Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

20 септември 2022 година*

[Текст, поправен с определение от 27 октомври 2022 година]

„Преюдициално запитване — Обработване на лични данни в сектора на електронните съобщения — Поверителност на съобщенията — Доставчици на електронни съобщителни услуги — Общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение — Директива 2002/58/ЕО — Член 15, параграф 1 — Харта на основните права на Европейския съюз — Членове 6, 7, 8 и 11 и член 52, параграф 1 — Член 4, параграф 2 ДЕС“

По съединени дела C-793/19 и C-794/19

с предмет преюдициални запитвания, отправени на основание член 267 ДФЕС от Bundesverwaltungsgericht (Федерален административен съд, Германия) с актове от 25 септември 2019 г., постъпили в Съда на 29 октомври 2019 г., в рамките на производства по дела

**Bundesrepublik Deutschland**, представлявана от Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

срещу

**SpaceNet AG** (C-793/19),

**Telekom Deutschland GmbH** (C-794/19),

СЪДЪТ (голям състав),

състоящ се от: K. Lenaerts, председател, Ал. Арабаджиев, A. Prechal, S. Rodin, I. Jarukaitis и I. Ziemele, председатели на състави, T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (докладчик), N. Piçarra, L. S. Rossi и A. Kumin, съдии,

генерален адвокат: M. Campos Sánchez-Bordona,

секретар: D. Dittert, началник на отдел,

предвид изложеното в писмената фаза на производството и в съдебното заседание от 13 септември 2021 г.,

* Език на производството: немски.

като има предвид становищата, представени:

– за Bundesrepublik Deutschland, представлявана от Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, от C. Mögelin, в качеството на представител,

– [поправено с определение от 27 октомври 2022 година] за SpaceNet AG, от M. Bäcker, Universitätsprofessor,

– за Telekom Deutschland GmbH, от T. Mayen, Rechtsanwalt,

– за германското правителство, от J. Möller, F. Halibi, M. Hellmann, D. Klebs и E. Lankenau, в качеството на представители,

– за датското правителство, от M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen и M. Søndahl Wolff, в качеството на представители,

– за естонското правителство, от A. Kalbus и M. Kriisa, в качеството на представители,

– за Ирландия, от A. Joyce и J. Quaney, в качеството на представители, подпомагани от D. Fennelly, BL, и P. Gallagher, SC,

– за испанското правителство, от L. Aguilera Ruiz, в качеството на представител,

– за френското правителство, от A. Daniel, D. Dubois, J. Illouz, E. de Moustier и T. Stéhelin, в качеството на представители,

– за кипърското правителство, от I. Neophytou, в качеството на представител,

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

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

– за финландското правителство, от A. Laine и M. Pere, в качеството на представители,

– за шведското правителство, от H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson и H. Shev, в качеството на представители,

– за Европейската комисия, от G. Braun, S. L. Kalėda, H. Kranenborg, M. Wasmeier и F. Wilman, в качеството на представители,

– за Европейския надзорен орган по защита на данните, от A. Buchta, D. Nardi, N. Stolič и K. Ujazdowski, в качеството на представители,

след като изслуша заключението на генералния адвокат, представено в съдебното заседание от 18 ноември 2021 г.,

постанови настоящото

## Решение

1 Преюдициалните запитвания се отнасят до тълкуването 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), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (ОВ L 337, 2009 г., стр. 11) (наричана по-нататък „Директива 2002/58“), във връзка с членове 6—8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“) и член 4, параграф 2 ДЕС.

2 Запитванията са отправени в рамките на спорове между Bundesrepublik Deutschland (Федерална република Германия), представлявана от Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Федерална агенция за мрежите в областта на електроенергията, природния газ, далекосъобщенията, пощите и железниците, Германия), от една страна, и SpaceNet AG (дело C-793/19) и Telekom Deutschland GmbH (дело C-794/19), от друга страна, относно предвиденото за последните задължение да съхраняват далекосъобщителните данни за трафик и данни за местонахождение на техните клиенти.

## Правна уредба

### *Правото на Съюза*

#### *Директива 95/46/ЕО*

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 (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46 (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1).

4 Член 3, параграф 2 от Директива 95/46 гласи:

„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 Договора за Европейския съюз, 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*

5 Съображения 2, 6, 7 и 11 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 Хартата.

[…]

(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 Общността. 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 [правата на човека] и основните свободи[, подписана в Рим на 4 ноември 1950 г.], съгласно тълкуването [в] решенията на Европейския съд [по правата на човека]. 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 [правата на човека] и основните свободи“.

6 Член 1 от тази директива е озаглавен „Обхват и цел“ и предвижда:

„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 Общността.

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 функционирането на ЕС], като тези[,] обхванати от дялове V и VI от Договора за [ЕС], 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“.

7 Съгласно член 2 от посочената директива, озаглавен „Дефиниции“:

„Освен ако не е предвидено друго, се прилагат дефинициите от Директива [95/46] 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.

[…]“.

8 Член 3 от Директива 2002/58 е озаглавен „Обхванати услуги“ и 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 Общността, включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация“.

9 Съгласно член 5 от тази директива, 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“.

10 Член 6 от Директива 2002/58 е озаглавен „Данни за трафик“ и 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.

[…]“.

11 Член 9 от тази директива е озаглавен „Данни за местонахождение, различни от данни за трафик“ и параграф 1 от него предвижда:

„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. […]“.

12 Член 15 от Директива 2002/58 е озаглавен „Приложение на някои разпоредби от Директива [95/46]“ и параграф 1 от него гласи:

„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 Общността, включително онези, упоменати в член 6, параграф[и] 1 и 2 [ДЕС]“.

### *Германското право*

*TKG*

13 Член 113a, параграф 1, първо изречение от Telekommunikationsgesetz (Закон за далекосъобщенията) от 22 юни 2004 г. (BGBl. 2004 I, стр. 1190), в редакцията му, приложима към спора в главното производство (наричан по-нататък „TKG“), гласи следното:

„Задълженията във връзка със съхраняването на данни за трафик и с използването и сигурността на данните съгласно членове 113b—113g се отнасят до операторите, които предоставят на крайните потребители обществено достъпни далекосъобщителни услуги“.

14 Съгласно член 113b от TKG:

„(1) Операторите, посочени в член 113a, параграф 1, съхраняват данните на територията на страната по следния начин:

1. десет седмици за данните, посочени в параграфи 2 и 3,

2. четири седмици за данните за местонахождение, посочени в параграф 4.

(2) Доставчиците на обществено достъпни телефонни услуги съхраняват:

1. телефонния номер или друг идентификатор на линията, от която се извършва повикването, и на линията, която приема повикването, както и на всяка друга участваща линия в случай на препращане или прехвърляне на повикване,

2. дата и час на началото и на края на връзката и посочване на съответната часова зона,

3. информация за използваната услуга, когато в рамките на телефонната услуга могат да се ползват различни услуги,

4. в случая на мобилни телефонни услуги също и
   a) международните идентификатори на абонатите на мобилни услуги на линията, от която се осъществява повикването, и на линията, която приема повикването,
   b) международния идентификатор на крайното съоръжение, от което се осъществява повикването и с което се приема повикването,
   c) дата и час на първото активиране на услугата и посочване на съответната часова зона, когато услугите са предплатени,

5. в случая на интернет телефония също и IP адресите (адресите по интернет протокол) на осъществяващата и на приемащата повикването линия и присвоените на ползвателите идентификатори.

Първата алинея се прилага mutatis mutandis

1. в случай на предаване на кратки, мултимедийни или подобни съобщения; в този случай информацията по първа алинея, точка 2 се заменя с момента на изпращане и на получаване на съобщението;

2. за повиквания без отговор или за неуспешен опит за повикване поради намеса в резултат на управлението на мрежата […]

(3) Доставчиците на обществено достъпни услуги за достъп до интернет съхраняват:

1. IP адрес, който е присвоен на абоната за ползване на интернет,

2. уникален идентификатор на линията, чрез която се осъществява ползването на интернет, както и присвоен на ползвателя идентификатор,

3. дата и час на началото и на края на ползването на интернет с присвоения IP адрес, с посочване на съответната часова зона.

(4) В случай на ползване на мобилни телефонни услуги се съхраняват знаците на клетките, които се използват в началото на връзката от осъществяващия и от приемащия повикването. Що се отнася до обществено достъпните услуги за достъп до интернет, при мобилно ползване се съхраняват знаците на клетката, която се използва в началото на интернет връзката. Следва също така да се съхраняват данните, които позволяват да се установят географското положение и посоките на максимално излъчване на антените, обслужващи съответната клетка.

(5) Съдържанието на съобщенията, данни за посетени интернет страници и данни за услуги за електронна поща не могат да бъдат съхранявани съгласно настоящата разпоредба.

(6) Данните, свързани със съобщенията по член 99, параграф 2, не могат да бъдат съхранявани съгласно настоящата разпоредба. Посоченото се прилага mutatis mutandis за телефонните разговори, започнати от субектите по член 99, параграф 2. Член 99, параграф 2, второ до седмо изречение се прилага mutatis mutandis.

[…]“.

15 Съобщенията по член 99, параграф 2 от TKG, към които препраща член 113b, параграф 6 от TKG, са връзки с лица, органи и организации в социалния сектор или в църковната сфера, които единствено или главно предлагат на по принцип анонимни събеседници услуги за телефонни консултации в случай на необходимост от спешна социална или психологическа помощ, като за самите тези лица, органи и организации или за техните сътрудници важат специални задължения за конфиденциалност в това отношение. Изключението по член 99, параграф 2, второ и четвърто изречение от TKG е обвързано с условието за вписване на получаващите повиквания лица, по тяхно искане, в списък, изготвен от Федералната агенция за мрежите в областта на електроенергията, природния газ, далекосъобщенията, пощите и железниците, след като притежателите на телефонни номера са доказали осъществяваната от тях дейност, като са представили удостоверение, издадено от образувание, орган или фондация, субект на публичното право.

16 Съгласно член 113c, параграфи 1 и 2 от TKG:

„(1) Данните, съхранени в съответствие с член 113b, могат:

1. да бъдат предавани на правоприлагащ орган, когато такъв орган поиска предаването, позовавайки се на законова разпоредба, която му разрешава да събира посочените в член 113b данни за целите на преследването на особено тежки престъпления;

2. да бъдат предавани на орган по сигурността в отделните провинции, когато такъв орган поиска предаването, позовавайки се на законова разпоредба, която му разрешава да събира посочените в член 113b данни за целите на предотвратяването на конкретна заплаха за телесната неприкосновеност, живота или свободата на дадено лице или за съществуването на федералната държава или на съответната провинция;

[…]

(2) Данните, съхранени съгласно член 113b, не могат да бъдат използвани от носителите на задълженията по член 113a, параграф 1 за цели, различни от посочените в параграф 1“.

17 Член 113d от TKG гласи:

„Носителят на задължението по член 113a, параграф 1 трябва да гарантира, че данните, съхранени в съответствие с член 113b, параграф 1 въз основа на задължението за съхраняване, са защитени чрез съобразени със състоянието на техниката технически и организационни мерки срещу неразрешен контрол и неразрешено използване. Тези мерки включват по-специално:

1. използване на високо сигурна процедура за криптиране,

2. съхраняване в инфраструктури за съхранение, отделни от предназначените за текущи оперативни задачи,

3. съхраняване при висока степен на защита срещу кибератаки в несвързани с интернет системи за обработка на данни,

4. ограничаване на достъпа до използваните за обработка на данни съоръжения само за лица, специално оправомощени от носителя на задължението, и

5. задължение за участие по време на достъпването на данните на най-малко две лица, специално оправомощени от носителя на задължението“.

18 Член 113e от TKG гласи следното:

„(1) Носителят на задължението по член 113a, параграф 1 трябва да гарантира, че за целите на контрола в областта на защитата на данни се отбелязва всеки достъп — по-специално четене, копиране, изменение, изтриване или заключване — до данните, съхранени в съответствие с член 113b, параграф 1 въз основа на задължението за съхраняване. Отбелязва се:

1. час на достъпа,

2. лицата, които достъпват данните,

3. предмет и естество на достъпа.

(2) Отбелязаните данни не могат да се използват за цели, различни от тези на контрола в областта на защитата на данните.

(3) Носителят на задължението по член 113a, параграф 1 трябва да гарантира, че отбелязаните данни се изтриват след една година“.

19 За да се гарантира особено високо равнище на сигурност и качество на данните, Федералната агенция за мрежите в областта на електроенергията, природния газ, далекосъобщенията, пощите и железниците въвежда, в съответствие с член 113f, параграф 1 от TKG, набор от изисквания, които по силата на член 113f, параграф 2 от него трябва постоянно да се проверяват и при необходимост да се адаптират. Член 113g от TKG изисква в изложението относно политиката в областта на сигурността, което трябва да бъде представено от носителя на задължението, да бъдат включени специфични мерки за сигурност.

*StPO*

20 Член 100g, параграф 2, първо изречение от Strafprozessordnung (Наказателно-процесуален кодекс, наричан по-нататък „StPO“) гласи следното:

„Ако определени обстоятелства позволяват да се подозира, че някой е извършил, в качеството си на извършител или на съучастник, особено тежко престъпление от посочените във второ изречение или — в случаите, в които опитът за извършване на престъпление е наказуем — се е опитал да извърши такова престъпление и ако престъплението е особено тежко в конкретния случай, данните за трафика, съхранени в съответствие с член 113b от [TKG], могат да бъдат събрани, в случай че разследването относно деянията или установяването на местонахождението на разследваното лице биха били прекомерно трудни или невъзможни с други средства и ако събирането на данните е пропорционално на значението на случая“.

21 Съгласно член 101a, параграф 1 от StPO за събирането на данни за трафика в съответствие с член 100g от StPO се изисква разрешение от съда. Съгласно член 101a, параграф 2 от StPO мотивите на решението на съда трябва да съдържат основните съображения относно необходимостта и целесъобразността на мярката в конкретния случай. Член 101a, параграф 6 от StPO предвижда задължение за уведомяване на лицата, участвали в съответната връзка.

## Споровете в главните производства и преюдициалният въпрос

22 SpaceNet и Telekom Deutschland предоставят в Германия обществено достъпни услуги за достъп до интернет. Освен това второто дружество предоставя в Германия обществено достъпни телефонни услуги.

23 Тези доставчици на услуги оспорват пред Verwaltungsgericht Köln (Административен съд Кьолн, Германия) наложеното им по силата на член 113a, параграф 1 във връзка с член 113b от TKG задължение, считано от 1 юли 2017 г., да съхраняват далекосъобщителните данни за трафик и за местонахождение на своите клиенти.

24 С решения от 20 април 2018 г. Verwaltungsgericht Köln (Административен съд Кьолн) постановява, че SpaceNet и Telekom Deutschland не са длъжни да съхраняват посочените в член 113b, параграф 3 от TKG далекосъобщителни данни за трафик на своите клиенти, на които предоставят достъп до интернет, и че освен това Telekom Deutschland не е длъжно да съхранява посочените в член 113b, параграф 2, първо и второ изречение от TKG далекосъобщителни данни за трафик на своите клиенти, на които предоставя достъп до обществено достъпни телефонни услуги. Всъщност този съд приема, че с оглед на решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970) това задължение за съхраняване е в противоречие с правото на Съюза.

25 Федерална република Германия подава ревизионни жалби срещу тези решения пред запитващата юрисдикция, Bundesverwaltungsgericht (Федерален административен съд, Германия).

26 Според запитващата юрисдикция отговорът на въпроса дали задължението за съхраняване, наложено с разпоредбите на член 113a, параграф 1 във връзка с член 113b от TKG, е в противоречие с правото на Съюза, зависи от тълкуването на Директива 2002/58.

27 В това отношение запитващата юрисдикция отбелязва, че в решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970), Съдът вече окончателно е установил, че правните уредби относно съхраняването на данни за трафика и данни за местонахождението, както и относно достъпването на тези данни от националните органи по принцип попадат в приложното поле на Директива 2002/58.

28 Тя отбелязва също, че доколкото разглежданото в главните производства задължение за съхраняване ограничава правата, произтичащи от член 5, параграф 1, член 6, параграф 1 и член 9, параграф 1 от Директива 2002/58, то може да бъде обосновано само на основание член 15, параграф 1 от тази директива.

29 В това отношение запитващата юрисдикция припомня, че видно от решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970), член 15, параграф 1 от Директива 2002/58 във връзка с 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 за целите на борбата с престъпността предвижда общо и неизбирателно съхраняване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства.

30 Според запитващата юрисдикция, подобно на националните правни уредби, разглеждани в делата, по които е постановено посоченото съдебно решение, разглежданата в главните производства национална правна уредба не изисква никакво основание за съхраняването на данни, нито каквато и да е връзка между съхранените данни и престъпление или заплаха за обществената сигурност. Всъщност тази национална правна уредба изисква общо съхраняване на по-голямата част от релевантните далекосъобщителни данни за трафик без основание и без оглед на лицето, периода или географското място.

31 Запитващата юрисдикция обаче счита, че не е изключено разглежданото в главните производства задължение за съхраняване да може да бъде обосновано съгласно член 15, параграф 1 от Директива 2002/58.

32 На първо място, тя отбелязва, че противно на националните правни уредби, разглеждани в делата, по които е постановено решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970), разглежданата в главните производства национална правна уредба не изисква съхраняването на всички далекосъобщителни данни за трафик на всички абонати и регистрирани ползватели на всички електронни съобщителни средства. Освен че съдържанието на съобщенията е изключено от обхвата на задължението за съхраняване, не се допуска и съхраняването на данни относно посетени интернет страници, данни от услуги за електронна поща, както и на данни, които указват връзките от и към някои линии в социалния сектор и в църковната сфера, както е видно от член 113b, параграфи 5 и 6 от TKG.

33 На второ място, запитващата юрисдикция посочва, че член 113b, параграф 1 от TKG предвижда данните за местонахождение да се съхраняват за срок от четири седмици, а данните за трафика — за срок от десет седмици, при положение че Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 2006 г., стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51), на която се основават националните правни уредби, разглеждани в делата, по които е постановено решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970), предвижда срок на съхраняване от шест месеца до две години.

34 Според запитващата юрисдикция, макар изключването на някои съобщителни средства или някои категории данни от обхвата на задължението за съхраняване и съкращаването на срока на съхраняване да не са достатъчни за премахване на всякаква опасност от съставянето на подробен профил на засегнатите лица, тази опасност поне е значително по-малка при прилагането на разглежданата в главните производства национална правна уредба.

35 На трето място, тази правна уредба предвижда строги ограничения, що се отнася до защитата на съхраняваните данни и на достъпа до тях. Съответно, от една страна, тя осигурява ефективна защита на съхраняваните данни срещу рискове от злоупотреба, както и срещу всякакъв неправомерен достъп до тези данни. От друга страна, съхраняваните данни могат да се използват само за борба с тежки престъпления или за предотвратяване на конкретна заплаха за телесната неприкосновеност, живота или свободата на дадено лице или за съществуването на федералната държава или на дадена провинция.

36 На четвърто място, тълкуването на член 15, параграф 1 от Директива 2002/58 в смисъл на обща несъвместимост с правото на Съюза на всяко съхраняване на данни без основание би могло да е в разрез със задължението на държавите членки за предприемане на действия, произтичащо от гарантираното в член 6 от Хартата право на сигурност.

37 На пето място, запитващата юрисдикция счита, че тълкуването на член 15 от Директива 2002/58 в смисъл, че не допуска общо съхраняване на данни, значително би ограничило свободата на действие на националния законодател в областта на наказателното преследване и на обществената сигурност, която съгласно член 4, параграф 2 ДЕС остава единствено в рамките на отговорността на всяка държава членка.

38 На шесто място, запитващата юрисдикция смята, че следва да се вземе предвид практиката на Европейския съд по правата на човека, и отбелязва, че последният съд е постановил, че член 8 от Европейската конвенция за защита на правата на човека и основните свободи (наричана по-нататък „ЕКПЧ“) допуска национални разпоредби, които предвиждат масово прихващане на трансгранични потоци на данни, предвид заплахите, пред които понастоящем са изправени редица държави, и техническите средства, които понастоящем могат да използват терористите и престъпниците, за да извършват неправомерни деяния.

39 При тези обстоятелства Bundesverwaltungsgericht (Федерален административен съд) решава да спре производството и да постави на Съда следния преюдициален въпрос:

„Трябва ли член 15 от Директива [2002/58] във връзка с членове 7, 8 и 11 и член 52, параграф 1 от [Хартата], от една страна, и с член 6 от [посочената харта], както и с член 4 [ДЕС], от друга страна, да се тълкува в смисъл, че не допуска национална правна уредба, която задължава доставчиците на обществено достъпни електронни съобщителни услуги да съхраняват данните за трафик и данните за местонахождението на крайните потребители на тези услуги, когато

1) за това задължение не е необходимо да е налице конкретно основание от гледна точка на място, време или пространство;

2) предмет на задължението за съхраняване при предоставянето на обществено достъпни телефонни услуги, включително при предаването на кратки, мултимедийни или подобни съобщения, както и на повиквания без отговор или на неуспешни повиквания, са следните данни:
   а) телефонният номер или друг идентификатор на линията, от която се извършва повикването, и на линията, която приема повикването, както и на всяка друга участваща линия в случай на препращане или прехвърляне;
   б) дата и час на началото и на края на връзката или, в случай на предаване на кратки, мултимедийни или подобни съобщения — времето на изпращането и на получаването на съобщението, и посочване на съответната часова зона;
   в) информация за използваната услуга, когато в рамките на телефонната услуга могат да се ползват различни услуги;
   г) в случая на мобилни телефонни услуги също и:
      i) международните идентификатори на абонатите на мобилни услуги на линията, от която се осъществява повикването, и на линията, която приема повикването;
      ii) международният идентификатор на крайното съоръжение, от което се осъществява повикването и с което се приема повикването;
      iii) дата и час на първото активиране на услугата и посочване на съответната часова зона, когато услугите са предплатени;
      iv) знаците на клетките, които се използват от осъществяващата и от приемащата повикването линия в началото на връзката;

д) в случая на интернет телефония също и адресите по интернет протокол на осъществяващата и на приемащата повикването линия и присвоените на ползвателите идентификатори;

3) предмет на задължението за съхраняване при предоставянето на обществено достъпни услуги за достъп до интернет са следните данни:
   а) адрес по интернет протокол, който е присвоен на абоната за ползване на интернет;
   б) уникален идентификатор на линията, чрез която се осъществява ползването на интернет, както и присвоен на ползвателя идентификатор;
   в) дата и час на началото и на края на ползването на интернет с присвоения адрес по интернет протокол, с посочване на съответната часова зона;
   г) при мобилно ползване: знаците на клетката, която се използва в началото на интернет връзката;

4) не се допуска съхраняването на следните данни:
   а) съдържанието на съобщенията;
   б) данни за посетени интернет страници;
   в) данни за услуги за електронна поща;
   г) данни, които указват връзките от и към някои линии на лица, органи и организации в социалния сектор или в църковната сфера;

5) срокът на съхраняване на данните за местонахождение, т.е. знаците на клетката, е четири седмици за използваната клетка и десет седмици за останалите данни;

6) е осигурена ефективна защита на съхранените данни срещу рискове от злоупотреба, както и срещу всякакъв неразрешен достъп, и

7) съхранените данни могат да се използват само за наказателното преследване на особено тежки престъпления и за предотвратяване на конкретна заплаха за телесната неприкосновеност, живота или свободата на дадено лице или за съществуването на федерацията или на дадена провинция, с изключение на адреса по интернет протокол, присвоен на даден абонат за ползване на интернет, чието използване е допустимо в рамките на справка със съхраняваните данни за целите на наказателното преследване на всякакви престъпления, предотвратяването на заплаха за обществения ред и сигурност, както и за изпълнението на функциите на разузнавателните служби?“.

## Производството пред Съда

40 С акт на председателя на Съда от 3 декември 2019 г. дела C-793/19 и C-794/19 са съединени за целите на писмената и устната фаза на производството, както и на съдебното решение.

41 С акт на председателя на Съда от 14 юли 2020 г. производството по съединени дела C-793/19 и C-794/19 е спряно на основание член 55, параграф 1, буква б) от Процедурния правилник на Съда до обявяване на решението по дело La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18).

42 След като на 6 октомври 2020 г. Съдът постановява решение по дело La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791), на 8 октомври 2020 г. председателят на Съда разпорежда възобновяване на производството по съединени дела C-793/19 и C-794/19.

43 Запитващата юрисдикция, която секретариатът уведомява за това решение, посочва, че поддържа преюдициалното си запитване.

44 В това отношение запитващата юрисдикция отбелязва най-напред, че задължението за съхраняване, предвидено в разглежданата в главните производства правна уредба, се отнася до по-малък брой данни и до по-кратък срок за съхраняване в сравнение с предвиденото в националните правни уредби, разглеждани в делата, по които е постановено решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791). Тези особености ограничават възможността съхранените данни да позволят извеждането на много точни заключения за личния живот на лицата, чиито данни са били съхранени.

45 На следващо място, тя отново посочва, че разглежданата в главните производства национална правна уредба осигурява ефективна защита на съхранените данни срещу рисковете от злоупотреба и неправомерен достъп.

46 На последно място, подчертава, че продължава да съществува неяснота относно съвместимостта с правото на Съюза на съхраняването на IP адреси, предвидено в разглежданата в главните производства национална правна уредба, поради непоследователност между точки 155 и 168 от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791). Съответно според запитващата юрисдикция това решение поражда неяснота по въпроса дали за съхраняването на IP адреси Съдът изисква да е налице основание за съхраняване, свързано с целта за опазване на националната сигурност, за борба с тежката престъпност или за предотвратяване на сериозни заплахи за обществената сигурност, както следва от точка 168 от посоченото решение, или съхраняването на IP адреси е позволено дори да няма конкретно основание, като единствено използването на съхранените данни е ограничено от посочените цели, както следва от точка 155 от същото решение.

**По преюдициалния въпрос**

47 С преюдициалния въпрос запитващата юрисдикция иска по същество да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 6—8 и 11, както и с член 52, параграф 1 от Хартата и с член 4, параграф 2 ДЕС трябва да се тълкува в смисъл, че не допуска национална законодателна мярка, която с някои изключения възлага на доставчиците на обществено достъпни електронни съобщителни услуги с оглед на целите, изброени в член 15, параграф 1 от тази директива, и по-специално на целите за преследване на тежки престъпления или предотвратяването на конкретна заплаха за националната сигурност, задължение за общо и неизбирателно съхраняване на основната част от данните за трафик и данните за местонахождение на крайните ползватели на тези услуги, като предвижда срок за съхраняване от няколко седмици и правила, с които да се гарантира ефективната защита на съхранените данни срещу рискове от злоупотреба, както и срещу всякакъв неправомерен достъп до тях.

***По приложимостта на Директива 2002/58***

48 По отношение на доводите на Ирландия, както и на френското, нидерландското, полското и шведското правителство, че доколкото разглежданата в главните производства национална правна уредба е приета по-специално за целите на опазване на националната сигурност, тя не попада в приложното поле на Директива 2002/58, е достатъчно да се припомни, че национална правна уредба, която възлага на доставчиците на електронни съобщителни услуги задължение да съхраняват данни за трафик и данни за местонахождение с оглед по-специално на опазването на националната сигурност и борбата срещу престъпността, като тази в делата по главните производства, попада в приложното поле на Директива 2002/58 (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 104).

***По тълкуването на член 15, параграф 1 от Директива 2002/58***

*Припомняне на принципите, изведени в практиката на Съда*

49 Съгласно постоянната съдебна практика, за да се тълкува разпоредба от правото на Съюза, трябва да се вземе предвид не само нейният текст, но и контекстът ѝ, както и целите, преследвани от правната уредба, от която тя е част, и по-специално генезисът на тази правна уредба (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 32 и цитираната съдебна практика).

50 От самия текст на член 15, параграф 1 от Директива 2002/58 следва, че законодателните мерки, които тя разрешава на държавите членки да приемат при определените в нея условия, могат единствено да имат за цел „да ограничат обхвата“ на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58 (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 33).

51 Що се отнася до въведената с тази директива система, в която се вписва член 15, параграф 1 от нея, следва да се припомни, че по силата на член 5, параграф 1, първо и второ изречение от посочената директива държавите членки са длъжни да гарантират — чрез националното си законодателство — конфиденциалност на съобщенията и свързаните с тях данни за трафика през публични съобщителни мрежи и публично достъпни електронни съобщителни услуги. По-специално те имат задължение да забранят 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 от същата директива (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 34).

52 В това отношение Съдът вече е постановил, че член 5, параграф 1 от Директива 2002/58 прогласява принципа на поверителност както на електронните съобщения, така и на свързаните с тях данни за трафика и въвежда по-специално принципна забрана за съхраняването им от лица, различни от потребителите, или без тяхното съгласие (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 107 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 35).

53 Тази разпоредба отразява целта, преследвана от законодателя на Съюза при приемането на Директива 2002/58. Всъщност 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] Както следва по-специално от съображения 6 и 7 от посочената директива, тя има за цел да се защитят ползвателите на електронни съобщителни услуги срещу рискове за техните лични данни и неприкосновеност на личния им живот в резултат на новите технологии, и по-специално в резултат на увеличаващата се способност за автоматизирано съхранение и обработка на данни. По-специално, както се посочва в съображение 2 от същата директива, волята на законодателя на Съюза е да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от Хартата, отнасящи се съответно до защитата на неприкосновеността на личния живот и до защитата на личните данни (вж. в този смисъл решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 36 и цитираната съдебна практика).

54 Така с приемането на Директива 2002/58 законодателят на Съюза конкретизира тези права, така че ползвателите на електронни съобщителни средства по принцип имат право да очакват, че ако не са дали съгласие, техните съобщения и свързаните с тях данни остават анонимни и няма да могат да бъдат записвани (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 109 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 37).

55 Що се отнася до обработването и съхранението от доставчиците на електронни съобщителни услуги на данни за трафик, отнасящи се до абонатите и ползвателите, член 6, параграф 1 от Директива 2002/58 предвижда, че тези данни трябва да бъдат изтрити или да се направят анонимни, когато не са необходими повече за целите на предаване на съобщение, а в параграф 2 от този член се уточнява, че данните за трафик, необходими за целите на изготвяне на сметката на абоната и плащания при взаимна връзка, могат да бъдат обработвани само до края на периода, през който сметката може законно да бъде оспорена или плащането търсено. Що се отнася до данните за местонахождение, различни от данните за трафик, член 9, параграф 1 от споменатата директива предвижда, че те могат да се обработват само при определени условия и след като бъдат направени анонимни или се получи съгласие от ползвателите или абонатите.

56 Следователно по отношение на достъпа до такива данни Директива 2002/58 не само предвижда гаранции, целящи предотвратяване на злоупотреби, но и закрепва в частност принципа на забрана на съхранението им от трети лица (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 39).

57 Доколкото член 15, параграф 1 от Директива 2002/58 позволява на държавите членки да приемат законодателни мерки, „за да ограничат обхвата“ на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от тази директива, като например произтичащите от припомнените в точка 52 от настоящото решение принципи на поверителност на съобщенията и на забрана на съхранението на свързаните с тях данни, тази разпоредба предвижда изключение от общото правило, предвидено по-специално в посочените членове 5, 6 и 9, и поради това съгласно постоянната съдебна практика трябва

да се тълкува стриктно. Ето защо такава разпоредба 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 от предвидената в член 5 от посочената директива забрана за съхраняване на тези данни, да се превърне в правило, без при това да се обезсмисли до голяма степен последната разпоредба (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 40 и цитираната съдебна практика).

58 Що се отнася до целите, които могат да обосноват ограничаване на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58, Съдът вече е постановил, че тези цели са изчерпателно изброени в член 15, параграф 1, първо изречение от Директива 2002/58, поради което приетата въз основа на тази разпоредба законодателна мярка трябва действително и строго да преследва някоя от тях (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 41 и цитираната съдебна практика).

59 Освен това от член 15, параграф 1, трето изречение от Директива 2002/58 следва, че мерките, приети от държавите членки въз основа на тази разпоредба, трябва да са съобразени с общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и да осигуряват спазването на основните права, гарантирани от Хартата. В това отношение Съдът вече е постановил, че задължението, наложено от държава членка на доставчиците на електронни съобщителни услуги с национална правна уредба, за съхраняване 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, но и на член 11 от Хартата, отнасящ се до свободата на изразяване на мнение, която представлява един от основните стълбове на демократичното и плуралистичното общество и отразява ценностите, на които се основава Европейският съюз в съответствие с член 2 ДЕС (вж. в този смисъл решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 42 и 43 и цитираната съдебна практика).

60 В това отношение следва да се уточни, че съхраняването на данни за трафик и на данни за местонахождение съставлява само по себе си, от една страна, дерогиране от предвидената в член 5, параграф 1 от Директива 2002/58 забрана всички лица, различни от потребителите, да съхраняват тези данни и от друга страна, намеса в основните права на зачитане на личния живот и на защита на личните данни, закрепени в членове 7 и 8 от Хартата, независимо дали съответните данни за личния живот имат чувствителен характер, дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса и дали съхранените данни ще бъдат използвани впоследствие (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 44 и цитираната съдебна практика).

61 Този извод изглежда още по-обоснован от обстоятелството, че данните за трафик и данните за местонахождение могат да разкрият информация за голям брой аспекти на личния живот на засегнатите лица, включително чувствителна информация като сексуалната ориентация, политическите възгледи, религиозните, философските, обществените или други убеждения, както и здравословното състояние, въпреки че подобни данни се ползват освен това с особена защита от правото на Съюза. От посочените данни, разгледани в съвкупност, е възможно да се изведат много точни заключения за личния живот на лицата, чиито данни са били съхранени, 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. По-специално тези данни предоставят средства да се установи профилът на съответните лица — информация, която с оглед на правото на зачитане на личния живот е също толкова чувствителна, колкото е и самото съдържание на съобщенията (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 45 и цитираната съдебна практика).

62 Ето защо, от една страна, съхраняването на данни за трафик и на данни за местонахождение за целите на полицията 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, като този ефект е още по-сериозен предвид големия брой и разнообразие на съхранените данни. От друга страна, предвид значителното количество данни за трафик и данни за местонахождение, които могат да се съхраняват постоянно чрез мярка за общо и неизбирателно съхраняване, както и предвид чувствителния характер на информацията, която тези данни могат да предоставят, самото им съхраняване от доставчиците на електронни съобщителни услуги създава опасност от злоупотреба и неправомерен достъп (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 46 и цитираната съдебна практика).

63 Доколкото обаче позволява на държавите членки да ограничат правата и задълженията, посочени в точки 51—54 от настоящото решение, член 15, параграф 1 от Директива 2002/58 отразява обстоятелството, че признатите в членове 7, 8 и 11 от Хартата права не са безусловни прерогативи, а трябва да се вземат предвид във връзка с тяхната социална функция. 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. Така тълкуването на член 15, параграф 1 от Директива 2002/58 в светлината на Хартата изисква да се отчита и значението на правата, закрепени в членове 3, 4, 6 и 7 от Хартата, както и значението на целите за защита на националната сигурност и борбата с тежката престъпност и приноса им за защитата на правата и свободите на други хора (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 48 и цитираната съдебна практика).

64 Така, що се отнася по-конкретно до ефективната борба срещу престъпленията, при които пострадали са по-специално ненавършили пълнолетие и други уязвими лица, следва да се има предвид обстоятелството, че от член 7 от Хартата могат да произтичат задължения за действие за публичните органи — за приемане на правни мерки за защита на личния и семейния живот. Такива задължения могат да произтичат от посочения член 7 и по отношение на защитата на жилището и на съобщенията, както и от членове 3 и 4, що се отнася до защитата на физическата и психическата неприкосновеност на лицата, както и до забраната на изтезанията и на нечовешкото и унизително отношение (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 49 и цитираната съдебна практика).

65 С оглед на тези различни задължения за действие обаче следва да се пристъпи към съвместяване на различните разглеждани законни интереси и права и да се въведе правна уредба, позволяваща това съвместяване (вж. в този смисъл решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 50 и цитираната съдебна практика).

66 При това положение от самия текст на член 15, параграф 1, първо изречение от Директива 2002/58 следва, че държавите членки могат да приемат мярка, с която да дерогират посочения в точка 52 от настоящото решение принцип на поверителност, когато това представлява „необходима, подходяща и пропорционална мярка в рамките на демократично общество“, като в съображение 11 от тази директива се уточнява, че такава мярка трябва да бъде „строго“ пропорционална на преследваната 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 се преследва, без да се отчете фактът, че тя трябва да бъде съвместена с основните права, които се засягат от мярката, като се претеглят, от една страна, целта от общ интерес и от друга страна, разглежданите права (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 52 и цитираната съдебна практика).

68 По-конкретно от практиката на Съда следва, че възможността за държавите членки да обосноват ограничение на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58, трябва да се прецени, като се измери тежестта на намесата, до която води подобно ограничение, и като се провери дали значението на преследваната с това ограничение цел от общ интерес е съразмерно с тази тежест (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 53 и цитираната съдебна практика).

69 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 налагат минимални изисквания, така че лицата, чиито лични данни са засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на тези данни срещу рискове от злоупотреби. Тази правна 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 особена категория лични данни (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 54 и цитираната съдебна практика).

70 Така национална правна уредба, предвиждаща съхраняване на личните данни, трябва винаги да отговаря на обективни критерии, установяващи връзка между подлежащите на съхраняване лични данни и преследваната цел (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 55 и цитираната съдебна практика).

71 Що се отнася до целите от общ интерес, които биха могли да обосноват приемането на мярка по член 15, параграф 1 от Директива 2002/58, видно от практиката на Съда и в частност от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791), съгласно принципа на пропорционалност съществува йерархия между тези цели в зависимост от съответното им значение, а значението на преследваната с такава мярка цел трябва да е съразмерно с тежестта на следващата от мярката намеса (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 56).

72 Съответно по отношение на опазването на националната сигурност, което е от по-голямо значение спрямо останалите цели, посочени в член 15, параграф 1 от Директива 2002/58, Съдът констатира, че тази разпоредба във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата допуска законодателни мерки, позволяващи с оглед опазването на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение в положения, при които съответната държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, като решението, съдържащо това разпореждане, трябва да подлежи на ефективен контрол от съд или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени, като посоченото разпореждане може да бъде издадено само за ограничен до строго необходимото период от време, който може да бъде удължен, ако заплахата продължи да съществува (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 58 и цитираната съдебна практика).

73 Що се отнася до целта за превенция, разследване, разкриване и преследване на престъпления, Съдът приема, че в съответствие с принципа на пропорционалност единствено борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност могат да обосноват сериозна намеса в основните права, закрепени в членове 7 и 8 от Хартата, като намесата, която предполага съхраняването на данни за трафик и на данни за местонахождение. При това положение само когато намесата в посочените основни права не е сериозна, тя може да бъде обоснована от целта за превенция, разследване, разкриване и преследване общо на престъпления (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 59 и цитираната съдебна практика).

74 Що се отнася до целта за борба с тежката престъпност, Съдът е постановил, че национална правна уредба, която за тази цел предвижда общо и неизбирателно съхраняване 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. Всъщност, като се има предвид чувствителният характер на информацията, която може да се извлече от данните за трафик и данните за местонахождение, поверителността на последните е от съществено значение за правото на зачитане на личния живот. Така, като се има предвид, от една страна, възпиращото въздействие върху упражняването на посочените в точка 62 от настоящото решение основни права, закрепени в членове 7 и 11 от Хартата, до което може да доведе съхраняването на тези данни, и от друга страна, сериозността на намесата, до която води такова съхраняване, в едно демократично общество е важно, така както предвижда установената с Директива 2002/58 система, то да бъде изключение, а не правило и тези данни да не могат да са предмет на системно и продължително

съхраняване. Този извод се налага дори по отношение на целите за борба с тежката престъпност и за предотвратяване на тежки заплахи срещу обществената сигурност, както и на значението, което следва да им се признае (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 65 и цитираната съдебна практика).

75 За сметка на това Съдът уточнява, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата допуска законодателни мерки, които предвиждат — за целите на борбата срещу тежката престъпност и на предотвратяването на сериозни заплахи срещу обществената сигурност:

– целево съхраняване на данни за трафик и на данни за местонахождение, което да е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите засегнати лица или посредством географски критерий, за ограничен до строго необходимото период от време, който може да бъде удължен,

– общо и неизбирателно съхраняване на IP адреси, дадени на източника на свързване с интернет, за ограничен до строго необходимото период от време,

– общо и неизбирателно съхраняване на данни относно самоличността на ползвателите на електронни съобщителни средства, и

– да се разпореди на доставчиците на електронни съобщителни услуги посредством решение на компетентния орган, подлежащо на ефективен съдебен контрол, да извършват за определен период бързо съхраняване („quick freeze“) на данните за трафик и на данните за местонахождение, с които разполагат тези доставчици на услуги,

при положение че тези мерки гарантират с ясни и точни правила, че съхраняването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 168 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 67).

*Относно мярка, която предвижда общо и неизбирателно съхраняване за срок от няколко седмици на по-голямата част от данните за трафик и от данните за местонахождение*

76 Характеристиките на разглежданата в главните производства национална правна уредба, изтъкнати от запитващата юрисдикция, следва да бъдат разгледани именно в светлината на тези принципни съображения.

77 На първо място, що се отнася до обхвата на съхранените данни, от акта за преюдициално запитване е видно, че при предоставянето на телефонни услуги установеното с тази правна уредба задължение за съхраняване се отнася по-специално до данните, необходими за идентифициране на източника и местоназначението на повикването, датата и часа на началото и на края на връзката, или, в случай на предаване на кратки, мултимедийни или подобни съобщения — времето на изпращането и на получаването на съобщението, както и при мобилно ползване — знаците на клетката, която се използва от осъществяващата и от приемащата повикването линия в началото на връзката. При предоставянето на услуги за достъп до интернет задължението за съхраняване се отнася в частност до присвоения на абоната IP адрес, датата и часа на началото и на края на ползването на интернет от

присвоения IP адрес, и при мобилно ползване — знаците на клетката, която се използва в началото на интернет връзката. Съхраняват се и данните, които позволяват да се установят географското положение и посоките на максимално излъчване на антените, обслужващи съответната клетка.

78 Макар разглежданата в главните производства национална правна уредба да предвижда, че в обхвата на задължението за съхраняване не попадат съдържанието на съобщенията и данните за посетените интернет страници, и да възлага задължение за съхраняване на идентификатора на клетката само в началото на връзката, следва да се отбележи, че това важи по същество и за националните правни уредби за транспониране на Директива 2006/24, разглеждани в делата, по които е постановено решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791). Въпреки тези ограничения обаче в посоченото решение Съдът е постановил, че категориите данни, съхранявани съгласно посочената директива и тези национални правни уредби, могат да позволят да се направят много точни заключения за личния живот на съответните лица, като 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, и по-специално да се предоставят средства за установяване на профила на тези лица.

79 Освен това е важно да се отбележи, че макар да не обхваща данните за посетените интернет страници, разглежданата в главните производства правна уредба все пак предвижда съхраняването на IP адресите. Тъй като обаче тези адреси могат да се използват по-специално за да се извърши изчерпателното проследяване на пътя на потребителя в сайтовете и страниците в интернет („clickstream“) и следователно на неговата онлайн дейност, тези данни позволяват да се установи подробният му профил. В този смисъл съхраняването и анализът на посочените IP адреси, необходими за такова проследяване, представляват сериозна намеса в основните права на интернет потребителя, закрепени в членове 7 и 8 от Хартата (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 153).

80 Освен това, както отбелязва SpaceNet в писменото си становище, макар данните за услуги за електронна поща да не попадат в обхвата на задължението за съхраняване, предвидено в разглежданата в главните производства правна уредба, те са само незначителна част от разглежданите данни.

81 Съответно, както генералният адвокат отбелязва по същество в точка 60 от заключението си, в обхвата на задължението за съхраняване, предвидено в разглежданата в главните производства национална правна уредба, попада голяма съвкупност от данни за трафик и данни за местонахождение, които по същество съответстват на данните, във връзка с които е установена постоянната съдебна практика, припомнена в точка 78 от настоящото решение.

82 Освен това в отговор на поставен в съдебното заседание въпрос германското правителство уточнява, че само 1300 образувания са включени в списъка на лицата, органите или организациите в социалния сектор или в църковната сфера, чиито данни за електронните съобщения не се съхраняват по силата на член 99, параграф 2 и на член 113b, параграф 6 от TKG, което явно представлява малка част от всички ползватели на далекосъобщителни услуги в Германия, чиито данни попадат в обхвата на задължението за съхраняване,

предвидено в разглежданата в главните производства национална правна уредба. Съответно се съхраняват по-специално данните на ползватели, които имат задължения за професионална тайна, като адвокати, лекари и журналисти.

83 Следователно от акта за преюдициално запитване е видно, че предвиденото в тази национална правна уредба съхраняване на данни за трафик и данни за местонахождение засяга почти цялото население, без съответните лица да се намират, дори непряко, в положение да бъдат изложени на наказателно преследване. Също така тази уредба предвижда задължение за общо и неизбирателно съхраняване на основната част от данните за трафик и данните за местонахождение без основание и без оглед на лицето, периода или географското място, като обхватът на тези данни съответства по същество на този на данните, съхранявани в случаите, във връзка с които е установена посочената в точка 78 от настоящото решение съдебна практика.

84 Поради това, с оглед на цитираната в точка 75 от настоящото решение съдебна практика, задължение за съхраняване на данните като разглежданото в главните производства не може да се счита за целево съхраняване на данните, противно на поддържаното от германското правителство.

85 На второ място, що се отнася до срока на съхраняване на данните, от член 15, параграф 1, второ изречение от Директива 2002/58 следва, че срокът на съхраняване, предвиден в национална мярка, с която се възлага задължение за общо и неизбирателно съхраняване, несъмнено е един от релевантните фактори, за да се определи дали правото на Съюза допуска такава мярка, доколкото в посоченото изречение се изисква срокът да бъде „ограничен“.

86 В случая тези срокове, които съгласно член 113b, параграф 1 от TKG са четири седмици за данните за местонахождение и десет седмици за другите данни, действително са значително по-кратки от установените в националните правни уредби, предвиждащи задължение за общо и неизбирателно съхраняване, разгледани от Съда в решения от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, EU:C:2016:970), от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791), и от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, EU:C:2022:258).

87 Както обаче следва от съдебната практика, цитирана в точка 61 от настоящото решение, тежестта на намесата произтича от риска, че съхранените данни в тяхната съвкупност, по-конкретно предвид техния брой и разнообразие, позволяват да се изведат много точни заключения за личния живот на лицето или лицата, чиито данни са били съхранени, и по-специално предоставят средства да се установи профилът на съответното лице или лица — информация, която с оглед на правото на зачитане на личния живот е също толкова чувствителна, колкото е и самото съдържание на съобщенията.

88 Следователно съхраняването на данни за трафик или данни за местонахождение, които могат да предоставят информация за извършените комуникации от ползвател на електронно съобщително средство или за местонахождението на използваните от него крайни устройства, при всички положения е сериозно, независимо от срока на съхраняване, от обема или вида на съхранените данни, когато от посочената съвкупност от данни може да се направят много точни изводи относно личния живот на засегнатото лице или лица (относно достъпа до такива данни вж. решение от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения), C-746/18, EU:C:2021:152, т. 39).

89 В това отношение дори съхраняването на ограничен обем данни за трафик или данни за местонахождение или съхраняването на тези данни за кратък срок може да предостави много точна информация за личния живот на даден ползвател на електронно съобщително средство. Освен това обемът налични данни и произтичащата от тях много точна информация за личния живот на съответното лице са обстоятелства, които могат да се преценят едва след запознаване с посочените данни. Произтичащата от съхраняването на посочените данни намеса обаче по необходимост настъпва, преди да може да се направи справка със съхранените данни и информация. В този смисъл преценката на тежестта на намесата, която представлява съхраняването, се извършва по необходимост в зависимост от риска, който обикновено се свързва с категорията съхранени данни за личния живот на съответните лица, без освен това да има значение дали произтичащата от тях информация за личния живот има конкретно чувствителен характер (вж. в този смисъл решение от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения), C-746/18, EU:C:2021:152, т. 40).

90 В случая, както следва от точка 77 от настоящото решение и както бе потвърдено в хода на съдебното заседание, съвкупност от данни за трафик и данни за местонахождение, съхранени през период от съответно десет и четири седмици, може да позволи да се изведат много точни заключения за личния живот на лицата, чиито данни са съхранени, като например за 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, и по-специално да се установи профилът на посочените лица.

91 На трето място, що се отнася до гаранциите, предвидени в разглежданата в главните производства национална правна уредба, за защита на съхранените данни срещу риска от злоупотреба или срещу всякакъв неправомерен достъп, следва да се отбележи, че както е видно от съдебната практика, припомнена в точка 60 от настоящото решение, съхраняването на тези данни и достъпът до тях представляват отделни видове намеса в основните права, гарантирани в членове 7 и 11 от Хартата, които изискват различна обосновка съгласно член 52, параграф 1 от нея. От това следва, че национална правна уредба, която осигурява пълното зачитане на условията, произтичащи от съдебната практика, с която се тълкува Директива 2002/58 в областта на достъпа до съхранените данни, по естеството си не може нито да ограничи, нито да отстрани тежката намеса, произтичаща от предвиденото в същата национална правна уредба общо съхраняване на тези данни, в правата, гарантирани в членове 5 и 6 от въпросната директива и чрез основните права, конкретизирани в тези членове (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 47).

92 На четвърто и последно място, що се отнася до довода на Европейската комисия, че особено тежката престъпност би могла да бъде приравнена на заплаха за националната сигурност, Съдът вече е постановил, че целта за опазване на националната сигурност съответства на първостепенния интерес от защита на съществените функции на държавата и основните интереси на обществото чрез 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 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 61 и цитираната съдебна практика).

93 За разлика от престъпността, дори и особено тежка, заплахата за националната сигурност трябва да бъде действителна и настояща или поне предвидима, което предполага настъпването на достатъчно конкретни обстоятелства, за да може да се обоснове общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение през ограничен период от време. Следователно такава заплаха се различава — по своето естество, тежест и специфика на свързаните с нея обстоятелства — от общия и постоянен риск от тежки престъпления или от възникване на напрежение или смущения на обществената сигурност дори ако те са сериозни (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 62 и цитираната съдебна практика).

94 Така престъпността, дори особено тежка, не може да се приравни на заплаха за националната сигурност. Всъщност подобно приравняване би могло да въведе междинна категория между националната сигурност и обществената сигурност, така че към обществената сигурност да се приложат изискванията, които са свързани с националната сигурност (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 63).

*Относно мерките, предвиждащи целево съхраняване, бързо съхраняване или съхраняване на IP адресите*

95 Няколко правителства, сред които и френското, подчертават, че само общото и неизбирателно съхраняване позволява ефективното осъществяване на целите, преследвани с мерките за съхраняване, като германското правителство уточнява по същество, че такъв извод не се опровергава от факта, че държавите членки могат да прибягнат до мерките за целево съхраняване и бързо съхраняване, посочени в точка 75 от настоящото решение.

96 В това отношение следва да се отбележи, на първо място, че ефективността на наказателното преследване по принцип зависи не от едно-единствено средство за разследване, а от всички средства за разследване, с които разполагат компетентните национални органи за тази цел (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 69).

97 На второ място, член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, както е тълкуван в припомнената в точка 75 от настоящото решение съдебна практика, позволява на държавите членки да приемат — за целите на борбата с тежката престъпност и на предотвратяването на сериозни заплахи за обществената сигурност — не само мерки, свързани с целево съхраняване и бързо съхраняване, но и мерки, предвиждащи общо и неизбирателно съхраняване, от една страна, на данните за самоличността на ползвателите на електронни съобщителни средства и от друга страна, на IP адресите, дадени на източника на свързването с интернет (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 70).

98 В това отношение е безспорно, че съхраняването на данните за самоличността на ползвателите на електронни съобщителни услуги може да допринесе за борбата с тежката престъпност, доколкото тези данни позволяват да се идентифицират лицата, използвали такива средства в контекста на подготвянето или извършването на тежко престъпление (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 71).

99 Директива 2002/58 обаче допуска — за целите на борбата с престъпността като цяло — общото съхраняване на данни за самоличност. При тези условия следва да се уточни, че нито тази директива, нито друг акт от правото на Съюза са пречка за приемането на национална правна уредба, която се отнася до борбата с тежката престъпност и по силата на която придобиването на електронно съобщително средство (като предплатена SIM карта) зависи от проверката на официални документи, удостоверяващи самоличността на купувача, и от регистрацията от продавача на получената по този начин информация, като продавачът е длъжен при необходимост да даде достъп до тази информация на компетентните национални органи (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 72).

100 Освен това следва да се припомни, че общото съхраняване на IP адресите, дадени на източника на свързване с интернет, представлява сериозна намеса в основните права, закрепени в членове 7 и 8 от Хартата, тъй като тези IP адреси могат да позволят да се направят точни изводи за личния живот на ползвателя на съответното електронно съобщително средство, и може да има възпиращо действие върху упражняването на свободата на изразяване на мнение, закрепена в член 11 от Хартата. При все това, що се отнася до подобно съхраняване, Съдът е приел, че за целите на необходимото съвместяване на разглежданите права и законни интереси, което се изисква съгласно посочената в точки 65—68 от настоящото решение съдебна практика, следва да се вземе предвид фактът, че в случай на извършено в интернет престъпление, и по-специално в случай на придобиване, разпространение, предаване или предоставяне онлайн на детска порнография по смисъла на член 2, буква в) от Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 година относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 2011 г., стр. 1 и поправка в ОВ L 18, 2012 г., стр. 7), IP адресът може да бъде единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което този адрес е бил предоставен към момента на извършване на това престъпление (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 73).

101 При тези условия, макар да е вярно, че законодателна мярка, която предвижда съхраняването на IP адресите на всички физически лица, собственици на крайно устройство, от което може да се осъществява достъп до интернет, се отнася до лица, които на пръв поглед нямат връзка с преследваните цели по смисъла на цитираната в точка 70 от настоящото решение съдебна практика, и че в съответствие с посоченото в точка 54 от настоящото решение интернет потребителите имат право да очакват, че по силата на членове 7 и 8 от Хартата тяхната самоличност по принцип няма да бъде разкривана, законодателна мярка, предвиждаща общо и неизбирателно съхраняване единствено на IP адресите, дадени на източника на свързването с интернет, по принцип не изглежда да е в противоречие с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, стига тази възможност да е поставена в зависимост от стриктното спазване на материалните и процесуалните условия, които трябва да регламентират използването на тези данни (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 155).

102 Предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, до която може да доведе това съхраняване, същата може да бъде обоснована единствено от борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност, подобно на опазването на националната сигурност. Освен това

срокът на съхраняването не може да надхвърля периода, който е строго необходим с оглед на преследваната цел. Накрая, мярка от такова естество трябва да предвижда строги правила и гаранции за използването на тези данни, по-специално чрез проследяване, по отношение на съобщенията и дейностите, извършвани онлайн от засегнатите лица (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 156).

103 Съответно, противно на подчертаното от запитващата юрисдикция, няма несъответствие между точки 155 и 168 от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791). Всъщност, както генералният адвокат отбелязва по същество в точки 81 и 82 от заключението си, от точка 155 във връзка с точки 156 и 168 от това решение ясно личи, че единствено борбата с тежката престъпност и предотвратяването на сериозните заплахи за обществената сигурност могат, подобно на опазването на националната сигурност, да обосноват общо съхраняване на IP адресите, дадени на източника на свързването с интернет, независимо от това дали за съответните лица може да се прилагат, дори и непряко, преследваните цели.

104 На трето място, що се отнася до законодателните мерки, предвиждащи целево съхраняване и бързо съхраняване на данни за трафик и на данни за местонахождение, някои съображения, изложени от държавите членки срещу такива мерки, разкриват по-тясно разбиране за обхвата на тези мерки от възприетото в съдебната практика, спомената в точка 75 от настоящото решение. Всъщност, макар в съответствие с напомненото в точка 57 от настоящото решение тези мерки за съхраняване да трябва да имат характер на дерогация в системата, установена с Директива 2002/58, последната, разглеждана в светлината на основните права, закрепени в членове 7, 8 и 11 и член 52, параграф 1 от Хартата, не поставя възможността да се разпореди целево съхраняване в зависимост от условието предварително да са известни местата, където би могло да бъде извършено тежко престъпление, нито лицата, заподозрени в участие в такова престъпление. Освен това посочената директива не изисква разпореждането за бързо съхраняване да бъде ограничено до идентифицирани преди издаването му заподозрени лица (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 75).

105 Що се отнася, първо, до целевото съхраняване, Съдът приема, че член 15, параграф 1 от Директива 2002/58 допуска национална правна уредба, основана на обективни обстоятелства, позволяващи с нея да се визират, от една страна, лица, чиито данни за трафик и данни за местонахождение могат да имат връзка, макар и непряка, с тежки престъпления, да допринесат за борбата с тежката престъпност или да предотвратят сериозна заплаха за обществената сигурност или заплаха за националната сигурност (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 76 и цитираната съдебна практика).

106 В това отношение Съдът уточнява, че макар тези обективни обстоятелства да могат да варират в зависимост от мерките, взети за целите на превенцията, разследването, разкриването и преследването на тежки престъпления, визираните по този начин лица могат по-специално да бъдат тези, които в рамките на приложимите национални процедури и въз основа на обективни и недискриминационни критерии са предварително идентифицирани като заплаха за обществената или националната сигурност на съответната държава членка (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 77).

107 Така държавите членки могат по-специално да приемат мерки за съхраняване по отношение на лица, спрямо които — във връзка с такова идентифициране — се провежда разследване или се прилагат други текущи мерки за наблюдение, или за които в националния регистър за съдимост е посочена предишна присъда за тежки престъпления, която може да предполага повишен риск от извършване на ново престъпление. Когато подобно идентифициране се основава на обективни и недискриминационни критерии, определени в националното право, целевото съхраняване на данни за така идентифицираните лица е оправдано (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 78).

108 От друга страна, мярка за целево съхраняване на данни за трафик и на данни за местонахождение може — според избора на националния законодател и при стриктно спазване на принципа на пропорционалност — да се основава и на географски критерий, когато въз основа на обективни и недискриминационни критерии компетентните национални органи установят, че в една или в няколко географски зони съществува повишен риск от подготвяне или извършване на тежки престъпления. Тези зони могат да бъдат по-специално места, характеризиращи се с голям брой тежки престъпления, места, особено изложени на извършването на тежки престъпления, като места или инфраструктури, редовно посещавани от много голям брой хора, или стратегически места като летища, гари, морски пристанища или зони за събиране на пътни такси (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 79 и цитираната съдебна практика).

109 Следва да се подчертае, че съгласно тази съдебна практика за посочените в предходната точка зони компетентните национални органи могат да приемат мярка за целево съхраняване, основана на географски критерий, като например средното равнище на престъпност в определена географска зона, без да разполагат непременно с конкретни данни за подготовката или извършването на тежки престъпления в съответните зони. Доколкото целево съхраняване, основано на такъв критерий, може да засегне — в зависимост от съответните тежки престъпления и от положението в съответните държави членки — както места, характеризиращи се с голям брой тежки престъпления, така и места, особено изложени на извършването на такива престъпления, то по принцип не може да доведе и до дискриминация, тъй като критерият, изведен от средното равнище на тежка престъпност, сам по себе си няма никаква връзка с потенциално дискриминационни обстоятелства (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 80).

110 В допълнение и преди всичко, мярка за целево съхраняване, насочена към места или инфраструктури, редовно посещавани от много голям брой хора, или към стратегически места като летища, гари, морски пристанища или зони за събиране на пътни такси, позволява на компетентните органи да събират данни за трафик и по-специално данни за местонахождението на всички лица, използващи в даден момент електронно съобщително средство на някое от тези места. Следователно такава мярка за целево съхраняване може да позволи на посочените органи чрез достъп до така съхранените данни да получат информация относно присъствието на тези лица на местата или в географските зони, до които мярката се отнася, както и относно придвижванията им между или в рамките на същите, и да направят изводи — за целите на борбата с тежката престъпност — относно присъствието им и дейността им на тези места или в тези географски зони в даден момент през периода на съхраняване (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 81).

111 Следва също да се отбележи, че географските зони, до които се отнася такова целево съхраняване, могат и при необходимост трябва да бъдат променени в зависимост от развитието на условията, обосновали избора им, като по този начин става възможно по-специално да се реагира на развитията в борбата с тежката престъпност. Всъщност Съдът вече е постановил, че продължителността на мерките за целево съхраняване, описани в точки 105—110 от настоящото решение, не може да надхвърля строго необходимото с оглед на преследваната цел, както и на обстоятелствата, които ги обосновават, без да се засяга евентуалното подновяване поради продължаваща необходимост от такова съхраняване (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 151 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 82).

112 Що се отнася до възможността да се предвидят отличителни критерии, различни от критерия относно категориите лица и от географския критерий, с оглед на осъществяването на целево съхраняване на данни за трафик и на данни за местонахождение, не може да се изключи възможността други обективни и недискриминационни критерии да бъдат взети предвид, за да се гарантира, че обхватът на целевото съхраняване е ограничен до строго необходимото, и за да се установи поне косвена връзка между тежките престъпления и лицата, чиито данни са съхранени. При все това, тъй като член 15, параграф 1 от Директива 2002/58 се отнася до законодателни мерки на държавите членки, именно последните, а не Съдът трябва да установят такива критерии, като се има предвид, че не може да става въпрос за ново въвеждане по този начин на общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 83).

113 Във всеки случай, както отбелязва генералният адвокат в точка 50 от заключението си, евентуалното наличие на трудности точно да се определят случаите и условията, при които следва да се извършва целево съхраняване, не оправдава държавите членки, превръщайки изключението в правило, да предвиждат общо и неизбирателно съхраняване на данните за трафик и на данните за местонахождение (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 84).

114 Второ, що се отнася до бързото съхраняване на данните за трафик и на данните за местонахождение, обработвани и съхранявани от доставчиците на електронни съобщителни услуги въз основа на членове 5, 6 и 9 от Директива 2002/58 или на законодателните мерки, приети по силата на член 15, параграф 1 от тази директива, следва да се припомни, че по принцип такива данни трябва, според случая, да бъдат изтрити или да се направят анонимни след изтичане на законовите срокове, в които трябва да се извършва обработването и съхранението им, в съответствие с националните разпоредби за транспониране на посочената директива. Съдът обаче приема, че по време на това обработване и съхранение могат да възникнат положения, при които е налице необходимост от запазване на посочените данни след изтичането на тези срокове с цел разкриването на тежки престъпления или посегателства върху националната сигурност както когато тези престъпления или посегателства върху националната сигурност вече са били установени, така и когато след обективна преценка на всички релевантни обстоятелства може разумно да се подозира, че съществуват (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 85).

115 При такова положение с оглед на посочената в точки 65—68 от настоящото решение необходимост да се съвместят разглежданите права и интереси, държавите членки могат да предвидят в законодателство, прието по силата на член 15, параграф 1 от Директива 2002/58, възможността посредством решение на компетентния орган, подлежащо на ефективен съдебен контрол, да бъде разпоредено на доставчиците на електронни съобщителни услуги да извършват за определен срок бързо съхраняване на данните за трафик и на данните за местонахождение, с които разполагат (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 163 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 86).

116 Доколкото целта на такова бързо съхраняване вече не съответства на целите, за които данните са събирани и съхранявани първоначално, и доколкото всяко обработване на данни трябва по силата на член 8, параграф 2 от Хартата да отговаря на определени цели, държавите членки трябва да уточнят в законодателството си целта, за която може да се осъществи бързото съхраняване на данните. Предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, която може да включва такова съхраняване, тази намеса може да бъде обоснована единствено с борбата с тежката престъпност и a fortiori, с опазването на националната сигурност, стига при тази мярка и при достъпа до така съхранените данни да се спазват границите на строго необходимото, посочени в точки 164—167 от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791) (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 87).

117 Съдът уточнява, че мярка за съхраняване от такова естество не трябва да се ограничава до данните на лицата, за които предварително е установено, че представляват заплаха за обществената сигурност или националната сигурност на съответната държава членка, или на лицата, конкретно заподозрени в извършване на престъпление или на посегателство срещу националната сигурност. Всъщност според Съда, спазвайки рамката, установена в член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, и предвид съображенията, изложени в точка 70 от настоящото решение, подобна мярка може, в зависимост от избора на националния законодател и при спазване на границите на строго необходимото, да бъде разширена до данните за трафик и данните за местонахождение, свързани с лица, различни от тези, за които има подозрения, че са подготвили или извършили тежко престъпление или посегателство срещу националната сигурност, ако тези данни въз основа на обективни и недискриминационни критерии могат да допринесат за разкриването на такова престъпление или посегателство срещу националната сигурност, като например данните на пострадалото от него лице, както и данните на неговото социално или професионално обкръжение (решения от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 165 и от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 88).

118 Така законодателна мярка може да разрешава да се разпореди на доставчиците на електронни съобщителни услуги да извършат бързо съхраняване на данни за трафик и данни за местонахождение по-специално на лица, с които преди възникването на сериозна заплаха за обществената сигурност или извършването на тежко престъпление пострадалият е бил в контакт чрез електронните си съобщителни средства (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 89).

119 Съгласно практиката на Съда, припомнена в точка 117 от настоящото решение, и при същите условия като посочените в тази точка такова бързо съхраняване може да се отнася и за определени географски зони, като мястото на извършване или подготовка на разглежданото престъпление или посегателство върху националната сигурност. Следва да се уточни, че такава мярка може да се приложи и за данните за трафик и данните за местонахождение, свързани с мястото, където лице, което евентуално е пострадало от тежко престъпление, е изчезнало, при условие че при прилагането на тази мярка и при достъпа до така съхранените данни са спазени границите на строго необходимото за целите на борбата с тежката престъпност или на опазването на националната сигурност, както са посочени в точки 164—167 от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791) (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 90).

120 Освен това е важно да се уточни, че член 15, параграф 1 от Директива 2002/58 допуска компетентните национални органи да разпоредят мярка за бързо съхраняване още на първия етап от разследването на сериозна заплаха за обществената сигурност или на евентуално тежко престъпление, тоест от момента, в който съгласно релевантните разпоредби от националното право тези органи могат да започнат такова разследване (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 91).

121 Що се отнася и до посочените в точка 75 от настоящото решение разнообразни мерки за съхраняване на данни за трафик и на данни за местонахождение, важно е да се уточни, че тези различни мерки могат да се приложат съвместно според избора на националния законодател и при спазване на границите на строго необходимото. При това положение член 15, параграф 1 от Директива 2002/58, разгледан във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата и тълкуван в решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791), допуска комбиниране на тези мерки (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 92).

122 На четвърто и последно място, важно е да се подчертае, че пропорционалността на приетите по силата на член 15, параграф 1 от Директива 2002/58 мерки изисква — съгласно постоянната практика на Съда, обобщена в решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791) — спазването не само на изискванията за пригодност и необходимост, но и на изискването, свързано с пропорционалния характер на тези мерки спрямо преследваната цел (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 93).

123 В този контекст следва да се припомни, че в точка 51 от решение от 8 април 2014 г., Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238) Съдът приема, че макар борбата с тежката престъпност да е от първостепенно значение за гарантиране на обществената сигурност и макар нейната ефективност да може до голяма степен да зависи от използването на модерни техники на разследване, сама по себе си подобна цел от общ интерес (въпреки че има основополагащо значение) не би могла да обоснове мярка на общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение като установената от Директива 2006/24 да се счита за необходима (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 94).

124 В същия смисъл Съдът уточнява в точка 145 от решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791), че дори задълженията за действие на държавите членки, които според случая могат да произтичат от членове 3, 4 и 7 от Хартата и (както бе отбелязано в точка 64 от настоящото решение) се отнасят до въвеждането на правила, позволяващи ефективна борба с престъпленията, не биха могли да обосноват толкова сериозна намеса в основните права, прогласени в членове 7 и 8 от Хартата, като съдържащата се в национална правна уредба, която предвижда съхраняване на данните за трафик и на данните за местонахождение на почти цялото население, без данните на засегнатите лица да имат връзка, макар и непряка, с преследваната цел (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 95).

125 Освен това решения на ЕСПЧ от 25 май 2021 г., Big Brother Watch и др. с/у Обединено кралство (CE:ECHR:2021:0525JUD 005817013), и от 25 май 2021 г., Centrum för Rättvisa с/у Швеция (CE:ECHR:2021:0525JUD 003525208), на които някои правителства се позовават в съдебното заседание в подкрепа на твърдението си, че ЕКПЧ допуска национални правни уредби, които по същество предвиждат общо и неизбирателно съхраняване на данни за трафик и данни за местонахождение, не могат да поставят под въпрос тълкуването на член 15, параграф 1 от Директива 2002/58, произтичащо от изложените по-горе съображения. Всъщност тези решения се отнасят до масовото прихващане на данни, свързани с международни комуникации. Съответно, както отбелязва Комисията в съдебното заседание, в посочените решения Европейският съд по правата на човека не се произнася по съответствието с ЕКПЧ на общо и неизбирателно съхраняване на данни за трафик и данни за местонахождение на територията на съответната страна, нито дори на прихващане от голям мащаб на тези данни за целите на предотвратяването, разкриването и разследването на тежки престъпления. При всички положения е уместно да се припомни, че член 52, параграф 3 от Хартата цели да гарантира необходимата съгласуваност между правата по Хартата и съответстващите им права, гарантирани от ЕКПЧ, без да се засяга самостоятелността на правото на Съюза и на Съда на Европейския съюз, поради което за целите на тълкуването на Хартата съответстващите права от ЕКПЧ трябва се вземат предвид само като минимален праг на защита (решение от 17 декември 2020 г., Centraal Israëlitisch Consistorie van België и др., C-336/19, EU:C:2020:1031, т. 56).

*Относно достъпа до данните, предмет на общо и неизбирателно съхраняване*

126 В съдебното заседание датското правителство поддържа, че компетентните национални органи би трябвало за целите на борбата с тежката престъпност да имат достъп до данните за трафик и до данните за местонахождение, съхранени общо и неизбирателно — съгласно практиката, установена с решение от 6 октомври 2020 г., La Quadrature du Net и др. (C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 135—139) — за целите на справянето със сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима.

127 Най-напред, следва да се отбележи, че предоставянето на достъп за целите на борбата с тежката престъпност до данни за трафик и до данни за местонахождение, които са били съхранени общо и неизбирателно, би поставило този достъп в зависимост от обстоятелства, които не са свързани с тази цел — тоест в зависимост от това дали в съответната държава членка съществува сериозна заплаха (като посочената в предходната точка) за националната сигурност — въпреки че с оглед единствено на целта за борба с тежката престъпност, която да оправдае съхраняването на тези данни и достъпа до тях, не

би могло да се обоснове различно третиране, по-специално между държавите членки (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 97).

128 Както Съдът вече е постановил, достъпът до данни за трафик и до данни за местонахождение, съхранени от доставчиците на електронни съобщителни услуги в приложение на мярка, приета на основание член 15, параграф 1 от Директива 2002/58 (като този достъп трябва да се осъществява при пълно спазване на условията, произтичащи от съдебната практика по тълкуването на посочената директива), по принцип може да бъде обоснован само с целта от общ интерес, за която тези доставчици са длъжни да ги съхраняват. Положението е различно само ако значението на целта, преследвана с достъпа, надхвърля това на целта, обосновала съхраняването (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 98).

129 Доводите на датското правителство се отнасят до положение, при което целта на евентуалното искане за достъп, а именно борба с тежката престъпност, е от по-малко значение в йерархията на целите от общ интерес, отколкото целта, обосновала съхраняването, а именно опазването на националната сигурност. При това положение предоставянето на достъп до съхранените данни не би съответствало на тази йерархия на целите от общ интерес, припомнена в предходната точка, както и в точки 68, 71, 72 и 73 от настоящото решение (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 99).

130 Освен това и преди всичко, съгласно съдебната практика, припомнена в точка 74 от настоящото решение, данните за трафик и данните за местонахождение не могат да бъдат предмет на общо и неизбирателно съхраняване за целите на борбата с тежката престъпност и следователно достъпът до тези данни не може да бъде обоснован за същите тези цели. Когато тези данни по изключение са били предмет на общо и неизбирателно съхраняване за целите на опазването на националната сигурност от действителна и настояща или предвидима заплаха при условията, посочени в точка 71 от настоящото решение, националните органи, компетентни в областта на разследването на престъпления, не биха могли да получат достъп до посочените данни в рамките на наказателно преследване, тъй като в противен случай би се лишила от всякакво полезно действие припомнената в посочената точка 74 забрана за такова съхраняване за целите на борбата с тежката престъпност (решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 100).

131 По всички изложени по-горе съображения на преюдициалния въпрос следва да се отговори, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национални законодателни мерки, предвиждащи общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение като превантивна мярка за целите на борбата с тежката престъпност и предотвратяването на сериозните заплахи за обществената сигурност. За сметка на това посоченият член 15, параграф 1 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че допуска национални законодателни мерки:

– позволяващи за целите на опазването на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение в положения, при които

съответната държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, като съдържащото това разпореждане решение трябва да подлежи на ефективен контрол от съд или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени, и посоченото разпореждане може да бъде издадено само за ограничен до строго необходимото период от време, който може да бъде удължен, ако заплахата продължи да съществува,

– предвиждащи за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност целево съхраняване на данни за трафик и на данни за местонахождение, което да е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите засегнати лица или посредством географски критерий, за ограничен до строго необходимото период от време, който може да бъде удължен,

– предвиждащи за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност общо и неизбирателно съхраняване на IP адреси, дадени на източника на свързване с интернет, за ограничен до строго необходимото период от време,

– предвиждащи за целите на опазването на националната сигурност, на борбата с престъпността и на опазването на обществената сигурност общо и неизбирателно съхраняване на данни относно самоличността на ползвателите на електронни съобщителни средства, и

– позволяващи за целите на борбата с тежката престъпност и a fortiori за опазване на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги посредством решение на компетентния орган, подлежащо на ефективен съдебен контрол, да извършват за определен период бързо съхраняване на данните за трафик и на данните за местонахождение, с които разполагат тези доставчици на услуги,

при положение че тези мерки гарантират с ясни и точни правила, че съхраняването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби.

**По съдебните разноски**

132 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:

**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 членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз**

**трябва да се тълкува в смисъл, че**

**не допуска национални законодателни мерки, предвиждащи общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение като превантивна мярка за целите на борбата с тежката престъпност и предотвратяването на сериозните заплахи за обществената сигурност;**

**допуска национални законодателни мерки:**

– **позволяващи за целите на опазването на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение в положения, при които съответната държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, като съдържащото това разпореждане решение трябва да подлежи на ефективен контрол от съд или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени, и посоченото разпореждане може да бъде издадено само за ограничен до строго необходимото период от време, който може да бъде удължен, ако заплахата продължи да съществува,**

– **предвиждащи за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност целево съхраняване на данни за трафик и на данни за местонахождение, което да е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите засегнати лица или посредством географски критерий, за ограничен до строго необходимото период от време, който може да бъде удължен,**

– **предвиждащи за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност общо и неизбирателно съхраняване на IP адреси, дадени на източника на свързване с интернет, за ограничен до строго необходимото период от време,**

– **предвиждащи за целите на опазването на националната сигурност, на борбата с престъпността и на опазването на обществената сигурност общо и неизбирателно съхраняване на данни относно самоличността на ползвателите на електронни съобщителни средства, и**

– **позволяващи за целите на борбата с тежката престъпност и a fortiori за опазване на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги посредством решение на компетентния орган, подлежащо на ефективен съдебен контрол, да извършват за определен период бързо съхраняване**

**на данните за трафик и на данните за местонахождение, с които разполагат тези доставчици на услуги,**

**при положение че тези мерки гарантират с ясни и точни правила, че съхраняването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби.**

Подписи