принципа на поверителност. При положение че това действие се извършва общо и неизбирателно, както е в настоящия случай, то превръща дерогирането от принципното задължение за гарантиране на поверителността на данните в правило, докато с установената с Директива 2002/58 система се изисква подобно дерогиране да бъде изключение.

70 Освен това съгласно постоянната практика на Съда предаването на трети лица на данни за трафика и на данни за местонахождение представлява намеса в основните права, закрепени в членове 7 и 8 от Хартата, независимо от последващото използване на тези данни. В това отношение е без значение дали съответните данни за личния живот имат чувствителен характер и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 124 и 126 и цитираната съдебна практика и решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 115 и116).

71 Произтичащата от предаването на службите за сигурност и разузнавателните служби на данни за трафик и на данни за местонахождение намеса в правото, закрепено в член 7 от Хартата, трябва да се счита за особено тежка най-вече предвид чувствителния характер на информацията, която тези данни могат да предоставят, и по-специално предвид възможността чрез тях да се установи профилът на съответните лица — информация, която е също толкова чувствителна, колкото е и самото съдържание на съобщенията. Освен тя може да породи усещане в съзнанието на съответните лица, че личният им живот е обект на постоянно наблюдение (вж. по аналогия решение от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 27 и 37 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 99 и 100).

72 Следва да се отбележи също, че предаването на данни за трафик и на данни за местонахождение на публичните органи за целите на сигурността само по себе си може да накърни правото на зачитане на тайната на съобщенията, закрепено в член 7 от Хартата, и да има възпиращ ефект върху упражняването от ползвателите на електронни съобщителни средства на свободата им на изразяване на мнение, гарантирана от член 11 от Хартата. Подобен възпиращ ефект обаче може да засегне по-специално лицата, чиито съобщения според националното право представляват професионална тайна, както и лицата, сигнализиращи за нередности, чиито действия са защитени от Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 година относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза (ОВ L 305, 2019 г., стр. 17). Освен това, колкото по-голям е броят и разнообразието на запазените данни, толкова по-сериозен е този ефект (вж. в този смисъл решения от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 28, от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 101 и от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 118).

73 Накрая, предвид значителното количество данни за трафик и данни за местонахождение, които могат да се запазват продължително чрез мярка за общо и неизбирателно запазване, както и предвид чувствителния характер на информацията, която тези данни могат да предоставят, самото им запазване от доставчиците на електронни съобщителни услуги създава опасност от злоупотреба и неправомерен достъп.

74 Що се отнася до целите, които могат да обосноват такава намеса, и по-специално целта за опазване на националната сигурност, разглеждана в главното производство, най-напред следва да се отбележи, че член 4, параграф 2 ДЕС гласи, че националната сигурност остава единствено в рамките на отговорността на всяка държава членка. Тази отговорност съответства на

първостепенния интерес от защита на съществените функции на държавата и основните интереси на обществото и включва предотвратяването и преследването на дейности, които могат сериозно да дестабилизират основните конституционни, политически, икономически или социални структури на дадена страна, и по-специално да заплашват пряко обществото, населението или самата държава, като например терористични дейности (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 135).

75 Значението на целта за опазване на националната сигурност във връзка с член 4, параграф 2 ДЕС обаче надхвърля това на другите цели, посочени в член 15, параграф 1 от Директива 2002/58, по-специално на целите за борба с престъпността като цяло, дори и с тежката престъпност, както и за опазване на обществената сигурност. Всъщност заплахи като посочените в предходната точка се различават по своето естество и особена тежест от общия риск от възникване на напрежение или смущения на обществената сигурност дори ако те са сериозни. При условие че се спазват другите изисквания, предвидени в член 52, параграф 1 от Хартата, целта за опазване на националната сигурност може да обоснове мерки, включващи по-сериозна намеса в основните права от тези, които биха могли да обосноват останалите цели (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, т. 136).

76 За да бъде изпълнено обаче изискването за пропорционалност, припомнено в точка 67 от настоящото решение, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото, национална правна уредба, съдържаща намеса в основните права, закрепени в членове 7 и 8 от Хартата, трябва да отговаря на изискванията, произтичащи от цитираната в точки 65, 67 и 68 от настоящото решение съдебна практика.

77 Що се отнася по-специално до достъпа на орган до лични данни, правната уредба не може да се ограничи до изискването достъпът до тези данни да отговаря на някоя от целите на тази правна уредба, а трябва да предвижда също и материални и процесуални условия за това използване (вж. по аналогия становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 192 и цитираната съдебна практика).

78 В този смисъл, тъй като общ достъп до всички запазени данни — при липсата на някаква, макар и непряка връзка с преследваната цел — не може да се счита за ограничен до строго необходимото, националната правна уредба, уреждаща достъпа до данни за трафик и данни за местонахождение, трябва да се основава на обективни критерии за определяне на обстоятелствата и условията, при които на компетентните национални органи трябва да се предоставя достъп до разглежданите данни (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 119 и цитираната съдебна практика).

79 Тези изисквания се прилагат a fortiori към законодателна мярка като разглежданата в главното производство, въз основа на която компетентните национални органи могат да задължават доставчиците на електронни съобщителни услуги да извършат разкриване чрез общо и неизбирателно предаване на данни за трафик и на данни за местонахождение на службите за сигурност и разузнавателните служби. Всъщност такова разкриване има за последица предоставянето на достъп до тези данни на публичните органи (вж. по аналогия становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 212).

80 Тъй като предаването на данни за трафик и на данни за местонахождение е общо и неизбирателно, то засяга абсолютно всички лица, които използват електронни съобщителни услуги. Следователно то се прилага дори за лица, за които не съществува никаква улика, даваща основание да се счита, че действията им биха могли да имат някаква, била тя непряка и далечна, връзка с целта за опазване на националната сигурност, и по-специално без да е установена

връзка между данните, които се предвижда да се предадат, и някаква заплаха за националната сигурност (вж. в този смисъл решения от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 57 и 58 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 105). С оглед на факта, че предаването на такива данни на публичните органи, в съответствие с посоченото в точка 79 от настоящото решение, е равностойно на достъп, следва да се приеме, че правна уредба, позволяваща общо и неизбирателно предаване на данни на публичните органи, предполага общ достъп.

81 От това следва, че национална правна уредба, която налага на доставчиците на електронни съобщителни услуги задължение за разкриване чрез общо и неизбирателно предаване на службите за сигурност и разузнавателните служби на данни за трафик и на данни за местонахождение, надхвърля границите на строго необходимото и не може да се счита за обоснована в едно демократично общество, така както изисква член 15, параграф 1 от Директива 2002/58 във връзка с член 4, параграф 2 ДЕС, членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

82 С оглед на всички гореизложени съображения на втория въпрос следва да се отговори, че член 15, параграф 1 от Директива 2002/58 във връзка с член 4, параграф 2 ДЕС, членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която позволява на държавен орган с цел опазването на националната сигурност да наложи на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно предаване на службите за сигурност и разузнавателните служби на данни за трафик и данни за местонахождение.

Относно разноските

83 С оглед на обстоятелството, че за страните по главното производство настоящото дело представлява отклонение от обичайния ход на производството пред запитващата юрисдикция, последната следва да се произнесе по съдебните разноски. Разходите, направени за представяне на становища пред Съда, различни от тези на посочените страни, не подлежат на възстановяване.

По изложените съображения Съдът (голям състав) реши:

1) **Член 1, параграф 3, член 3 и член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година, във връзка с член 4, параграф 2 ДЕС трябва да се тълкуват в смисъл, че национална правна уредба, която позволява на държавен орган да задължи доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби данни за трафик и данни за местонахождение с цел опазването на националната сигурност, попада в приложното поле на тази директива.**

2) **Член 15, параграф 1 от Директива 2002/58, изменена с Директива 2009/136, във връзка с член 4, параграф 2 ДЕС, членове 7, 8 и 11 и член 52, параграф 1 от Хартата за основните права на Европейския съюз, трябва да се тълкува в смисъл, че не допуска национална правна уредба, която позволява на държавен орган с цел опазването на националната сигурност да наложи на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно предаване на службите за сигурност и разузнавателните служби на данни за трафик и данни за местонахождение.**

Подписи