Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

6 октомври 2020 година*

[Текст, поправен с определение от 16 ноември 2020 година]

Съдържание

Правна уредба 7
Правото на Съюза 7
Директива 95/46 7
Директива 97/66 8
Директива 2000/31 8
Директива 2002/21 10
Директива 2002/58 11
Регламент 2016/679 15
Френското право 20
Code de la sécurité intérieure 20
CPCE 25
Закон № 2004-575 от 21 юни 2004 г. за доверието в цифровата икономика 27
Декрет № 2011-219 28
Белгийско право 30
Споровете в главните производства и преюдициалните въпроси 32
Дело C-511/18 32

* Език на производството: френски.

Дело C-512/18 35

Дело C-520/18 37

Относно производството пред Съда 39

Относно преюдициалните въпроси 39

По първите въпроси по дела C-511/18 и C-512/18, както и по първия и втория въпрос по дело C-520/18 39

Предварителни бележки 39

По приложното поле на Директива 2002/58 40

По тълкуването на член 15, параграф 1 от Директива 2002/58 44

– По законодателните мерки, предвиждащи превантивното запазване на данни за трафик и на данни за местонахождение с цел опазване на националната сигурност 50

– По законодателните мерки, предвиждащи превантивното запазване на данни за трафик и на данни за местонахождение за целите на борбата с престъпността и опазването на обществената сигурност 51

– По законодателните мерки, предвиждащи превантивното запазване на IP адресите и на данните за самоличност за целите на борбата с престъпността и опазването на обществената сигурност 53

– По законодателните мерки, предвиждащи бързото запазване на данни за трафик и на данни за местонахождение за целите на борбата с тежката престъпност 55

По втория и третия въпрос по дело C-511/18 58

По автоматизирания анализ на данни за трафик и на данни за местонахождение 59

По събирането в реално време на данни за трафик и на данни за местонахождение . . . 61

По уведомяването на лицата, чиито данни са били събрани или анализирани 63

По втория въпрос по дело C-512/18 64

По третия въпрос по дело C-520/18 68

По съдебните разноски 71

„Преюдициално запитване — Обработване на лични данни в сектора на електронните съобщения — Доставчици на електронни съобщителни услуги — Доставчици на хостинг услуги и доставчици на достъп до интернет — Общо и неизбирателно запазване на данни за трафик и на данни за местонахождение — Автоматизиран анализ на данните — Достъп в реално време до данните — Защита на националната сигурност и борба с

тероризма — Борба с престъпността — Директива 2002/58/ЕО — Приложно поле — Член 1, параграф 3 и член 3 — Поверителност на електронните съобщения — Защита — Член 5 и член 15, параграф 1 — Директива 2000/31/ЕО — Приложно поле — Харта на основните права на Европейския съюз — Членове 4, 6—8 и 11 и член 52, параграф 1 — Член 4, параграф 2 ДЕС“

По съединени дела C-511/18, C-512/18 и C-520/18,

с предмет преюдициални запитвания, отправени на основание член 267 ДФЕС от Conseil d'État (Държавен съвет, Франция) с актове от 26 юли 2018 г., постъпили в Съда на 3 август 2018 г. (C-511/18 и C-512/18), и от Cour constitutionnelle (Конституционен съд, Белгия) с акт от 19 юли 2018 г., постъпил в Съда на 2 август 2018 г. (C-520/18), в рамките на производства по дела

La Quadrature du Net (C-511/18 и C-512/18),

French Data Network (C-511/18 и C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 и C-512/18),

Igwan.net (C-511/18),

срещу

Premier ministre (C-511/18 и C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 и C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), при участието на:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

и

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

срещу

Conseil des ministres,

при участието на:

Child Focus (C-520/18),

СЪДЪТ (голям състав),

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

генерален адвокат: M. Campos Sánchez-Bordona,

секретар: C. Strömholm, администратор

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

като има предвид становищата, представени:

– за La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net и Center for Democracy and Technology, от A. Fitzjean Ò Cobhthaigh, адвокат,

– за French Data Network, от Y. Padova, адвокат,

– за Privacy International, от H. Roy, адвокат,

– за Ordre des barreaux francophones et germanophone, от E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart и J.-F. Henrotte, адвокати,

– за Académie Fiscale ASBL и UA, от J.-P. Riquet,

– за Liga voor Mensenrechten ASBL, от J. Vander Velpen, адвокат,

– за Ligue des Droits de l'Homme ASBL, от R. Jespers и J. Fermon, адвокати,

– за VZ, WY и XX, от D. Pattyn, адвокат,

– за Child Focus, от N. Buisseret, K. De Meester и J. Van Cauter, адвокати,

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

– за белгийското правителство, от J.-C. Halleux, P. Cottin и C. Pochet, в качеството на представители, подпомагани от J. Vanpraet, Y. Peeters, S. Depré и E. de Lophem, адвокати,

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

– за датското правителство, първоначално от J. Nymann-Lindegren, M. Wolff и P. Ngo, впоследствие от J. Nymann-Lindegren и M. Wolff, в качеството на представители,

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

– за естонското правителство, от N. Grünberg и A. Kalbus, в качеството на представители,

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

– за испанското правителство, първоначално от L. Aguilera Ruiz и A. Rubio González, впоследствие от L. Aguilera Ruiz, в качеството на представители,

– за кипърското правителство от E. Neofytou, в качеството на представител,

– за литовското правителство, от V. Soņeca, в качеството на представител,

– за унгарското правителство, първоначално от M. Z. Fehér и Z. Wagner, впоследствие от M. Z. Fehér, в качеството на представител,

– за нидерландското правителство от M. K. Bulterman и A. M. de Ree, в качеството на представители,

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

– за шведското правителство, първоначално от H. Shev, H. Eklinder, C. Meyer-Seitz, и A. Falk, а впоследствие от H. Shev, H. Eklinder, C. Meyer-Seitz и J. Lundberg, в качеството на представители,

– за правителството на Обединеното кралство от S. Brandon, в качеството на представител, подпомаган от G. Facenna, QC, и C. Knight, barrister,

– [заличено с определение от 16 ноември 2020 г.],

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

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

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

постанови настоящото

Решение

1 Преюдициалните запитвания се отнасят до тълкуването, от една страна, на член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63 и поправка в ОВ L 145, 8.6.2017 г., стр. 27), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (ОВ L 337, 2009 г., стр. 11 и поправка в ОВ L 241, 10.9.2013 г., стр. 9) (наричана по-нататък „Директива 2002/58“), и от друга страна, на членове 12—15 от Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 2000 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 29, стр. 257), във връзка с членове 4, 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 Запитването по дело C-511/18 е отправено в рамките на спорове между La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs и Igwan.net, от една страна, и Premier ministre (министър-председател, Франция), Garde des Sceaux, ministre de la Justice (министър на правосъдието, Франция), ministre de l'Intérieur (министър на вътрешните работи, Франция) и ministre des Armées (министър на отбраната, Франция), от друга страна, относно законосъобразността на Décret n.º 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Декрет № 2015-1185 от 28 септември 2015 г. за определяне на специализираните разузнавателни служби) (JORF от 29 септември 2015 г., текст 1 от 97, наричан по-нататък „Декрет № 2015-1185“), Décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Декрет № 2015-1211 от 1 октомври 2015 г. относно съдебните спорове във връзка с използването на разузнавателните средства, които подлежат на разрешителен режим, и на досиетата, свързани със сигурността на държавата) (JORF от 2 октомври 2015 г., текст 7 от 108, наричан по-нататък „Декрет № 2015-1211“), Décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (Декрет № 2015-1639 от 11 декември 2015 г. относно определянето на службите, различни от специализираните разузнавателни служби, на които е разрешено да използват средствата, посочени в дял V, книга VIII на Кодекса за вътрешната сигурност, приет в изпълнение на член L. 811-4 от Кодекса за вътрешната сигурност) (JORF от 12 декември

2015 г., текст 28 от 127, наричан по-нататък „Декрет № 2015-1639“) и Décret n.° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Декрет № 2016-67 от 29 януари 2016 г. относно средствата за събиране на разузнавателна информация) (JORF от 31 януари 2016 г., текст 2 от 113, наричан по-нататък „Декрет № 2016-67“).

3 Запитването по дело C-512/18 е отправено в рамките на спорове между French Data Network, La Quadrature du Net и Fédération des fournisseurs d'accès à Internet associatifs, от една страна, и министър-председателя (Франция) и министъра на правосъдието (Франция), от друга страна, относно законосъобразността на член R. 10-13 от Code des postes et des communications électroniques (Кодекс на пощите и електронните съобщения) (наричан по-нататък „CPCE“) и на Décret no 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Декрет № 2011-219 от 25 февруари 2011 г. относно запазването на данните, позволяващи идентифицирането на всяко лице, допринесло за създаването на съдържание, предлагано в интернет) (JORF от 1 март 2011 г., текст 32 от 170, наричан по-нататък „Декрет № 2011-219“).

4 Запитването по дело C-520/18 е отправено в рамките на спорове между Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des droits de l'Homme ASBL, VZ, WY и XX, от една страна, и Conseil des ministres (Министерски съвет, Белгия), от друга страна, относно законосъобразността на Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (Закон от 29 май 2016 г. за събирането и съхраняването на данни в областта на електронните съобщения) (Moniteur belge от 18 юли 2016 г., стр. 44717, наричан по-нататък „Закон от 29 май 2016 г.“).

Правна уредба

Правото на Съюза

Директива 95/46

5 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10) е отменена, считано от 25 май 2018 г., с Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1 и поправка в ОВ L 127, 23.5.2018 г., стр. 2). Член 3, параграф 2 от Директива 95/46 е гласял:

„Настоящата директива не се прилага за обработването на лични данни:

– при извършване на дейности, извън приложното поле на правото на Общността, например дейностите, предвидени в дял V и дял VI от [ДЕС], и във всички случаи при дейности по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност (включително икономическото благосъстояние на

държавата, когато процесът на обработка е свързан[…] с държавната сигурност) и при дейности на държавата в областта на наказателното право,

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

6 Член 22 от Директива 95/46, който се намира в глава III от нея, озаглавена „Средства за правна защита, отговорност и санкции“, е имал следното съдържание:

„Без това да засяга и да е административно средство за правна защита, което може да бъде предвидено, inter alia, пред надзорния орган, посочен в член 28, преди сезиране на съдебен орган, държавите членки предвиждат правото на всяко лице на правна защита за всяко нарушение на правата, гарантирани от националното право, приложимо към въпросната обработка“.

Директива 97/66

7 Съгласно член 5 от Директива 97/66/ЕО на Европейския парламент и на Съвета от 15 декември 1997 година относно обработката на лични данни и защитата на неприкосновеността на личния живот в телекомуникационния сектор (ОВ L 24, 1997 г., стр. 1), озаглавен „Конфиденциалност на комуникациите“ [неофициален превод]:

„1. Държавите членки осигуряват посредством вътрешни разпоредби конфиденциалността на комуникациите посредством обществена телекомуникационна мрежа и обществено достъпни телекомуникационни услуги. По-специално те забраняват подслушването, записването, съхранението или други видове прихващане или наблюдение на комуникации от други лица, освен ползвателите, без тяхното съгласие, освен ако това не е законно разрешено в съответствие с член 14, параграф 1.

2. Параграф 1 не засяга което и да е законно разрешено записване на комуникации в рамките на законосъобразната търговска практика с оглед предоставяне на доказателства за търговска сделка или за която и да е друга служебна комуникация“. [неофициален превод]

Директива 2000/31

8 Съображения 14 и 15 от Директива 2000/31 предвиждат:

„(14) Защитата на лицата по отношение на обработката на лични данни е уредена единствено в Директива [95/46] и Директива [97/66], които са напълно приложими за услугите на информационното общество; тези директиви вече са установили правната рамка на Общността в областта на личните данни и, следователно, не е необходимо този въпрос да бъде включван в настоящата директива, за да се гарантира безпрепятственото функциониране на вътрешния пазар, и по-специално свободното движение на лични данни между държавите членки; изпълнението и прилагането на настоящата директива следва да се осъществява в пълно съответствие с принципите за защита на личните данни, и по-специално във връзка

с непоръчани търговски съобщения и отговорността на посредниците; настоящата директива не може да предотврати анонимното използване на отворени мрежи като например Интернет.

(15) Конфиденциалността на съобщенията се гарантира от член 5 от Директива [97/66]; в съответствие с тази директива, държавите членки трябва да забраняват всякакъв вид засичания или контрол върху такива съобщения от други лица, освен от изпращачите и получателите, с изключение на случаите, когато това е разрешено от закона“.

9 Член 1 от Директива 2000/31 гласи следното:

„1. Настоящата директива има за цел да допринесе за нормалното функциониране на вътрешния пазар, като осигурява свободното движение на услуги на информационното общество между държавите членки.

2. Настоящата директива сближава, до степен, необходима за постигането на целта, посочена в параграф 1, определени национални разпоредби за услугите на информационното общество по отношение на вътрешния пазар, установяване на доставчиците на услуги, търговските съобщения, електронните договори, отговорността на посредниците, кодекси за поведение, извънсъдебно уреждане на спорове, средства за правна защита и сътрудничество между държавите членки.

3. Настоящата директива допълва правото на Общността, което е приложимо към услугите на информационното общество, без да се засяга степента на защита, и по-специално на общественото здраве и интересите на потребителите, както е установено от актовете на Общността и националното законодателство, доколкото това не ограничава свободата за предоставяне на услуги на информационното общество.

[…]

5. Настоящата директива не се прилага за:

[…]

б) въпроси, които се отнасят до услуги на информационното общество, които са предмет на Директиви [95/46] и [97/66];

[…]“.

10 Член 2 от Директива 2000/31 гласи следното:

„По смисъла на настоящата директива, следните термини означават:

а) „услуги на информационното общество“: услуги по смисъла на член 1, параграф 2 от Директива 98/34/ЕО [на Европейския парламент и на Съвета от 22 юни 1998 година за определяне на процедура за предоставяне на информация в областта на техническите стандарти и регламенти (ОВ L 204, 1998 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 23, стр. 207)], изменена с Директива 98/48/ЕО [на Европейския парламент и на Съвета от 20 юли 1998 година за изменение на Директива

98/34/ЕО относно определяне на процедура за предоставяне на информация в областта на техническите стандарти и правила ОВ L 217, 1998 г., стр. 18; Специално издание на български език, 2007 г., глава 13, том 23, стр. 282)];

[…]“.

11 Член 15 от Директива 2000/31 предвижда:

„1. Държавите членки не налагат общо задължение на доставчиците при предоставянето на услугите по членове 12, 13 и 14 да контролират информацията, която пренасят или съхраняват, нито общо задължение да търсят активно факти или обстоятелства за незаконна дейност.

2. Държавите членки могат да установят задължения за доставчиците на услуги на информационното общество за бързо информиране на компетентните публични органи за предполагаеми незаконни действия или информация, предоставена на получателите на техните услуги, или задължения за предаване на компетентните органи, по тяхно искане, на информация която позволява идентифицирането на получатели на техните услуги, с които те имат договори за съхраняване на данни“.

Директива 2002/21

12 Съгласно съображение 10 от Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно общата регулаторна рамка за електронните съобщителни 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):

„Определението „услуга на информационното общество“ в член 1 от Директива [98/34], се отнася за широк спектър от стопански дейности, които се извършват онлайн. Повечето от тези дейности не попадат в обхвата на действие на настоящата директива, защото те не се състоят изцяло или главно в пренасянето на сигнали на електронни съобщителни мрежи. Гласовата телефония и услугите за пренос по електронна поща са предмет на настоящата директива. Едно и също предприятие, например доставчик на интернет услуга, може да предлага както електронни съобщителни услуги, достъп до Интернет, така и услуги, които не се обхващат от настоящата директива, като осигуряване на поддържано в мрежата съдържание“.

13 Член 2 от Директива 2002/21 предвижда:

„За целите на настоящата директива:

[…]

в) „електронна съобщителна услуга“ означава услуга, осигурявана обикновено срещу заплащане, която се състои изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи, включително далекосъобщителни услуги и предавателни услуги в мрежи, използвани за разпръскване, но изключват услугите, осигуряващи или упражняващи редакторски контрол върху съдържанието, предавано посредством

електронни съобщителни мрежи и услуги; тя не включва услуги на информационното общество, както е определено в член 1 от Директива [98/34], които не се състоят изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи;

[…]“.

Директива 2002/58

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

„(2) Настоящата директива се стреми да зачита основните права и да спазва признатите принципи, по-специално от [Хартата]. По-специално настоящата директива се стреми да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от 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 [Съюза]. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 5, параграф 1 от настоящата директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право. Следователно, настоящата директива не засяга възможността на държавите членки да провеждат законно прихващане на електронни комуникации или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с Европейската конвенция за защита на човешките права и основните свободи [подписана в Рим на 4 ноември 1950 г.], съгласно тълкуването на решенията на Европейския съд за човешките права. Такива мерки трябва да бъдат уместни, строго пропорционални на предвидената цел и необходими в едно демократично общество, и следва да бъдат предмет на съответна защита в съответствие с Европейската конвенция за защита на човешките права и основните свободи.

[…]

(22) Забраната да се съхраняват съобщения и свързаните данни за трафик от лица, различни от потребителите, или без тяхното съгласие, не е насочено да забрани автоматично, междинно и временно съхранение на тази информация, доколкото това се прави с единствената цел осъществяване на предаване в електронни комуникационни мрежи и при условие че тази информация не се съхранява за период, по-дълъг от необходимия за предаване и за целите на ръководене на трафика, и че през периода на съхранение, конфиденциалният характер остава гарантиран. […]

[…]

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

[…]

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

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

„1. Настоящата директива предвижда да се хармонизират националните разпоредби, необходими за осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по отношение на обработката на лични данни в електронно съобщителния сектор[,] и да се осигури свободно движение на такива данни и оборудване за електронни съобщения и услуги в [Европейския съюз].

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

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

държавата, когато дейностите се отнасят до проблемите за сигурността на държавата) и дейностите на държавата в областта на наказателното право“.

16 Съгласно член 2 от Директива 2002/58, озаглавен „Дефиниции“:

„Освен ако не е предвидено друго, се прилагат дефинициите от Директива [95/46] и от Директива [2002/21].

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;

[…]“.

17 Член 3 от Директива 2002/58, озаглавен „Обхванати услуги“, предвижда:

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

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

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

[…]

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

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

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

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

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

[…]

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

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

„Когато данни за местонахождение, различни от данни за трафик, отнасящи се до потребители или абонати на публични комуникационни мрежи или публично достъпни електронни комуникационни услуги, могат да бъдат обработени, такива данни могат да бъдат обработени, само когато се направят анонимни или със съгласието на потребители или абонати до степен и продължителност необходими за предоставяне на услуга с добавена стойност. Доставчикът на

услуга трябва да информира потребители или абонати, преди да получи тяхното съгласие, за типа на данни за местонахождение, различни от данни за трафик, които ще бъдат обработени, за целите и за продължителността на обработката и дали данните ще бъдат предадени на трета страна с цел предоставяне на услуга с добавена стойност. […]“.

21 Член 15 от посочената директива, озаглавен „Приложение на някои разпоредби от Директива [95/46]“, гласи:

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

[…]

2. Разпоредбите на глава III относно средствата за съдебна защита, отговорността и санкциите от Директива [95/46] трябва да се прилагат по отношение на национални разпоредби, одобрени съгласно настоящата директива и по отношение на правата на личността, произтичащи от настоящата директива.

[…]“.

Регламент 2016/679

22 Съображение 10 от Регламент 2016/679 гласи:

„За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, нивото на защита на правата и свободите на физическите лица във връзка с обработването на такива данни следва да бъде равностойно във всички държави членки. Следва да се гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на основните права и свободи на физическите лица във връзка с обработването на лични данни. […]“.

23 Член 2 от този регламент гласи:

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

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

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

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

[…]

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

[…]

4. Настоящият регламент не засяга прилагането на Директива [2000/31], и по-специално разпоредбите относно отговорностите на междинните доставчици на услуги в членове 12—15 от посочената директива“.

24 Член 4 от посочения регламент предвижда:

„За целите на настоящия регламент:

1) „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

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

[…]“.

25 Член 5 от Регламент 2016/679 гласи:

„1. Личните данни са:

а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“);

в) подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);

д) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

[…]“.

26 Член 6 от този регламент гласи следното:

„1. Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

[…]

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

[…]

3. Основанието за обработването, посочено в параграф 1, букви в) и д), е установено от:

а) правото на Съюза или

б) правото на държавата членка, което се прилага спрямо администратора.

Целта на обработването се определя в това правно основание […]. Това правно основание може да включва конкретни разпоредби за адаптиране на прилагането на разпоредбите на

настоящия регламент, inter alia общите условия, които определят законосъобразността на обработването от администратора, видовете данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани лични данни, и целите, за които се разкриват; ограниченията по отношение на целите на разкриването; периодът на съхранение и операциите и процедурите за обработване, включително мерки за гарантиране на законосъобразното и добросъвестно обработване, като тези за други конкретни случаи на обработване съгласно предвиденото в глава IX. Правото на Съюза или правото на държавата членка се съобразява с обществения интерес и е пропорционално на преследваната легитимна цел.

[…]“.

27 Член 23 от посочения регламент предвижда:

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

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

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

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

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

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

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

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

й) изпълнението по гражданскоправни искове.

2. По-специално, всяка законодателна мярка, посочена в параграф 1, съдържа специални разпоредби най-малко, където е целесъобразно, по отношение на:

а) целите на обработването или категориите обработване;

б) категориите лични данни;

в) обхвата на въведените ограничения;

г) гаранциите за предотвратяване на злоупотреби или незаконен достъп или предаване;

д) спецификацията на администратора или категориите администратори;

е) периодите на съхранение и приложимите гаранции, като се вземат предвид естеството, обхватът и целите на обработването или категориите обработване;

ж) рисковете за правата и свободите на субектите на данни; и

з) правото на субектите на данни да бъдат информирани за ограничаването, освен ако това би било в разрез с целта на ограничаването“.

28 Съгласно член 79, параграф 1 от посочения регламент:

„Без да се засягат които и да било налични административни или несъдебни средства за защита, включително правото на подаване на жалба до надзорен орган съгласно член 77, всеки субект на данни има право на ефективна съдебна защита, когато счита, че правата му по настоящия регламент са били нарушени в резултат на обработване на личните му данни, което не е в съответствие с настоящия регламент“.

29 Съгласно член 94 от Регламент 2016/679:

„1. Директива [95/46] се отменя, считано от 25 май 2018 г.

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

30 Член 95 от този регламент гласи:

„Настоящият регламент не налага допълнителни задължения на физическите или юридическите лица по отношение на обработването във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Съюза, по отношение на въпроси, за които са им наложени специални задължения със същата цел, установени в Директива [2002/58]“.

Френското право

Code de la sécurité intérieure

31 Книга VIII от законодателната част на Code de la sécurité intérieure (Кодекс за вътрешната сигурност, наричан по-нататък „CSI“) предвижда в членове L. 801-1—L. 898-1 правила относно разузнаването.

32 [Член] L. 811-3 от CSI гласи:

„Специализираните разузнавателни служби могат да използват средствата за събиране на разузнавателна информация по дял V от настоящата книга единствено с цел изпълнение на възложените им задачи и за защитата и насърчаването на следните основни интереси на нацията:

1° националната независимост, териториалната цялост и националната отбрана;

2° основните интереси в областта на външната политика, изпълнението на европейските и международните задължения на Франция и предотвратяването на всяка форма на чуждестранна намеса;

3° важни икономически, промишлени и научни интереси на Франция;

4° предотвратяването на тероризма;

5° предотвратяването на:
a) посегателства върху републиканската форма на институциите;
b) действия за поддържане или възстановяване на организации, разтурени съгласно член L. 212-1;
c) актове на колективно насилие, които могат сериозно да засегнат обществения мир;

6° предотвратяването на престъпността и на организираната престъпност;

7° предотвратяването на разпространението на оръжия за масово унищожение“.

33 Член L. 811-4 от CSI гласи:

„С декрет на Conseil d'État [Държавен съвет], приет след становище на Commission nationale de contrôle des techniques de renseignement [Национална комисия за контрол на разузнавателните средства], се определят службите, различни от специализираните разузнавателни служби, към министрите на отбраната, на вътрешните работи и на правосъдието, както и към министрите, отговарящи за икономиката, бюджета или митниците, които могат да използват средства по дял V от настоящата книга при условията, предвидени в нея. За всяка от службите в декрета се посочват целите по член L. 811-3 и средствата, за които може да бъде дадено разрешение“.

34 В член L. 821-1, първа алинея от CSI е посочено следното:

„За използването на територията на страната на средствата за събиране на разузнавателна информация по глави I—IV, дял V от настоящата книга се изисква предварително разрешение

от министър-председателя, издадено след становище на Националната комисия за контрол на разузнавателните средства“.

35 Член L. 821-2 CSI предвижда:

„Разрешението по член L. 821-1 се издава по мотивирано писмено искане на министъра на отбраната, министъра на вътрешните работи, министъра на правосъдието или на министрите, отговарящи за икономиката, бюджета или митниците. Всеки министър може да делегира това правомощие индивидуално само на преки сътрудници, които имат достъп до информация, класифицирана като поверителна от гледна точка на националната отбрана.

В искането се посочват:

1° средството или средствата, които трябва да се използват;

2° службата, за която се подава искането;

3° преследваната цел/цели;

4° основанията за мерките;

5° срокът на действие на разрешението;

6° лицето/лицата, мястото/местата или превозните средства, предмет на искането.

За изпълнението на [точка] 6 лицата, чиято самоличност е неизвестна, могат да бъдат определени чрез техните идентификатори или качество, а местата или превозните средства могат да бъдат определени чрез посочване на лицата, за които се отнася искането.

[…]“.

36 Съгласно член L. 821-3, първа алинея от CSI:

„Искането се съобщава на председателя или при невъзможност — на един от посочените в член L. 831-1, [точки] 2 и 3 членове на Националната комисия за контрол на разузнавателните средства, който в срок от 24 часа представя на министър-председателя писмено становище. Ако искането се разглежда от ограничен състав или от пленума на комисията, министър-председателят незабавно бива уведомен за това, а становището се издава в срок от 72 часа“.

37 Член L. 821-4 от CSI гласи:

„Разрешението за използване на разузнавателните средства по глави I—IV, дял V от настоящата книга се издава от министър-председателя за период не по-дълъг от четири месеца. […] Разрешението съдържа основанията и данните, предвидени в член L. 821-2, точки 1—6. Разрешението се подновява при условията, предвидени в настоящата глава.

Когато разрешението е издадено след отрицателно становище на Националната комисия за контрол на разузнавателните средства, в него се посочват мотивите, поради които това становище не е възприето.

[…]“.

38 Член L. 833-4 от CSI, който се намира в глава III от този дял, гласи:

„По собствена инициатива или по административна жалба от лице, което желае да провери дали спрямо него е използвано неправомерно разузнавателно средство, комисията извършва проверка на посоченото средство или средства, за да установи дали са използвани или се използват в съответствие с настоящата книга. Комисията уведомява подателя на жалбата, че е извършила необходимите проверки, без да потвърждава или да опровергава използването на средствата“.

39 Член L. 841-1, първа и втора алинея от CSI гласи следното:

„Държавният съвет е компетентен да разглежда жалби за използването на разузнавателните средства по дял V от настоящата книга при условията, предвидени в глава III bis, дял VII, книга VII от Административнопроцесуалния кодекс, и при спазване на специалните разпоредби на член L. 854-9 от настоящия кодекс.

Той може да бъде сезиран от:

1° всяко лице, което желае да провери дали спрямо него е използвано неправомерно разузнавателно средство и което излага мотиви за предварителното прилагане на предвидената в член L. 833-4 процедура;

2° Националната комисия за контрол на разузнавателните средства — при условията, предвидени в член L. 833-8“.

40 Намиращият се в книга VIII от законодателната част на CSI дял V относно „Средства за събиране на разузнавателна информация, за които се изисква разрешение“ съдържа по-специално глава I, озаглавена „Административен достъп до данни за свързване“, която съдържа членове L. 851-1—L. 851-7 от CSI.

41 Член L. 851-1 от CSI гласи:

„При условията, предвидени в глава I от дял II от настоящата книга, може да се разреши събирането от операторите на електронни съобщителни услуги и от лицата по член L. 34-1 от [CPCE], както и от лицата по член 6, [параграф] I, [точки] 1 и 2 от Loi no 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique [Закон № 2004-575 от 21 юни 2004 г. за доверието в цифровата икономика] [(JORF от 22 юни 2004 г., стр. 11168)] на информация или документи, обработвани или съхранявани от техните електронни съобщителни мрежи или услуги, включително технически данни за идентифицирането на абонатните номера или номерата за свързване с електронни съобщителни услуги, за установяването на абонатните номера или номерата за свързване на дадено лице, за установяването на местонахождението на използваните крайни устройства, както и за съобщенията на даден абонат, отнасящи се до списъка на изходящите и входящите номера, продължителността и датата на съобщенията.

По изключение от член L. 821-2 мотивираните писмени искания относно техническите данни за установяването на абонатните номера или на номерата за свързване с електронни съобщителни услуги или за установяването на всички абонатни номера или номера за свързване на дадено лице се предават директно на Националната комисия за контрол на разузнавателните средства от индивидуално определените и оправомощени служители на разузнавателните служби,

посочени в членове L. 811-2 и L. 811-4. Комисията дава становището си при условията, предвидени в член L. 821-3.

Подчинена на министър-председателя служба отговаря за събирането на информацията или документите от операторите и лицата, посочени в първа алинея на настоящия член. Националната комисия за контрол на разузнавателните средства разполага с постоянен, пълен, пряк и незабавен достъп до събраната информация или документи.

Редът и условията за прилагане на настоящия член се определят с декрет на Държавния съвет, приет след становище на Националната комисия по информационните технологии и свободите и на Националната комисия за контрол на разузнавателните средства“.

42 Член L. 851-2 от CSI гласи:

„I. – При условията, предвидени в глава I от дял II от настоящата книга, и единствено с цел предотвратяването на тероризма, за всеки конкретен случай може да бъде издадено разрешение за събирането в реално време в мрежите на операторите и лицата, посочени в член L. 851-1, на информацията или документите, посочени в същия член L. 851-1, относно лице, за което преди това е установено, че може да има връзка със заплаха. Когато са налице сериозни основания да се счита, че едно или повече лица от обкръжението на лицето, за което се отнася разрешението, могат да предоставят данни, свързани с целта, за която то е издадено, разрешението може също да бъде предоставено за всяко от тези лица поотделно.

I bis. – Максималният брой на едновременно издадените съгласно настоящия член разрешения се определя от министър-председателя след становище на Националната комисия за контрол на разузнавателните средства. Решението за определяне на максималния брой разрешения и разпределението им между министрите, посочени в член L. 821-2, първа алинея, както и броят на издадените разрешения за прихващане се съобщават на комисията.

[…]“.

43 Член L. 851—3 от CSI предвижда:

„I. – При условията, предвидени в глава I от дял II от настоящата книга, и единствено с цел предотвратяването на тероризма, от операторите и лицата, посочени в член L. 851-1, може да се изисква да извършват в мрежите си дейности по автоматизирано обработване, предназначени — съгласно уточнени в разрешението параметри — да разкриват случаи на свързване, които могат да имат отношение към терористична заплаха.

Това автоматизирано обработване може да използва единствено посочените в член L. 851-1 информация или документи, без да се събират други данни, които не отговарят на заложените критерии, и без да се допуска установяването на самоличността на лицата, за които се отнасят информацията или документите.

В разрешението на министър-председателя се посочва техническият обхват на обработването, което трябва да се извърши, при спазване на принципа на пропорционалност.

II. – Националната комисия за контрол на разузнавателните средства дава становище по искането за разрешение за автоматизираното обработване и по определените параметри за разкриване на данни. Тя има постоянен, пълен и пряк достъп до обработването, както и до събраната информация и данни. Всички промени в данните и параметрите се съобщават на комисията, която може да дава препоръки.

Първоначалното разрешение за извършване на автоматизираното обработване, предвидено в [параграф] I от настоящия член, се издава за период от два месеца. Разрешението може да бъде подновено при спазването на условията относно периода на действие, предвидени в глава I от дял II от настоящата книга. Искането за подновяване съдържа справка за броя на идентификаторите, засечени в резултат на автоматизираното обработване, и анализ на релевантността на засечените данни.

III. – Условията, предвидени в член L. 871-6, се прилагат по отношение на извършените при автоматизираното обработване фактически действия от операторите и лицата, посочени в член L. 851-1.

IV. – Когато операциите по обработка по [параграф] I от настоящия член открият данни за наличието на заплаха с терористичен характер, министър-председателят или упълномощено от него лице, след становище на Националната комисия за контрол на разузнавателните средства и при условията, предвидени в глава I, от дял II от настоящата книга, може да разреши установяването на самоличността на съответното лице или лица и събирането на свързаните с това данни. Тези данни се използват в срок от 60 дни от събирането им и се унищожават след изтичането на този срок, освен в случай на сериозни доказателства за наличието на терористична заплаха, свързана с едно или повече от засегнатите лица.

[…]“.

44 Член L. 851-4 от CSI гласи следното:

„При условията, предвидени в глава I от дял II от настоящата книга, техническите данни относно местонахождението на използваните крайни устройства, посочени в член L. 851-1, могат да бъдат събрани от мрежата при искане и да бъдат предавани в реално време от операторите на подчинена на министър-председателя служба“.

45 Член R. 851-5 от CSI, който се съдържа в подзаконовата част на този кодекс, предвижда:

„I. – Посочените в член L. 851-1 информация или документи, с изключение на съдържанието на разменената кореспонденция или на прегледаната информация, са:

1° изброените в членове R. 10-13 и R. 10-14 от [CPCE] и в член 1 от Декрет [№ 2011-219];

2° технически данни, различни от посочените в [точка] 1, които:

a) позволяват установяването на местонахождението на крайното устройство;

b) са свързани с достъпа на крайните устройства до обществените съобщителни мрежи или услуги в интернет;

c) са свързани с пренасяне на електронни съобщения чрез мрежите;

d) са свързани установяването и удостоверяването на самоличността на потребител, на връзка, на обществена съобщителна мрежа или услуга в интернет;

e) се отнасят до характеристиките на крайните устройства и до данните за конфигурацията на техния софтуер.

II. – В изпълнение на член L. 851-1 могат да бъдат събрани единствено информацията и документите, посочени в [параграф] I, [точка] 1. Това събиране се извършва отложено във времето.

Посочената в [параграф] I, [точка] 2 информация може да бъде събрана единствено съгласно членове L. 851-2 и L. 851-3, при предвидените в тях условия и ограничения и при спазването на член R. 851-9“.

CPCE

46 Член L. 34-1 от CPCE гласи:

„I. – Настоящият член се прилага при обработката на лични данни във връзка с предоставянето на публично достъпни електронни съобщителни услуги; по-специално той се прилага спрямо мрежи, поддържащи събиране на данни и устройства за идентификация.

II. – Операторите на електронни съобщителни услуги, и по-специално лицата, чиято дейност се състои в предоставяне на достъп до обществени съобщителни услуги в интернет, изтриват или правят анонимни всички данни за трафика, без да се накърняват параграфи III, IV, V и VI.

Лицата, които предоставят обществени електронни съобщителни услуги, предвиждат в съответствие с предходната алинея вътрешни процедури, позволяващи им да изпълняват исканията на компетентните органи.

Лицата, чиято основна или допълнителна професионална дейност се изразява в публично осигуряване на свързаност, позволяваща съобщения в интернет посредством достъп до мрежата, дори без заплащане, са длъжни да изпълняват разпоредбите, приложими спрямо операторите на електронни съобщителни услуги съгласно настоящия член.

III. – За целите на разследването, разкриването и наказателното преследване на престъпления или на неизпълнението на задължението по член L. 336-3 от Code de la propriété intellectuelle [Кодекс на интелектуалната собственост] или с оглед на предотвратяването на посегателствата върху системите за автоматизирана обработка на данни, предвидени и санкционирани в членове 323-1—323-3-1 от Наказателния кодекс, и с единствената цел да се направи възможно евентуално предоставяне на съда или на висшия орган по член L. 331-12 от Кодекса на интелектуалната собственост или на националния орган относно сигурността на информационните системи, посочен в член L. 2321-1 от Code de la défense [Кодекс на отбраната], могат да се отложат за максимален период от една година действията, целящи изтриването или анонимизирането на определени категории технически данни. С декрет на Държавния съвет, приет след получаване на становището на Националната комисия по информационните технологии и свободите, се определят — в границите, установени в [параграф] VI — категориите данни и продължителността на тяхното запазване в зависимост от дейността на операторите и от естеството на съобщенията, както и евентуалното обезщетяване за установимите и специфични допълнителни разходи за услугите, предоставяни от операторите в това отношение по искане на държавата.

[…]

VI. – Данните, които са запазвани и обработвани при условията, определени в [параграфи] III, IV и V, се отнасят изключително до идентифицирането на потребителите на услугите, предоставяни от операторите, до техническите характеристики на съобщенията, осигурявани от последните, и до установяването на местоположението на крайните устройства.

Те не могат в никакъв случай да се отнасят до съдържанието на разменените съобщения или до консултираната информация, под каквато и да е форма, в рамките на съответната комуникация.

Запазването и обработването на тези данни се извършва при спазване на разпоредбите на Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Закон № 78-17 от 6 януари 1978 г. за информационните технологии, компютърните файлове и гражданските свободи].

Операторите приемат всички мерки, за да попречат на използването на тези данни за цели, различни от предвидените в настоящия член".

47 Член R. 10-13 от CPCE гласи следното:

„I. – В изпълнение на член L. 34-1, [параграф] III, за целите на разследването, разкриването и наказателното преследване на престъпления операторите на електронни съобщения трябва да запазват следните данни:

a) данните, позволяващи идентифицирането на потребителя;

b) данните относно използваните крайни устройства за комуникация;

c) техническите характеристики, както и датата, часа и продължителността на всяко съобщение;

d) данните относно поисканите или използваните допълнителни услуги и техните доставчици;

e) данните, които позволяват идентифицирането на получателя или получателите на съобщението.

II. – За дейностите, свързани с телефония, операторът трябва да запазва посочените в [параграф] II данни, както и данни, които позволяват да се установи източникът и местонахождението на съобщението.

III. – Периодът на запазване на посочените в настоящия член данни е една година, считано от деня на записването им.

IV. – Установимите и специфични допълнителни разходи, направени от операторите в изпълнение на разпореждане на съдебните органи за предоставянето на посочените в настоящия член категории данни, се възстановяват съгласно условията, предвидени в член R. 213-1 от Наказателно-процесуалния кодекс".

48 Член R. 10-14 от CPCE предвижда:

„I. – В изпълнение на член L. 34-1, [параграф] IV операторите на електронни съобщения имат право да съхраняват за нуждите на операциите по фактуриране и плащане данните с технически характер, позволяващи идентифицирането на потребителя, както и посочените в член R. 10-13, [параграф] I, [букви] b, c) и d) данни.

II. – За дейностите, свързани с телефония, операторите трябва да запазват освен посочените в [параграф] I данни, и техническите данни относно местонахождението на съобщението, относно идентифицирането на получателя или получателите на съобщението и данните, позволяващи изготвянето на фактури.

III. – Посочените в [параграфи] I и II от настоящия член данни, могат да бъдат запазени само ако са необходими за изготвянето на фактури и плащането на предоставените услуги. Тяхното запазване трябва да се ограничи до периода от време, който е строго необходим за постигането на тази цел, но не повече от една година.

IV. – За сигурността на мрежите и съоръженията операторите могат да запазват за период не по-дълъг от три месеца:

a) данни, позволяващи да се установи източникът на съобщението;

b) техническите характеристики, както и датата, часа и продължителността на всяко съобщение;

c) данните, които позволяват идентифицирането на получателя или получателите на съобщението;

d) данните относно поисканите или използваните допълнителни услуги и техните доставчици“.

Закон № 2004-575 от 21 юни 2004 г. за доверието в цифровата икономика

49 Член 6, от Loi no 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (Закон № 2004-575 от 21 юни 2004 г. за доверието в цифровата икономика) (JORF от 22 юни 2004 г., стр. 11168, наричан по-нататък „LCEN“) предвижда:

„I. – 1. Лицата, чиято дейност се състои в предоставяне на достъп до обществени съобщителни услуги в интернет, уведомяват абонатите си за наличието на технически средства, позволяващи да се ограничи достъпът до някои услуги или те да се подберат, и им предлагат най-малко едно от тези средства.

[…]

2. Физическите и юридическите лица, които осигуряват — дори без заплащане и за целите на публичното им предоставяне посредством обществени съобщителни услуги в интернет — съхранението на предоставени от получателите на тези услуги сигнали, текстове, изображения, звуци или съобщения от всякакво естество, не носят гражданска отговорност за действията и информацията, които се съхраняват по искане на получател на тези услуги, ако действително не са знаели за незаконния им характер или за фактите или за обстоятелствата, позволяващи да се установи този характер, или ако веднага след като са узнали за това, са предприели незабавни действия да премахнат тези данни или да блокират достъпа до тях.

[…]

II. – Посочените в [параграф] I, [точки] 1 и 2 лица задържат и запазват данните, годни да позволят идентифицирането на всяко лице, допринесло за създаването на съдържанието или на част от съдържанието на предоставяните от тях услуги.

Те предоставят на лицата, които публикуват обществена съобщителна услуга в интернет, технически средства, позволяващи им да изпълнят условията за идентификация, предвидени в [параграф] III.

Съдът може да поиска от доставчиците по [параграф] I, [точки] 1 и 2 да му съобщят данните по първа алинея.

За обработването на тези данни се прилагат разпоредбите на членове 226-17, 226-21 и 226-22 от Наказателния кодекс.

С декрет на Държавния съвет, приет след становище на Националната комисия по информационните технологии и свободите, се определят данните по първа алинея и продължителността и условията за тяхното запазване.

[…]“.

Декрет № 2011-219

50 Глава I от Декрет № 2011-219, приета на основание член 6, [параграф] II, последна алинея от LCEN, съдържа членове 1—4 от този декрет.

51 Член 1 от Декрет № 2011-219 гласи:

„Посочените в член 6 от [LCEN] данни, които лицата са длъжни да съхраняват по силата на тази разпоредба, са следните:

1° лицата, посочени в [параграф] I, [точка] 1 от същия член — за всяко свързване на техните абонати съхраняват:

a) идентификатора на свързването;

b) идентификатора на абоната, даден от тези лица;

c) идентификатора на крайното устройство, използвано за свързването, когато те имат достъп до него;

d) дата и час на началото и на края на свързването;

e) характеристиките на абонатната линия;

2° лицата, посочени в [параграф] I, [точка] 2 от същия член — за всяко действие по създаване съхраняват:

a) идентификатора на свързването, стоящо в основата на съобщението;

b) определения от информационната система идентификатор на съдържанието, за което се отнася действието;

c) видовете протоколи, използвани за свързването към услугата и за прехвърлянето на съдържанието;

d) естеството на действието;

e) дата и час на действието;

f) идентификатора, използван от лицето, извършващо действието, когато последното е предоставило такъв;

3° лицата, посочени в [параграф] I, [точки] 1 и 2 от същия член, съхраняват следните данни, предоставени от потребителя при сключването на договор или при създаването на профил:

a) идентификатора на свързването при създаването на профила;

b) фамилно име и собствено(и) име(на) или наименование;

c) свързаните пощенски адреси;

d) използваните псевдоними;

e) свързаните адреси за електронна поща или адреси на профил;

f) телефонните номера;

g) паролата и данните, позволяващи същата да бъде проверена или изменена, в тяхната актуална версия;

4° лицата, посочени в [параграф] I, [точки] 1 и 2 от същия член, когато сключването на договор или създаването на профил се заплаща, за всяка платежна операция съхраняват следните данни относно плащането:

a) вид на плащането;

b) референция на плащането;

c) сума;

d) дата и час на трансакцията.

Посочените в [точки] 3 и 4 данни трябва да се съхраняват само ако лицата обичайно ги събират“.

52 Член 2 от този декрет гласи следното:

„Приносът към създаването на съдържание включва действията, отнасящи се до:

a) първоначално създаване на съдържание;

b) изменения на съдържанието и на данните, свързани с него;

c) премахване на съдържанието“.

53 Член 3 от посочения декрет предвижда:

„Периодът на запазване на посочените в член 1 данни е една година:

a) по отношение посочените в [точки] 1 и 2 данни — считано от деня на създаването на съдържанието, за всяко действие, допринасящо за създаването на съдържание по смисъла на член 2;

b) по отношение на посочените в [точка] 3 данни — считано от датата на прекратяване на договора или от закриването на профила;

c) по отношение на посочените в [точка] 4 данни — считано от датата на издаване на фактурата или на платежната операция, за всяка фактура или платежна операция“.

Белгийско право

54 Законът от 29 май 2016 г. изменя по-специално Loi du 13 juin 2005 relative aux communications électroniques (Закон от 13 юни 2005 г. за електронните съобщения) (Moniteur belge от 20 юни 2005 г., стр. 28070, наричан по-нататък „Законът от 13 юни 2005 г.“), Code d'instruction criminelle (Кодекс за наказателно разследване) и Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Закон от 30 ноември 1998 г. за устройството на службите за разузнаване и сигурност) (Moniteur belge от 18 декември 1998 г., стр. 40312, наричан по-нататък „Законът от 30 ноември 1998 г.“).

55 Член 126 от Закона от 13 юни 2005 г., в редакцията му съгласно Закона от 29 май 2016 г., гласи:

„§ 1. Без да се засяга Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [Закон от 8 декември 1992 г. относно защитата на правото на неприкосновеност на личния живот при обработването на лични данни], доставчиците на обществени телефонни услуги, включително в интернет, на достъп до интернет, на електронна поща в интернет, операторите, предоставящи обществени електронни съобщителни мрежи, и операторите, предоставящи една от тези услуги, запазват данните, посочени в параграф 3, които се генерират или обработват от тях при предоставянето на съответните съобщителни услуги.

Настоящият член не се отнася до съдържанието на съобщенията.

Задължението за запазване на данните, посочени в параграф 3, се прилага и по отношение на неуспешните опити за повикване, при условие че в рамките на предоставяне на съответните съобщителни услуги тези данни са:

1° по отношение на данните за телефонните разговори, създадени или обработени от операторите на обществено достъпни електронни съобщителни услуги или на обществени електронни съобщителни мрежи или

2° що се отнася до данните от интернет, записани от тези доставчици.

§ 2. Само следните органи при поискване могат да получат от доставчиците и операторите, посочени в параграф 1, първа алинея, данните, запазени съгласно настоящия член, за целите и при условията, посочени по-долу:

1° съдебните органи — с цел разкриване, разследване и наказателно преследване на престъпления, за изпълнение на мерките, посочени в членове 46bis и 88bis от Code d'instruction criminelle [Наказателно-процесуален кодекс], и при условията, предвидени в тези членове;

2° службите за разузнаване и сигурност — за изпълнение на разузнавателни мисии чрез използване на методите за събиране на данни, посочени в членове 16/2, 18/7 и 18/8 от Loi du 30 novembre 1998 organique des services de renseignement et de Sécurité [Устройствен закон от 30 ноември 1998 г. относно службите за разузнаване и сигурност] и при условията, установени в настоящия закон;

3° всеки полицейски служител на [Institut belge des services postaux et des télécommunications (Белгийски институт за пощенски услуги и телекомуникации)] — с цел разкриване, разследване и наказателно преследване на нарушенията на членове 114, 124 и на настоящия член;

4° службите за спешна помощ, предлагащи помощ на място, когато след спешно повикване не получат от доставчика или от съответния оператор идентификационните данни на лицето, осъществяващо повикването, въз основа на данните, посочени в член 107, параграф 2, алинея 3, или получат непълни или неточни данни. Могат да бъдат изискани единствено идентификационните данни на лицето, извършващо повикването, при това не по-късно от 24 часа след повикването;

5° полицейските служители от отдела за безследно изчезнали лица на федералната полиция — в рамките на мисията им за подпомагане на лица в опасност, търсене на лица, чието изчезване буди безпокойство, и когато има сериозни съмнения или улики, че физическата неприкосновеност на изчезналото лице е в непосредствена опасност. Единствено данните, посочени в параграф 3, първа и втора алинея, отнасящи се до изчезналото лице и запазени през 48-те часа, предхождащи искането за получаване на данните, могат да бъдат изискани от оператора или от съответния доставчик посредством определена от краля полицейска служба;

6° службата по медиация за далекосъобщенията — с цел идентифициране на лица, злоупотребили с електронна съобщителна мрежа или услуга съгласно условията, посочени в член 43bis, параграф 3, [точка] 7 от Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [Закон от 21 март 1991 г. за преструктуриране на определени публични икономически предприятия]. Могат да бъдат изискани единствено идентификационни данни.

Доставчиците и операторите, посочени в параграф 1, първа алинея, гарантират, че достъпът от Белгия на посочените в параграф 3 данни е неограничен и че тези данни и всяка друга необходима информация относно тези данни могат да бъдат предоставени незабавно и само на органите, посочени в настоящия параграф.

Без да се засягат други правни разпоредби, доставчиците и операторите, посочени в параграф 1, първа алинея, не могат да използват запазваните съгласно параграф 3 данни за други цели.

§ 3. Данните, предназначени за идентифициране на ползвателя или абоната и на средствата за комуникация, с изключение на данните, специално предвидени във втора и трета алинея, се запазват в продължение на дванадесет месеца от датата, от която за последен път е възможно съобщение с помощта на използваната услуга.

Данните, свързани с достъпа и връзката на крайното оборудване с мрежата и услугата и с местонахождението на това оборудване, включително крайната точка на мрежата, се запазват в продължение на дванадесет месеца от датата на съобщението.

Данните от съобщения, с изключение на съдържанието, включително техният източник и тяхното местоназначение, се запазват за период от дванадесет месеца от датата на съобщението.

С кралски декрет, обсъден от Министерския съвет, по предложение на министъра на правосъдието и министъра [компетентен по въпросите на електронните съобщенията] и след становище на Комисията за защита на неприкосновеността на личния живот и на Института, Кралят определя данните, които трябва да се запазят, що се отнася до всяка от категориите, посочени в първа, втора и трета алинея, както и изискванията, на които трябва да отговарят тези данни.

[…]“.

Споровете в главните производства и преюдициалните въпроси

Дело C-511/18

56 С жалби, подадени на 30 ноември 2015 г. и на 16 март 2016 г., съединени в главното производство, La Quadrature du Net, French Data Network, Fédération des fournisseurs d’accès à internet associatifs и Igwan.net искат от Държавния съвет (Франция) да отмени Декрети №№ 2015-1185, 2015-1211, 2015-1639 и 2016-67, тъй като по-специално те нарушават Конституцията на Франция, Европейската конвенция за защита на правата на човека и основните свободи (наричана по-нататък „ЕКПЧ“) и директиви 2000/31 и 2002/58 във връзка с членове 7, 8 и 47 от Хартата.

57 Що се отнася по-специално до правните основания, изведени от неспазването на Директива 2000/31, запитващата юрисдикция отбелязва, че разпоредбите на член L. 851-3 от CSI задължават операторите на електронни съобщения и техническите доставчици „да извършват в мрежите си дейности по автоматизирано обработване, предназначени — съгласно уточнени в разрешението параметри — да разкриват случаи на свързване, които могат да имат отношение към терористична заплаха“. Това техническо средство имало за цел единствено ограничено във времето събиране, измежду всички данни за свързване,

обработвани от тези оператори и доставчици, на онези данни за свързване, които може имат връзка с тежко престъпление. При тези условия посочените разпоредби, които не налагали общо задължение за активно наблюдение, не нарушавали член 15 от Директива 2000/31.

58 Що се отнася до основанията, изведени от неспазването на Директива 2002/58, запитващата юрисдикция счита, че от разпоредбите на тази директива, както и от решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, наричано по-нататък „решение Tele2“, EU:C:2016:970) следва по-специално, че националните разпоредби, които налагат задължения на доставчиците на електронни съобщителни услуги — като задължението за общо и неизбирателно запазване на данни за трафик и на данни за местонахождение на техните потребители и абонати за посочените в член 15, параграф 1 от Директивата цели, сред които е и гарантирането на национална сигурност, отбраната и обществена безопасност — попадат в приложното поле на посочената директива, тъй като тези правила уреждат дейността на въпросните доставчици. Същото се отнасяло и за законодателството, уреждащо достъпа на националните органи до данните и тяхното използване.

59 Оттук запитващата юрисдикция прави извода, че в приложното поле на Директива 2002/58 попадат както задължението за запазване, произтичащо от член L. 851-1 от CSI, така и административният достъп до посочените данни, включително достъпът в реално време, предвидени в членове L. 851-1, L. 851-2 и L. 851-4 от кодекса. Според тази юрисдикция същото важи и за разпоредбите на член L. 851-3 от кодекса, които, макар да не налагат на съответните оператори общо задължение за запазване, все пак ги задължават да използват в мрежите си средства за автоматизирана обработка, предназначени да откриват случаи на свързване, които може да показват терористична заплаха.

60 Обратно, тази юрисдикция счита, че посочените в исканията за отмяна разпоредби на CSI, отнасящи се до използваните пряко от държавата средства за събиране на разузнавателна информация, без да уреждат дейността на доставчиците на електронни съобщителни услуги, като им налагат специфични задължения, не попадат в приложното поле на Директива 2002/58. Следователно тези разпоредби не могат да се разглеждат като разпоредби, прилагащи правото на Съюза, поради което изтъкнатите срещу тях твърдения за нарушения на Директива 2002/58, не могат да бъдат приети.

61 Така, с оглед на решаването на споровете относно законосъобразността на декрети № 2015-1185, № 2015-1211, № 2015-1639 и № 2016-67 от гледна точка на Директива 2002/58, доколкото те са приети за прилагането на членове L. 851-1—L. 851-4 от CSI, се поставяли три въпроса за тълкуване на правото на Съюза.

62 Относно тълкуването на член 15, параграф 1 от Директива 2002/58 запитващата юрисдикция иска да се установи, на първо място, дали задължението за общо и неизбирателно запазване, наложено на доставчиците на електронни съобщителни услуги на основание членове L. 851-1 и R. 851-5 от CSI, не трябва да се разглежда — по-специално с оглед гаранциите и проверките, предвидени по отношение на административния достъп до данните за свързване и на тяхното използване — като намеса, обоснована с правото на сигурност, гарантирано в член 6 от Хартата, и с изискванията на националната сигурност, отговорността за която носят единствено държавите членки по силата на член 4 ДЕС.

63 На второ място, що се отнася до другите задължения, които могат да бъдат наложени на доставчиците на електронни съобщителни услуги, запитващата юрисдикция отбелязва, че разпоредбите на член L. 851-2 от CSI разрешават събирането от същите лица на информация или документи, предвидени в член L. 851-1 от този кодекс, единствено за целите на предотвратяването на тероризма. Това събиране, което засягало само едно или няколко лица, за които преди това е установено, че може да са свързани с терористична заплаха, се осъществявало в реално време. Същото се отнасяло и за разпоредбите на член L. 851-4 от посочения кодекс, които разрешават операторите да предават в реално време само техническите данни за установяване на местонахождението на крайните устройства. Тези техники регулирали административния достъп в реално време до запазените данни за различни цели и съгласно различни ред и условия съгласно CPCE и LCEN, без обаче да налагат на засегнатите доставчици изискване за допълнително запазване, извън това, което е необходимо за фактурирането и предоставянето на техните услуги. Освен това разпоредбите на член L. 851-3 от CSI, които предвиждат задължение за доставчиците на услуги да извършват в своите мрежи автоматизиран анализ на връзките, също не налагали задължение за общо и неизбирателно запазване.

64 От една страна обаче, запитващата юрисдикция счита, че както общото и неизбирателно запазване, така и достъпът в реално време до данни за свързване, в условията на сериозни и постоянни заплахи за националната сигурност, свързани по-специално с риска от тероризъм, са изключително полезни от оперативна гледна точка. Всъщност общото и неизбирателно запазване позволявало на разузнавателните служби да получат достъп до данните за съобщенията, преди да се установят причините, поради които се счита, че съответното лице представлява заплаха за обществената сигурност, отбраната или държавната сигурност. Освен това достъпът в реално време до данни за свързване позволявал проследяване и незабавна реакция на действията на лица, които могат да представляват непосредствена заплаха за обществения ред.

65 От друга страна, предвиденото в член L. 851-3 от CSI средство позволявало въз основа на определени конкретно за тази цел критерии да се засекат лицата, чиито действия, по-специално предвид използваните от тях съобщителни средства, могат да имат отношение към терористична заплаха.

66 На трето място, що се отнася до достъпа на компетентните органи до запазените данни, запитващата юрисдикция иска да се установи дали Директива 2002/58, разглеждана във връзка с Хартата, трябва да се тълкува в смисъл, че за да са законосъобразни производствата за събиране на данни за свързване, във всички случаи трябва да е изпълнено изискването да се информират засегнатите лица, когато такава информация вече не може да попречи на водените от компетентните органи разследвания, или такива производства могат да се разглеждат като законосъобразни с оглед на всички останали предвидени в националното право процесуални гаранции, доколкото последните осигуряват ефективността на правото на обжалване.

67 Относно тези други процесуални гаранции запитващата юрисдикция уточнява по-специално, че всяко лице, което желае да провери за евентуално неправомерно използване на разузнавателни средства спрямо него, може да сезира специализиран съд към Държавния съвет, компетентен да извърши проверка с оглед на доказателствата, които са му представени извън състезателното производство, дали спрямо жалбоподателя е приложено такова средство и дали то е използвано в съответствие с книга VIII от CSI. Предоставените на специализирания съд правомощия да провежда разследвания по

жалбите, гарантирали ефективността на упражнявания от него съдебен контрол. В този смисъл той бил компетентен при провеждането на разследвания по жалбите да установява служебно всички констатирани незаконосъобразни действия и да разпорежда на администрацията да вземе всички подходящи мерки за отстраняването на констатираните нарушения. Освен това Националната комисия за контрол на разузнавателните средства била компетентна да осъществи проверка дали тези средства за събиране на разузнавателна информация са използвани на територията на страната в съответствие с изискванията на CSI. Така обстоятелството, че разглежданите в главното производство разпоредби на закона не предвиждат засегнатите лица да бъдат уведомявани за приложените спрямо тях мерки за наблюдение, не представлявало само по себе си прекомерно накърняване на правото на зачитане на личния живот.

68 При тези условия Conseil d'État (Държавен съвет, Франция) решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) Трябва ли задължението за общо и неизбирателно запазване, наложено на доставчиците на основание на разрешителните разпоредби на член 15, параграф 1 от Директива [2002/58], да се разглежда — в условията на сериозни и постоянни заплахи за националната сигурност, свързани по-специално с риска от тероризъм — като намеса, обоснована с правото на сигурност, гарантирано в член 6 от [Хартата], и с изискванията на националната сигурност, отговорността за която е единствено на държавите членки по силата на член 4 [ДЕС]?

2) Трябва ли Директива [2002/58], разглеждана във връзка с [Хартата], да се тълкува в смисъл, че разрешава законодателни мерки — като мерките за събиране в реално време на данни за трафика и за местонахождението на определени лица — които, макар да засягат правата и задълженията на доставчиците на електронна съобщителна услуга, не им налагат специфично задължение за запазване на техните данни?

3) Трябва ли Директива [2002/58], разглеждана във връзка с [Хартата], да се тълкува в смисъл, че за да са законосъобразни производствата за събиране на данни за свързване, във всички случаи трябва да е изпълнено изискването да се информират засегнатите лица, когато такава информация вече не може да попречи на водените от компетентните органи разследвания, или такива производства могат да се считат за законосъобразни с оглед на всички останали съществуващи процесуални гаранции, доколкото последните осигуряват ефективността на правото на обжалване?“.

Дело C-512/18

69 С жалба, подадена на 1 септември 2015 г., French Data Network, La Quadrature du Net и Fédération des fournisseurs d'accès à Internet associatifs сезират Държавния съвет с жалба за отмяна на мълчаливия отказ, произтичащ от липсата на отговор от страна на министър-председателя по искането им за отмяна на член R. 10-13 от CPCE, както и на Декрет № 2011-219, по-специално с мотива, че тези текстове нарушават член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 от Хартата. Допуснато е встъпването в главното производство на Privacy International и Center for Democracy and Technology.

70 Що се отнася до член R. 10-13 от CPCE и предвиденото в него задължение за общо и неизбирателно запазване на данни за съобщенията, запитващата юрисдикция, която излага съображения, подобни на изложените по дело C-511/18, отбелязва, че такова запазване позволява на съда достъп до данните за съобщенията, които дадено лице е осъществило, преди да бъде заподозряно в извършването на престъпление, така, че това запазване е от изключителна полза за разследването, разкриването и преследването на престъпленията.

71 Що се отнася до Декрет № 2011-219, запитващата юрисдикция счита, че член 6, параграф II от LCEN, който налага задължение за задържане и запазване единствено и само данните, свързани със създаването на съдържание, не попада в приложното поле на Директива 2002/58, която съгласно член 3, параграф 1 от нея се отнася единствено до предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Съюза, а в приложното поле на Директива 2000/31.

72 Тази юрисдикция обаче счита, че от член 15, параграфи 1 и 2 от Директива 2000/31 следва, че тя не установява принципна забрана за запазване на данните, свързани със създаването на съдържание, дерогация от която да е възможна само по изключение. Така се поставя въпросът дали членове 12, 14 и 15 от посочената директива във връзка с членове 6—8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкуват в смисъл, че допускат държава членка да приеме национална правна уредба като член 6, параграф II от LCEN, с която да задължи засегнатите лица да запазват данните, годни да позволят идентифицирането на всяко лице, което допринася за създаването на съдържанието или на част от съдържанието на предоставяните от тях услуги, за да може съдът евентуално да ги изисква с оглед на зачитането на нормите в областта на гражданската или наказателната отговорност.

73 При тези условия Conseil d'État (Държавен съвет, Франция) решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) Трябва ли задължението за общо и неизбирателно запазване, наложено на доставчиците на основание на разрешителните разпоредби на член 15, параграф 1 от Директива [2002/58], да се разглежда — по-специално с оглед на гаранциите и проверките, които са предвидени по-нататък по отношение на събирането и използването на тези данни за свързване — като намеса, обоснована с правото на сигурност, гарантирано в член 6 от [Хартата], и с изискванията на националната сигурност, отговорността за която е единствено на държавите членки по силата на член 4 [ДЕС]?

2) Трябва ли разпоредбите на Директива [2000/31], разглеждани във връзка с членове 6, 7, 8 и 11, както и с член 52, параграф 1 от [Хартата], да се тълкуват в смисъл, че допускат дадена държава да приеме национална правна уредба, с която да задължи лицата, чиято дейност се състои в осигуряване на достъп до публични съобщителни услуги в интернет, и физическите или юридическите лица, които осигуряват — дори без заплащане и за целите на публичното им предоставяне посредством публични съобщителни услуги в интернет — съхранението на предоставени от получателите на тези услуги сигнали, текстове, изображения, звуци или съобщения от всякакво естество, да запазват данните, годни да позволят идентифицирането на всяко лице, което допринася за създаването на съдържанието или на част от съдържанието на предоставяните от тях услуги, за да може съдът евентуално да ги изиска с оглед на зачитането на нормите в областта на гражданската или наказателната отговорност?“.

Дело C-520/18

74 С жалби, подадени на 10 януари, 16 януари, 17 януари и 18 януари 2017 г., които са съединени в рамките на главното производство, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL и UA, Liga voor Mensenrechten ASBL и Ligue des Droits de l'Homme ASBL, както и VZ, WY и XX подават пред Cour constitutionnelle (Конституционен съд, Белгия) жалби за отмяна на Закона от 29 май 2016 г. с мотива, че той нарушавал членове 10 и 11 от Конституцията на Белгия, във връзка с членове 5, 6—11, 14, 15, 17 и 18 от ЕСПЧ, членове 7, 8, 11, 47 и член 52, параграф 1 от Хартата, член 17 от Международният пакт за гражданските и политическите права, приет от Общото събрание на Организацията на обединените нации на 16 декември 1966 г., влязъл в сила на 23 март 1976 г., общите принципи на правна сигурност, на пропорционалност и на самоопределянето в областта на информацията, а също и член 5, параграф 4 ДЕС.

75 В подкрепа на жалбите си жалбоподателите в главното производство изтъкват по същество, че незаконосъобразността на Закона от 29 май 2016 г. се дължи по-специално на факта, че той надхвърля границите на строго необходимото и не предвижда достатъчни гаранции за защита. В частност, нито разпоредбите му относно запазването на данни, нито тези, които уреждат достъпа на органите до запазените данни, отговаряли на изискванията, произтичащи от решение от 8 април 2014 г., Digital Rights Ireland и др. (C-293/12 и C-594/12, наричано по-нататък „решение Digital Rights", EU:C:2014:238) и от решение от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970). Всъщност тези разпоредби съдържали риск от установяване на личностни профили с произтичащите от това възможни злоупотреби от страна на компетентните органи и също така не предвиждали подходящо равнище на сигурност и защита на запазените данни. Накрая, този закон обхващал лицата, за които се прилагат изискванията за професионална тайна, както и лицата, които имат задължение за поверителност, и се отнасял до чувствителни лични данни за съобщения, без да съдържа специални гаранции за защитата на тези данни.

76 Запитващата юрисдикция отбелязва, че данните, които трябва да запазват доставчиците на телефонни услуги, включително в интернет, на достъп до интернет, на електронна поща в интернет, както и операторите, предоставящи обществени електронни съобщителни мрежи по силата на Закона от 29 май 2016 г., са идентични с изброените в 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), без да е направено разграничение по отношение на засегнатите лица или в зависимост от преследваната цел. Във връзка с последното посочената юрисдикция уточнява, че целта, преследвана от законодателя с този закон, е не само борбата с тероризма и детската порнография, но и да може да се използват запазените данни в голям брой случаи в рамките на наказателното разследване. Освен това запитващата юрисдикция констатира, че видно от изложението на мотивите към посочения закон, националният законодател е приел, че с оглед на преследваната цел е невъзможно да се въведе задължение за целево и избирателно запазване и че той е решил да обвърже задължението за общо и неизбирателно запазване със стриктни гаранции както от гледна точка на запазените данни, така и от гледна точка на достъпа до тях, за да се ограничи до минимум намесата в правото на зачитане на личния живот.

77 Запитващата юрисдикция добавя, че член 126, параграф 2, точки 1° и 2° от Закона от 13 юни 2005 г., в редакцията му съгласно Закона от 29 май 2016 г., предвижда условията, при които съответно съдебните органи и службите за разузнаване и сигурност могат да получат достъп до запазените данни, така че проверката на законосъобразността на този закон с оглед на изискванията на правото на Съюза трябва да бъде спряна до произнасянето на Съда по две висящи пред него преюдициални производства относно такъв достъп.

78 Накрая, запитващата юрисдикция отбелязва, че Законът от 29 май 2016 г. има за цел да позволява ефективно наказателно разследване и ефективно наказване в случай на сексуалното насилие над ненавършили пълнолетие лица и да позволява ефективно идентифициране на извършителя на подобно престъпление, включително когато са използвани електронни съобщителни средства. В хода на производството пред нея в това отношение е било обърнато внимание на задълженията за действие, произтичащи от членове 3 и 8 от ЕКПЧ. Тези задължения можели да произтичат и от съответните разпоредби на Хартата, които могат да имат отражение върху тълкуването на член 15, параграф 1 от Директива 2002/58.

79 При тези условия Cour constitutionnelle (Конституционен съд, Белгия) решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) Трябва ли член 15, параграф 1 от Директива [2002/58] във връзка с правото на сигурност, гарантирано от член 6 на [Хартата], и правото на защита на личните данни, гарантирано от членове 7, 8 и член 52, параграф 1 от [Хартата], да се тълкува в смисъл, че не допуска национална правна уредба като разглежданата, която предвижда за операторите и доставчиците на електронни съобщителни услуги общо задължение да запазват данни за трафик и за местонахождение по смисъла на Директива [2002/58], генерирани или обработвани от тях при доставянето на тези услуги, като се има предвид, че тази национална правна уредба няма за цел само разследването, разкриването и наказателното преследване на тежки престъпления, но и гарантирането на националната сигурност, отбраната на територията и обществената сигурност, разследването, разкриването и наказателното преследване на други престъпления, освен тежките, или предотвратяването на неправомерното използване на електронни комуникационни системи или постигането на друга цел, определена от член 23, параграф 1 от Регламент [2016/679], по отношение на която освен това са предвидени уточнени в тази правна уредба гаранции, свързани със запазването на данните и достъпа до тях?

2) Трябва ли член 15, параграф 1 от Директива [2002/58] във връзка с членове 4, 7, 8, 11 и член 52, параграф 1 от [Хартата] да се тълкува в смисъл, че не допуска национална правна уредба като разглежданата, която предвижда за операторите и доставчиците на електронни съобщителни услуги общо задължение да запазват данни за трафик и за местонахождение по смисъла на Директива [2002/58], генерирани или обработвани от тях при доставянето на тези услуги, ако тази правна уредба има по-специално за цел реализирането на наложените на органа положителни задължения по силата на членове 4 и [7] от Хартата, които се състоят във въвеждането на правна уредба, която позволява ефективно досъдебно производство и ефективно наказване на сексуалното насилие над ненавършили пълнолетие лица и която позволява ефективно идентифициране на извършителя на престъплението, включително когато са използвани електронни съобщителни средства?

3) Ако въз основа на отговорите, дадени на първия или втория преюдициален въпрос, Cour constitutionnelle [Конституционен съд] стигне до заключението, че атакуваният закон нарушава едно или повече от задълженията, произтичащи от посочените в тези въпроси разпоредби, може ли той временно да запази правните последици на закона от [29 май 2016 г.], за да се избегне правната несигурност и да се позволи събраните и запазени преди това данни да продължат да се използват за посочените в закона цели?“.

Относно производството пред Съда

80 С решение на председателя на Съда от 25 септември 2018 г. дело C-511/18 и дело C-512/18 са съединени за целите на писмената и устната фаза на производство и на съдебното решение. С решение на председателя на Съда от 9 юли 2020 г. дело C-520/18 е съединено с тези дела за целите на съдебното решение.

Относно преюдициалните въпроси

По първите въпроси по дела C-511/18 и C-512/18, както и по първия и втория въпрос по дело C-520/18

81 С първите въпроси по дела C-511/18 и C-512/18, както и с първия и втория въпрос по дело C-520/18, които следва да се разгледат заедно, запитващите юрисдикции искат по същество да се установи дали член 15, параграф 1 от Директива 2002/58 трябва да се тълкува в смисъл, че не допуска национална правна уредба, която налага на доставчиците на електронни съобщителни услуги за целите, предвидени в посочения член 15, параграф 1, общо и неизбирателно запазване на данни за трафик и на данни за местонахождение.

Предварителни бележки

82 От представените пред Съда преписки е видно, че разглежданите в главното производство правни уредби обхващат всички електронни съобщителни средства и всички ползватели на тези средства, без в това отношение да се прави разграничение или изключение. Освен това данните, които съгласно посочените разпоредби доставчиците на електронни съобщителни услуги са задължени да съхраняват, са по-специално данните, необходими за откриване на източника и местоназначението на дадено съобщение, за определяне на датата, часа, продължителността и естеството му, за установяване на използваното съобщително оборудване и за определяне на местонахождението на крайните устройства и съобщенията — данни, сред които по-конкретно са името и адресът на ползвателя, телефонните номера на викащия и на повикания, както и IP адресът за интернет услугите. За сметка на това посочените данни не обхващат съдържанието на съответните съобщения.

83 Така данните, които съгласно разглежданата в главното производство национална правна уредба трябва да бъдат съхранявани в продължение на една година, позволяват по-специално да се установи с кое лице и чрез какво средство се е свързал ползвателят на електронно съобщително средство, да се определят датата, часът и продължителността на съобщенията и свързването с интернет, както и мястото, от което те са осъществени, и да се разбере къде се намират крайните устройства, без непременно да се пренася съобщение. Освен това те предоставят възможност за определяне на честотата на осъществяване на

съобщения на ползвателя с определени лица за определен период. Накрая, що се отнася до разглежданата по дела C-511/18 и C-512/18 национална правна уредба, изглежда, че доколкото обхваща и данните относно пренасянето на електронни съобщения чрез мрежите, тя позволява също да се установи естеството на консултираната в интернет информация.

84 Що се отнася до преследваните цели, следва да се отбележи, че разглежданите по дела C-511/18 и C-512/18 правни уредби имат за цел, наред с останалото, разследването, разкриването и преследването на престъпленията като цяло, защитата на националната независимост, териториалната цялост и националната отбрана, на основните интереси в областта на външната политика, на изпълнението на европейските и международните задължения на Франция, на важните икономически, промишлени и научни интереси на Франция, както и предотвратяването на тероризма, на посегателствата срещу републиканската форма на институциите и на актове на колективно насилие, които могат сериозно да засегнат обществения мир. Що се отнася до разглежданата по дело C-520/18 правна уредба, тя има за цел, inter alia, разследването, разкриването и преследването на престъпления, както и гарантирането на националната сигурност, отбраната на територията и обществената сигурност.

85 Запитващите юрисдикции искат по-специално да се установи евентуалното отражение на правото на сигурност, закрепено в член 6 от Хартата, върху тълкуването на член 15, параграф 1 от Директива 2002/58. Освен това те искат да се установи дали намесата в основните права, закрепени в членове 7 и 8 от Хартата, до която води предвиденото в разглежданата в главното производство правна уредба запазване на данни, може да се счита за обоснована с оглед на наличието на правила, ограничаващи достъпа на националните органи до запазените данни. Освен това според Държавният съвет, тъй като този въпрос се поставя в условията на сериозни и постоянни заплахи за националната сигурност, той трябва да се прецени и от гледна точка на член 4, параграф 2 ДЕС. От своя страна Конституционният съд подчертава, че разглежданата по дело C-520/18 национална правна уредба е в изпълнение на задълженията за действие, произтичащи от членове 4 и 7 от Хартата, които се състоят в предвиждането на правна уредба, позволяваща ефективно наказване на сексуалното насилие над ненавършили пълнолетие лица.

86 Докато Държавният съвет и Конституционният съд изхождат от предпоставката, че разглежданите в главното производство национални правни уредби, които регламентират запазването на данни за трафик и на данни за местонахождение, както и достъпа на националните органи до тези данни за предвидените в член 15, параграф 1 от Директива 2002/58 цели, като опазването на националната сигурност, попадат в приложното поле на тази директива, някои страни в главното производство и някои държави членки, представили писмени становища пред Съда, изразяват различно становище в това отношение, по-конкретно относно тълкуването на член 1, параграф 3 от Директивата. Ето защо най-напред следва да се провери дали тези правни уредби попадат в приложното поле на Директивата.

По приложното поле на Директива 2002/58

87 La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International и Center for Democracy and Technology изтъкват по същество, като се позовават в това отношение на практиката на Съда относно приложното поле на Директива 2002/58, че както запазването на данни, така и достъпът до запазените данни попадат в това

приложно поле, независимо дали този достъп се осъществява отложено във времето, или в реално време. Всъщност, тъй като целта за опазване на националната сигурност е изрично посочена в член 15, параграф 1 от тази директива, преследването ѝ не водело до неприложимост на Директивата. Изтъкваният от запитващите юрисдикции член 4, параграф 2 ДЕС не засягал тази преценка.

88 Що се отнася до мерките за разузнаване, които компетентните френски органи прилагат пряко, без да регламентират дейността на доставчиците на електронни съобщителни услуги чрез налагането на специфични задължения, Center for Democracy and Technology отбелязва, че тези мерки по необходимост попадат в приложното поле на Директива 2002/58 и на Хартата, тъй като представляват изключения от принципа на поверителност, гарантиран от член 5 от тази директива. Следователно посочените мерки трябвало да отговарят на изискванията, произтичащи от член 15, параграф 1 от нея.

89 Обратно, френското, чешкото и естонското правителство, Ирландия, кипърското, унгарското, полското и шведското правителство и правителството на Обединеното кралство по същество твърдят, че Директива 2002/58 не се прилага към национални правни уредби като разглежданите в главното производство, тъй като тяхната цел е опазването на националната сигурност. Доколкото се отнасят до поддържането на обществения ред и опазването на вътрешната сигурност и териториалната цялост, дейностите на разузнавателните служби спадали към съществените функции на държавите членки и следователно били единствено от компетентността на последните, за което свидетелствал по-специално член 4, параграф 2, трето изречение ДЕС.

90 Тези правителства и Ирландия освен това се позовават на член 1, параграф 3 от Директива 2002/58, който изключвал от приложното ѝ поле, подобно на вече предвиденото в член 3, параграф 2, първо тире от Директива 95/46, дейностите, свързани с обществената сигурност, отбраната и сигурността на държавата. В това отношение те се позовават на тълкуването на последната разпоредба, съдържащо се в решение от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346).

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

92 Член 1, параграф 3 от тази директива изключва от приложното ѝ поле „дейностите на държавата“ в определени посочени в нея области, сред които дейностите на държавата в областта на наказателното право, както и тези, отнасящи се до обществената сигурност, отбраната, сигурността на държавата, включително икономическото благосъстояние на държавата, когато дейностите се отнасят до сигурността на държавата. Примерно посочените по този начин дейности във всички случаи са присъщи на държавите или на държавните органи дейности, които са извън областите на дейност на частноправните субекти (решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 32 и цитираната съдебна практика).

93 Освен това, член 3 от Директива 2002/58 предвижда, че тази директива се прилага при обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Съюза, включително

обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация (наричани по-нататък „електронни съобщителни услуги“). Споменатата директива трябва следователно да се разглежда като уреждаща дейността на доставчиците на такива услуги (решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 33 и цитираната съдебна практика).

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

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

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

97 Освен това предвид изложените в точка 95 от настоящото решение съображения и общата структура на Директива 2002/58 тълкуване на тази директива в смисъл, че законодателните мерки по член 15, параграф 1 от Директива 2002/58 са изключени от приложното ѝ поле, тъй като целите, които трябва да се преследват с такива мерки по същество съвпадат с целите, които се преследват с дейностите по член 1, параграф 3 от същата директива, би лишило от смисъл посочения член 15, параграф 1 (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 72 и 73).

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

99 Разпоредбите на член 4, параграф 2 ДЕС, на които се позовават посочените в точка 89 от настоящото решение правителства, не могат да оборят този извод. Всъщност съгласно постоянната практика на Съда, макар държавите членки да са тези, които определят основните интереси на своята сигурност и предприемат подходящи мерки, за да

гарантират вътрешната и външната си сигурност, единствено фактът, че национална мярка е приета за защита на националната сигурност, не може да доведе до изключване на приложимостта на правото на Съюза и да освободи държавите членки от необходимостта от спазване на това право (вж. в този смисъл решения от 4 юни 2013 г., ZZ, C-300/11, EU:C:2013:363, т. 38, от 20 март 2018 г., Комисия/Австрия (Държавна печатница), C-187/16, EU:C:2018:194, т. 75 и 76 и от 2 април 2020 г., Комисия/Полша, Унгария и Чешка република (Схема за временно преместване на кандидати за международна закрила), C-715/17, C-718/17 и C-719/17, EU:C:2020:257, т. 143 и 170).

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

101 При все това с оглед на изложените в точки 93, 95 и 96 от настоящото решение съображения тази съдебна практика не може да се приложи към тълкуването на член 1, параграф 3 от Директива 2002/58. Всъщност, както по същество отбелязва генералният адвокат в точки 70—72 от заключението си по съединени дела La Quadrature du Net и др. (C-511/18 и C-512/18, EU:C:2020:6), член 3, параграф 2, първо тире от Директива 95/46, към който се отнася посочената съдебна практика, оставя извън приложното поле на тази директива по общ начин „обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност“, без да въвежда разграничение, свързано със субекта, осъществяващ обработването на съответните данни. За сметка на това при тълкуването на член 1, параграф 3 от Директива 2002/58 такова разграничение се оказва необходимо. Всъщност, както следва от точки 94—97 от настоящото решение, всички видове обработване на лични данни, извършвано от доставчиците на електронни съобщителни услуги, попадат в приложното поле на посочената директива, включително обработването, което произтича от наложени им от публичните органи задължения, като последното обработване може евентуално да попада в изключението, предвидено в член 3, параграф 2, първо тире от Директива 95/46, като се има предвид по-широката формулировка на тази разпоредба, която се отнася до всеки вид обработване на данни, независимо от лицето, което го извършва, свързани с обществената сигурност, отбраната или държавната сигурност.

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

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

104 С оглед на изложените по-горе съображения национална правна уредба, която налага на доставчиците на електронни съобщителни услуги задължение да съхраняват данни за трафик и данни за местонахождение с оглед опазването на националната сигурност и борбата срещу престъпността, като тази в делата по главните производства, попада в приложното поле на Директива 2002/58.

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

105 В самото начало следва да се припомни, че съгласно постоянната практика на Съда, за да се тълкува разпоредба от правото на Съюза, трябва не само да се вземе предвид нейният текст, но и контекстът ѝ, както и целите, преследвани от правната уредба, от която тя е част, и по-специално генезисът на тази правна уредба (вж. в този смисъл решение от 17 април 2018 г., Egenberger, C-414/16, EU:C:2018:257, т. 44).

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

107 За тази цел 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.

108 Що се отнася, по-специално до обработването и съхранението на данни за трафик от доставчиците на електронни съобщителни услуги, от член 6 и съображения 22 и 26 от Директива 2002/58 следва, че такова обработване се разрешава само ако и докато е

необходимо за целите на пускането на пазара на услугите, фактурирането им или облагането им с данък върху добавената стойност. След изтичането на този период обработените и съхранени данни трябва да се изтрият или да се направят анонимни. По отношение на 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 (решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 86 и цитираната съдебна практика).

109 По този начин с приемането на тази директива законодателят на Съюза конкретизира правата, признати в членове 7 и 8 от Хартата, така че ползвателите на електронни съобщителни средства по принцип имат право да очакват, че техните съобщения и свързаните с тях данни, без тяхно съгласие, остават анонимни и няма да могат да бъдат записвани.

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

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

112 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 (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 52 и цитираната съдебна практика).

113 Освен това от член 15, параграф 1, трето изречение от Директива 2002/58 следва, че на държавите членки се разрешава да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, посочени в членове 5, 6 и 9 от тази директива само при зачитане на общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и на основните права, гарантирани от Хартата. В това отношение Съдът вече е постановил, че задължението, наложено на доставчиците на електронни съобщителни услуги с национална правна уредба, за запазване на данни за трафик с цел да може, когато се налага, да се предоставя достъп до тях на компетентните национални

органи, повдига въпроси относно зачитането не само на членове 7 и 8 от Хартата, отнасящи се съответно до защитата на личния живот и до защитата на личните данни, но и на член 11 от Хартата, отнасящ се до свободата на изразяване на мнение (вж. в този смисъл решения от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 25 и 70 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 91 и 92 и цитираната съдебна практика).

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

115 В това отношение следва да се уточни, че запазването 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, съставлява 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 и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 124 и 126 и цитираната съдебна практика; вж. по аналогия, относно член 8 от ЕКПЧ, ЕСПЧ, решение от 30 януари 2020 г., Breyer с/у Германия, CE:ECHR:2020:0130JUD005000112, § 81).

116 Също така е без значение последващото използване на запазените данни (вж. по аналогия, относно член 8 от ЕКПЧ, ЕСПЧ, решение от 16 февруари 2000 г., Amann с/у Швеция, CE:ECHR:2000:0216JUD002779895, § 69 и от 13 февруари 2020 г., Trjakovski и Chipovski с/у Северна Македония, CE:ECHR:2020:0213JUD005320513, § 51), тъй като достъпът до такива данни, независимо от използването им, което е последващ факт, представлява определена намеса в посочените в предходната точка основни права (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 124 и 126).

117 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 запазени, например относно навиците им в ежедневния живот, мястото на постоянно или временно пребиваване, ежедневните им или други пътувания, упражняваните дейности, социалните връзки на тези лица и социалните кръгове, в които се движат. 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 (вж. в този смисъл решения от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 27 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 99).

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

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

120 При това положение, доколкото позволява на държавите членки да въведат дерогациите, посочени в точка 110 от настоящото решение, член 15, параграф 1 от Директива 2002/58 отразява обстоятелството, че правата, закрепени в членове 7, 8 и 11 от Хартата, не са абсолютни, а трябва да се разглеждат във връзка с тяхната социална функция (вж. в този смисъл решение от 16 юли 2020 г., Facebook Ireland и Schrems, C-311/18, EU:C:2020:559, т. 172 и цитираната съдебна практика).

121 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.

122 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.

123 В това отношение член 6 от Хартата, на който се позовават Държавният съвет и Конституционният съд, закрепва правото на всеки не само на свобода, но и на сигурност и гарантира права, съответстващи на тези по член 5 от ЕКПЧ (вж. в този смисъл решения от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 47, от 28 юли 2016 г., JZ, C-294/16 PPU, EU:C:2016:610, т. 48 и от 19 септември 2019 г., Районна прокуратура Лом, C-467/18, EU:C:2019:765, т. 42 и цитираната съдебна практика).

124 Освен това следва да се припомни, че член 52, параграф 3 от Хартата има за цел да гарантира необходимата последователност между правата по Хартата и съответстващите им права, гарантирани от ЕКПЧ, без да засяга автономността на правото на Съюза и Съда на Европейския съюз. Следователно за целите на тълкуването на Хартата трябва да се държи сметка за съответстващите права от ЕКПЧ, разглеждани като минимален праг на защита (вж. в този смисъл решения от 12 февруари 2019 г., TC, C-492/18 PPU, EU:C:2019:108, т. 57 и от 21 май 2019 г., Комисия/Унгария (Ползване на земеделски земи), C-235/17, EU:C:2019:432, т. 72 и цитираната съдебна практика).

125 Що се отнася до член 5 от ЕКПЧ, който закрепва „правото на свобода“ и „правото на сигурност“, съгласно практиката на Европейския съд по правата на човека той цели да защити личността от всяко произволно или необосновано лишаване от свобода (вж. в този смисъл ЕСПЧ, решение от 18 март 2008 г., Ladent с/у Полша, CE:ECHR:2008:0318JUD001103603, §§ 45 и 46, от 29 март 2010 г., Медведиев и др. с/у Франция, CE:ECHR:2010:0329JUD000339403, §§ 76 и 77 и от 13 декември 2012 г., El-Masri с/у Бивша югославска република Македония, CE:ECHR:2012:1213JUD003963009, § 239). Доколкото обаче тази разпоредба се отнася до лишаване от свобода, извършено от публичен орган, член 6 от Хартата не може да се тълкува в смисъл, че налага на публичните органи задължение да приемат специални мерки за преследване на определени престъпления.

126 Обратно, що се отнася по-специално до изтъкнатата от Конституционния съд ефективна борба срещу престъпленията, при които пострадали са по-специално ненавършили пълнолетие и други уязвими лица, следва да се подчертае, 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 (вж. в този смисъл решение от 18 юни 2020 г. Комисия/Унгария (Прозрачност на сдруженията) C-78/18, EU:C:2020:476, т. 123 и цитираната съдебна практика на Европейския съд по правата на човека). Такива задължения могат да произтичат и от посочения член 7, що се отнася до 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 или унизително отношение.

127 С оглед на тези различни задължения за действие обаче следва да се пристъпи към необходимото съвместяване на различните разглеждани интереси и права.

128 Всъщност Европейският съд по правата на човека приема, че задълженията за действие, произтичащи от членове 3 и 8 от ЕКПЧ, чиито съответни гаранции се съдържат в членове 4 и 7 от Хартата, включват по-специално приемането на материални и процесуални разпоредби, както и на мерки от практическо естество, позволяващи ефикасна борба срещу престъпленията срещу лицата чрез ефективно разследване и преследване, като това задължение е още по-важно, когато е застрашено физическото и моралното благосъстояние на дете. При това положение мерките, които компетентните органи следва да предприемат, трябва да зачитат изцяло правните способи и другите гаранции, които могат да ограничат обхвата на правомощията за наказателно разследване, както и другите свободи и права. По-специално, според тази юрисдикция следва да се въведе правна уредба, позволяваща да се съвместят различните интереси и права, които следва да бъдат защитени (ЕСПЧ, решения от 28 октомври 1998 г., Osman с/у Обединено кралство, CE:ECHR:1998:1028JUD002345294, §§ 115 и 116, от 4 март 2004 г., M.C. с/у България,

CE:ECHR:2003:1204JUD003927298, § 151, от 24 юни 2004 г., Von Hannover с/у Германия, CE:ECHR:2004:0624JUD005932000, §§ 57 и 58 и от 2 декември 2008 г., K.U. с/у Финландия, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 и 49).

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

130 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 (вж. в този смисъл решения от 16 декември 2008 г., Satakunnan Markkinapörssi и Satamedia, C-73/07, EU:C:2008:727, т. 56, от 9 ноември 2010 г., Volker und Markus Schecke и Eifert, C-92/09 и C-93/09, EU:C:2010:662, т. 76, 77 и 86 и от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 52 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 140).

131 По-конкретно от практиката на Съда следва, че възможността за държавите 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 в съответните основни права, която включва подобно ограничение, и като се провери дали значението на преследваната с това ограничение цел от общ интерес е свързано с тази тежест (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 55 и цитираната съдебна практика).

132 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 уредба трябва да е задължителна по вътрешното право, и в частност да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни, като по този начин гарантира ограничаване на намесата до строго необходимото. Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматизирано обработване, по-специално когато съществува значителен риск от неправомерен достъп до тези данни. Тези съображения важат най-вече, когато става дума за защита на чувствителни данни, които са особената категория лични данни (вж. в този смисъл решения от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 54 и 55 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 117 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 141).

133 Така уредба, предвиждаща запазване на личните данни, трябва винаги да отговаря на обективни критерии, установяващи връзка между подлежащите на запазване лични данни и преследваната цел (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 191 и цитираната съдебна практика и решение от 3 октомври 2019 г., A и др., C-70/18, EU:C:2019:823, т. 63).

– По законодателните мерки, предвиждащи превантивното запазване на данни за трафик и на данни за местонахождение с цел опазване на националната сигурност

134 Следва да се отбележи, че изтъкваната от запитващите юрисдикции и представилите становища правителства цел за опазване на националната сигурност все още не е била специално разглеждана от Съда в решенията му за тълкуване на Директива 2002/58.

135 В това отношение в самото начало следва да се отбележи, че член 4, параграф 2 ДЕС гласи, че националната сигурност остава единствено в рамките на отговорността на всяка държава членка. Тази отговорност съответства на първостепенния интерес от защита на съществените функции на държавата и основните интереси на обществото и включва предотвратяването и преследването на дейности, които могат сериозно да дестабилизират основните конституционни, политически, икономически или социални структури на дадена страна, и по-специално да заплашват пряко обществото, населението или самата държава, като например терористични дейности.

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

137 Така в случаи като описаните в точки 135 и 136 от настоящото решение член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата допуска по принцип законодателна мярка, която дава право на компетентните органи да задължат доставчиците на електронни съобщителни услуги да запазват данни за трафик и данни за местонахождение на всички ползватели на електронни съобщителни средства за ограничен период от време, ако има достатъчно конкретни обстоятелства, които позволяват да се приеме, че съответната държава членка е изправена пред сериозна заплаха за националната сигурност, като посочената в точки 135 и 136 от настоящото решение, която е действителна и настояща или предвидима. Макар такава мярка да се отнася без разграничение до всички ползватели на електронни съобщителни средства, без да изглежда на пръв поглед те да имат връзка по смисъла на посочената в точка 133 от настоящото решение съдебна практика със заплаха за националната сигурност на тази държава членка, все пак следва да се приеме, че наличието на такава заплаха може само по себе си да създаде тази връзка.

138 Разпореждането, предвиждащо превантивното запазване на данните на всички ползватели на електронни съобщителни средства, трябва все пак да бъде ограничено във времето до строго необходимото. Макар да не може да се изключи възможността за подновяване на разпореждането към доставчиците на електронни съобщителни услуги за запазване на данни, тъй като такава заплаха продължава да съществува, срокът на действие на всяко разпореждане не може да надвишава предвидим период от време. Освен това за подобно запазване на данните трябва да се налагат ограничения и да се предвидят строги гаранции, позволяващи ефикасна защита на личните данни на засегнатите лица срещу рискове от злоупотреби. Следователно това запазване не може да има системен характер.

139 Предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, произтичаща от такава мярка за общо и неизбирателно запазване на данни, е важно да се гарантира, че използването ѝ действително се ограничава до положенията, при които е налице сериозна заплаха за националната сигурност като посочените в точки 135 и 136 от настоящото решение. За тази цел е от съществено значение решението, с което на доставчиците на електронни съобщителни услуги се разпорежда да извършат такова запазване на данни, да може да подлежи на ефективен контрол от юрисдикция 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.

– По законодателните мерки, предвиждащи превантивното запазване на данни за трафик и на данни за местонахождение за целите на борбата с престъпността и опазването на обществената сигурност

140 Що се отнася до целта за превенция, разследване, разкриване и преследване на престъпления, 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 запазването 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 (вж. в този смисъл решения от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 102 и от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 56 и 57 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 149).

141 Националната правна уредба, която предвижда общо и неизбирателно запазване на данни за трафик и на данни за местонахождение с цел борба с тежката престъпност, надхвърля границите на строго необходимото и не може да се счита за обоснована в едно демократично общество, както изисква член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 107).

142 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 118 от настоящото решение основни права, закрепени в членове 7 и 11 от Хартата, до което може да доведе запазването на тези данни, и от друга страна,

сериозността на намесата, до която води такова запазване, 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 запазване. 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.

143 Освен това Съдът е подчертал, че правна уредба, която предвижда общо и неизбирателно запазване на данни за трафик и на данни за местонахождение, обхваща електронните съобщения на почти цялото население, без да се прави никакво разграничение, ограничение или изключение в зависимост от преследваната цел. Такава правна уредба, противно на изискванията, припомнени в точка 133 от настоящото решение, засяга абсолютно всички лица, които използват електронни съобщителни услуги, без да е необходимо тези лица да се намират, макар и непряко, в положение, което би могло да даде повод за наказателно преследване. Следователно тя се прилага дори за лица, за които не съществува никаква улика, даваща основание да се счита, че действията им биха могли да имат някаква, била тя непряка и далечна, връзка с тази цел за борба с тежките престъпления, и по специално, без да се изисква никаква връзка между данните, които се предвижда да бъдат запазени, и наличието на заплаха за обществената сигурност (вж. в този смисъл решения от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 57 и 58 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 105).

144 По-конкретно, както Съдът вече е постановил, такава правна уредба не се ограничава до запазването само на данни, отнасящи се за определен период и/или за определена географска зона, и/или за кръг от определени лица, които е възможно по един или друг начин да са участвали в тежко престъпление, нито само за лица, които поради други съображения биха могли да допринесат чрез запазване на данните им за борбата с тежката престъпност (вж. в този смисъл решения от 8 април 2014 г., Digital Rights, C-293/12 и C-594/12, EU:C:2014:238, т. 59 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 106).

145 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 точки 126 и 128 от настоящото решение, се отнасят до въвеждането на правила, позволяващи ефективна борба с престъпленията, не биха могли обаче да обосноват толкова сериозна намеса в основните права, прогласени в членове 7 и 8 от Хартата, като съдържащата се в правна уредба, която предвижда запазване на данните за трафик и на данните за местонахождение на почти всички лица, без данните на засегнатите лица да могат да имат връзка, макар и непряка, с преследваната цел.

146 Обратно, в съответствие с посоченото в точки 142—144 от настоящото решение и с оглед на необходимостта да се съвместят разглежданите права и интереси, целите за борба с тежката престъпност, за предотвратяване на тежки посегателства срещу обществената сигурност и a fortiori, за опазване на националната сигурност могат, предвид тяхното значение, с оглед на задълженията за действие, припомнени в предходната точка и на които по-специално се позовава Конституционният съд, да обосноват особено сериозната намеса, до която води целево запазване на данни за трафик и на данни за местонахождение.

147 Така, както Съдът вече е постановил, член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата допуска държава членка да приеме правна уредба, която позволява целево запазване на данни за трафик и на данни за местонахождение като превантивна мярка за целите на борбата с тежката престъпност и за предотвратяване на сериозните заплахи срещу обществената сигурност, както и за целите на опазването на националната сигурност, при условие че такова запазване е ограничено до строго необходимото, що се отнася до подлежащите на запазване категории данни, визираните съобщителни средства, съответните лица, както и установения период на запазване (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 108).

148 Що се отнася до обхвата, който трябва да се посочи за такава мярка за запазване, той може по-специално да се определи в зависимост от категориите засегнати лица, при положение че член 15, параграф 1 от Директива 2002/58 допуска правна уредба, основана на обективни обстоятелства, позволяващи с нея да се визират лица, чиито данни за трафик и данни за местонахождение могат да имат връзка, макар и непряка, с тежки престъпления, да допринася по един или друг начин за борбата с тежката престъпност или да предотвратява сериозен риск за обществената сигурност или риск за националната сигурност (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 111).

149 В това отношение следва да се уточни, че визираните по този начин лица могат по-специално да бъдат тези, които в рамките на приложимите национални процедури и въз основа на обективни обстоятелства са предварително идентифицирани като заплаха за обществената или националната сигурност на съответната държава членка.

150 Определянето на обхвата на мярка, която предвижда запазване на данни за трафик и данни за местонахождение, може да се основава и на географски критерий, когато въз основа на обективни обстоятелства с недискриминационен характер компетентните национални органи установят, че в една или в няколко географски зони съществува повишен риск от подготвяне или извършване на тежки престъпления (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 111). 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 или зони за събиране на пътни такси.

151 За да се гарантира, че намесата, до която водят описаните в точки 147—150 от настоящото решение мерки за целево запазване, е в съответствие с принципа на пропорционалност, продължителността им 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 запазване.

– По законодателните мерки, предвиждащи превантивното запазване на IP адресите и на данните за самоличност за целите на борбата с престъпността и опазването на обществената сигурност

152 Следва да се отбележи, че IP адресите, макар и да са част от данните за трафик, се генерират, без да са свързани с определено съобщение и служат главно за идентифициране, посредством доставчиците на електронни съобщителни услуги, на физическото лице, собственик на крайно устройство, от което се осъществява комуникация чрез интернет.

Така в областта на електронната поща, както и на интернет телефонията, доколкото са запазени само IP адресите на източника на съобщението, но не и тези на неговия адресат, тези адреси сами по себе си не разкриват никаква информация за третите лица, които са били в контакт с лицето, стоящо в основата на съобщението. Следователно тази категория данни е с по-ниска степен на чувствителност в сравнение с другите данни за трафика.

153 При все това, тъй като IP адресите 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, която може да окаже възпиращо действие като посоченото в точка 118 от настоящото решение.

154 За целите на необходимото съвместяване на разглежданите права и интереси, което се изисква съгласно цитираната в точка 130 от настоящото решение съдебна практика, обаче следва да се вземе предвид фактът, че в случай на извършено в интернет престъпление 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. Към това се добавя фактът, че съхраняването на IP адреси от доставчиците на електронни съобщителни услуги извън периода на предоставяне на тези данни по принцип не изглежда необходимо за целите на изготвянето на сметки за разглежданите услуги, поради което разкриването на извършените престъпления в интернет може да се окаже невъзможно, без да се прибегне до законодателна мярка на основание член 15, параграф 1 от Директива 2002/58, както посочват няколко правителства в представените пред Съда становища. Както изтъкват тези правителства, такъв може да бъде по-специално случаят с особено тежки престъпления в областта на детската порнография, като придобиването, разпространението, предаването или предоставянето 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).

155 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 133 от настоящото решение съдебна практика, и че в съответствие с посоченото в точка 109 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 запазване 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, 8,11 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.

156 Предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, до която може да доведе това запазване, 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 продължителността на запазване 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.

157 Накрая, що се отнася до данните за самоличността на ползвателите на електронни съобщителни средства, тези данни сами по себе си не позволяват да се установи нито датата, часът, продължителността и адресатите на комуникациите, нито местата, на които те са осъществени, или тяхната честота с определени лица през даден период, така че освен координати като адресите на лицата те не предоставят никаква информация относно дадените комуникации и следователно относно техния личен живот. Поради това намесата, до която води запазването на тези данни, по принцип не може да бъде квалифицирана като „тежка“ (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 59 и 60).

158 От това следва, че в съответствие с изложеното в точка 140 от настоящото решение законодателните мерки, насочени към обработването на тези данни като такива, по-специално тяхното запазване и достъпът до тях единствено с цел да се установи самоличността на съответният ползвател, без посочените данни да могат се свържат с информация за осъществяваната комуникация, могат да бъдат обосновани от целта за превенция, разследване, разкриване и преследване общо на престъпления, посочена в член 15, параграф 1, първо изречение от Директива 2002/58 (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 62).

159 При тези условия, като се има предвид необходимостта да се съвместят разглежданите права и интереси и по изложените в точки 131 и 158 от настоящото решение съображения, следва да се приеме, че дори при липса на връзка между всички ползватели на електронни съобщителни средства и преследваните цели член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата допуска законодателна мярка, налагаща на доставчиците на електронни съобщителни услуги да запазват за неопределен период данните за самоличността на всички ползватели на електронни съобщителни средства за целите на превенция, разследване, разкриване и преследване на престъпления и за опазване на обществената сигурност, без да е необходимо престъпленията и заплахите за или посегателствата върху обществената сигурност да са тежки.

– По законодателните мерки, предвиждащи бързото запазване на данни за трафик и на данни за местонахождение за целите на борбата с тежката престъпност

160 Що се отнася до данните за трафик и до 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 въз основа на законодателни мерки, приети съгласно член 15, параграф 1 от нея, като описаните в точки 134—159 от настоящото решение, следва да се отбележи, че по принцип тези 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 тази директива.

161 По време на това обработване и съхранение обаче 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.

162 В това отношение следва да се отбележи, че член 14 от Конвенцията за престъпления в кибернетичното пространство на Съвета на Европа от 23 ноември 2001 г. (Серия от европейски договори — № 185), подписана от 27-те държави членки и ратифицирана от 25 от тях, чиято цел е да улесни борбата с престъпленията, извършени посредством компютърни мрежи, предвижда, че за целите на конкретни наказателни разследвания или производства договарящите страни приемат редица мерки относно вече съхраняваните данни за трафика, като бързото запазване на тези данни. По-конкретно член 16, параграф 1 от тази конвенция предвижда, че договарящите страни приемат необходимите законодателни мерки, за да дадат възможност на компетентните си органи да разпоредят или да осигурят по друг начин бързото запазване на данните за трафика, които се съхраняват посредством компютърна система, по-конкретно в случаите, в които съществуват основания да се смята, че тези данни са особено уязвими към опасностите от загубване или изменяне.

163 В положение като посоченото в точка 161 от настоящото решение, с оглед на посочена в точка 130 от него 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 разпоредят на доставчиците на електронни съобщителни услуги да извършват за определен срок бързо запазване на данните за трафик и на данните за местонахождение, с които разполагат.

164 Доколкото целта на такова бързо запазване 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 за определени цели, държавите членки трябва да уточнят в законодателството си целта, за която може да се осъществи бързото запазване на данните. Предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, която може да включва такова запазване, тази намеса може да бъде обоснована единствено с борбата с тежката престъпност и a fortiori, с опазването на националната сигурност. Освен това, за да се гарантира, че намесата, която води до такава мярка, е сведена до строго необходимото, от една страна, задължението за запазване следва да се отнася само до данните за трафик и данните за местонахождение, които могат да допринесат за разкриването на тежко престъпление или на посегателство върху съответната национална сигурност. От друга страна, периодът на запазване на данните трябва да бъде ограничен до строго необходимото, като той все пак може да бъде удължен, когато обстоятелствата и целта на посочената мярка оправдават това.

165 В това отношение е важно да се уточни, че такова бързо запазване не трябва да се ограничава до данните на лицата, конкретно заподозрени в извършване на престъпление или на посегателство срещу националната сигурност. 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 133 от настоящото решение, подобна мярка може, в зависимост от избора на законодателя 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 за националната сигурност, като например данните на пострадалото от него лице, неговото социално или професионално обкръжение, или за определени географски райони, като мястото на извършване или подготовка на разследваното престъпление или на посегателство върху националната сигурност. Освен това достъпът на компетентните органи до така запазените данни трябва да се осъществява при спазване на условията, произтичащи от съдебната практика по тълкуването на Директива 2002/58 (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 118—121 и цитираната съдебна практика).

166 Следва също така да се добави, че както следва по-специално от точки 115 и 133 от настоящото решение, достъпът до данни за трафик и до данни за местонахождение, запазени от доставчиците в приложение на мярка, приета на основание член 15, параграф 1 от Директива 2002/58, по принцип може да бъде обоснован само с целта от общ интерес, за която тези доставчици са длъжни да ги съхраняват. От това по-специално следва, че достъп до такива данни не може в никакъв случай да се предостави с цел наказателно преследване и наказване на обикновено престъпление, когато запазването им е било обосновано от целта за борба с тежката престъпност или, a fortiori, за опазване на националната сигурност. За сметка на това в съответствие с принципа на пропорционалност, посочен в точка 131 от настоящото решение, достъпът до запазените данни с оглед на борбата с тежката престъпност може да бъде обоснован с целта за опазване на националната сигурност, стига да са спазени посочените в предходната точка материални и процесуални условия, съпровождащи такъв достъп.

167 В това отношение държавите членки могат да предвидят в законодателството си, че при спазване на същите тези материални и процесуални условия достъпът до данни за трафик и до данни за местонахождение може да се осъществи за целите на борбата с тежката престъпност или за опазването на националната сигурност, когато тези данни са запазени от доставчик в съответствие с членове 5, 6 и 9 или с член 15, параграф 1 от Директива 2002/58.

168 С оглед на всички гореизложени съображения на първите въпроси по дела C-511/18 и C-512/18, както и на първия и втория въпрос по дело C-520/18 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 законодателни мерки, които предвиждат превантивно общо и неизбирателно запазване на данни за трафик и на данни за местонахождение за целите, предвидени в посочения член 15, параграф 1. Обратно, посоченият член 15, параграф 1 във връзка с членове 7, 8 и 11, както и с член 52, параграф 1 от Хартата допуска законодателни мерки:

– позволяващи с оглед опазването на националната сигурност да се разпореди доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно запазване 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, предвиждащо това разпореждане, трябва да подлежи на ефективен контрол от

юрисдикция 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,

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

– предвиждащи общо и неизбирателно запазване на данни относно самоличността на ползвателите на електронни съобщителни средства за целите на опазването на националната сигурност, на борбата с престъпността и на опазването на обществената сигурност, 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 запазване 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 запазването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби.

По втория и третия въпрос по дело C-511/18

169 С втория и третия въпрос по дело C-511/18 запитващата юрисдикция иска по същество да се установи дали 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 налага на доставчиците на електронни съобщителни услуги да прилагат в своите мрежи мерки, позволяващи, от една страна, автоматизиран анализ и събиране в реално време на данни за трафик и на данни за местонахождение и от друга страна, събиране в реално време на технически данни за местонахождението на използваните крайни устройства, без да е предвидено уведомяване на лицата, засегнати от това обработване и събиране.

170 Запитващата юрисдикция уточнява, че предвидените в членове L. 851-2—L. 851-4 от CSI средства за събиране на разузнавателна информация не налагат за доставчиците на електронни съобщителни услуги конкретно изискване за запазване на данни за трафик и на

данни за местонахождение. Що се отнася по-конкретно до автоматизирания анализ, посочен в член L. 851-3 от CSI, тази юрисдикция отбелязва, че целта на обработката е да се установят, в зависимост от определените за тази цел критерии, свързвания с интернет, които могат да разкрият терористична заплаха. Що се отнася до предвиденото в член L. 851-2 от CSI събиране в реално време, тази юрисдикция посочва, че то се отнася единствено до едно или повече лица, за които преди това е установено, че могат да имат връзка с терористична заплаха. Според същата юрисдикция тези две технически средства могат да се използват само с цел предотвратяване на тероризма и се отнасят до данните, посочени в членове L. 851-1 и R. 851-5 от CSI.

171 В самото начало следва да се уточни, че обстоятелството, че съгласно член L. 851-3 от CSI предвиденият в него автоматизиран анализ не позволява сам по себе си да се установи самоличността на ползвателите, чиито данни са подложени на такъв анализ, не е пречка такива данни да се квалифицират като „лични данни“. Всъщност, след като процедурата, предвидена в точка IV от същата разпоредба, позволява на по-късен етап да се установи самоличността на лицето или лицата, за които се отнасят данните, за които автоматизираният анализ е разкрил, че могат да обуславят наличието на терористична заплаха, всички лица, чиито данни са предмет на автоматизиран анализ, могат да бъдат идентифицирани въз основа на тези данни. Съгласно определението за лични данни по член 4, точка 1 от Регламент 2016/679 обаче такива данни представляват информацията, свързана по-специално с лице, което може да бъде идентифицирано.

По автоматизирания анализ на данни за трафик и на данни за местонахождение

172 От член L. 851-3 от CSI следва, че предвиденият в него автоматизиран анализ по същество съответства на филтриране на всички данни за трафик и данни за местонахождение, запазени от доставчиците на електронни съобщителни услуги, извършено от последните по искане на компетентните национални органи и в изпълнение на определените от тях критерии. От това следва, че всички данни на ползвателите на електронни съобщителни средства се проверяват, ако съответстват на тези критерии. Ето защо трябва да се приеме, че подобен автоматизиран анализ предполага съответните доставчици на електронни съобщителни услуги да извършват за сметка на компетентния орган общо и неизбирателно обработване под формата на употреба чрез автоматични средства по смисъла на член 4, точка 2 от Регламент 2016/679, което обхваща всички данни за трафик и данни за местонахождение на всички ползватели на електронни съобщителни средства. Това обработване не зависи от последващо събиране на данни за лицата, идентифицирани след автоматизирания анализ, което е разрешено на основание член L. 851-3, [параграф] IV от CSI.

173 Национална правна уредба, която разрешава подобен автоматизиран анализ на данни за трафик и на данни за местонахождение, обаче допуска изключение от предвиденото в член 5 от Директива 2002/58 принципно задължение да се гарантира поверителността на електронните съобщения и свързаните с тях данни. Подобна правна уредба също съставлява намеса в основните права, закрепени в членове 7 и 8 от Хартата, независимо от последващото използване на тези данни. Накрая, в съответствие със съдебната практика, цитирана в точка 118 от настоящото решение, посочената правна уредба може да има възпиращо действие върху упражняването на свободата на изразяване на мнение, закрепена в член 11 от Хартата.

174 Освен това намесата, произтичаща от автоматизиран анализ на данни за трафик и на данни за местонахождение като разглежданата в главното производство, се оказва особено тежка, тъй като обхваща общо и неизбирателно данните на лицата, които използват електронни съобщителни средства. Тази констатация се налага с още по-голяма сила, когато, както следва от разглежданата в главното производство национална правна уредба, данните, предмет на автоматизирания анализ, могат да разкрият естеството на информацията, до която е осъществяван достъп в интернет. Освен това такъв автоматизиран анализ се прилага общо за всички лица, използващи електронни съобщителни средства, а следователно и за тези, за които не съществува никаква улика, даваща основание да се счита, че действията им биха могли да имат някаква, дори непряка или далечна, връзка с терористични дейности.

175 Що се отнася до обосноваването на подобна намеса, следва да се уточни, че изискването по член 52, параграф 1 от Хартата всяко ограничение на упражняването на основни права да бъде предвидено в закон, означава, че самото правно основание, позволяващо тази намеса, трябва да определя обхвата на ограничението при упражняване на съответното право (вж. в този смисъл решение от 16 юли 2020 г., Facebook Ireland и Schrems, C-311/18, EU:C:2020:559, т. 175 и цитираната съдебна практика).

176 Освен това, за да бъде изпълнено припомненото в точки 130 и 131 от настоящото решение изискване за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото, национална правна уредба, която урежда достъпа на компетентните органи до запазените данни за трафик и данни за местонахождение, трябва да отговаря на изискванията, произтичащи от цитираната в точка 132 от настоящото решение съдебна практика. По-конкретно такава правната уредба не може да се ограничи до изискването достъпът на органите до тези данни да отговаря на целта на тази правна уредба, а трябва да предвижда също и материални и процесуални условия за това използване (вж. по аналогия становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 192 и цитираната съдебна практика).

177 В това отношение следва да се припомни, че особено сериозната намеса, произтичаща от общото и неизбирателно запазване на данни за трафик и на данни за местонахождение, посочена в съображенията в точки 134—139 от настоящото решение, както и особено сериозната намеса, която представлява автоматизираният им анализ, могат да отговорят на изискването за пропорционалност само в случаи, при които държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, и при условие че продължителността на това запазване е ограничена до строго необходимото.

178 В случаи като посочените в предходната точка може да се приеме, че извършването на автоматизиран анализ на данни за трафик и на данни за местонахождение на всички ползватели на електронни съобщителни средства и за строго ограничен период от време може да се счита за обосновано с оглед на изискванията, произтичащи от член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

179 При това положение, за да се гарантира, че прибягването до такава мярка действително се ограничава до строго необходимото за защита на националната сигурност, и по-специално за предотвратяването на тероризма, от съществено значение е, в съответствие с

установеното в точка 139 от настоящото решение, решението, с което се разрешава автоматизираният анализ, да подлежи на ефективен контрол, осъществяван от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, обосноваващи въпросната мярка, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени.

180 В това отношение следва да се уточни, че предварително изготвените модели и критерии, на които се основава този вид обработване на данни, трябва да бъдат, от една страна, конкретни и надеждни, като позволяват достигане до резултати, изразяващи се в идентифицирането на лица, по отношение на които може да съществува разумно подозрение за участие в терористични престъпления, а от друга страна — недискриминационни (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 172).

181 Освен това е важно да се припомни, че всеки автоматизиран анализ, извършен въз основа на модели и критерии, изхождащи от положението, че расовият или етнически произход, политическите възгледи, религиозните или философските убеждения, членството в професионални съюзи, здравословното състояние или сексуалния живот на дадено лице сами по себе си и независимо от индивидуалното поведение на това лице биха могли се окажат релевантни с оглед на предотвратяването на тероризма, би бил в нарушение на гарантираните в членове 7 и 8 от Хартата права, разгледани във връзка с член 21 от нея. В този смисъл предварително изготвените модели и критерии за целите на автоматизиран анализ с цел предотвратяване на терористични действия, представляващи сериозна заплаха за националната сигурност, не могат да се основават само на тези чувствителни данни (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 165).

182 Освен това, тъй като автоматизираните анализи на данни за трафик и на данни за местонахождение по необходимост включват определена степен на грешки, всеки положителен резултат, получен вследствие на автоматизирано обработване, трябва да премине през индивидуално преразглеждане с неавтоматизирани средства преди приемането на индивидуална мярка с неблагоприятно въздействие върху съответните лица, като например последващото събиране на данни за трафик и на данни за местонахождение в реално време, като подобна мярка всъщност не може да се основава само на резултата от автоматизираното обработване. Също така, за да се гарантира на практика, че предварително изготвените модели и критерии, тяхното използване, както и прилаганите бази данни са с недискриминационен характер и се ограничават до строго необходимото с оглед на целта да се предотвратят терористични действия, представляващи сериозна заплаха за националната сигурност, надеждността и актуалността на тези предварително изготвени модели и критерии, както и прилаганите бази данни трябва да бъдат редовно преразглеждани (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 173 и 174).

По събирането в реално време на данни за трафик и на данни за местонахождение

183 Що се отнася до предвиденото в член L. 851-2 от CSI събиране на данни за трафик и на данни за местонахождение в реално време, следва да се отбележи, че то може да бъде разрешено за всеки отделен случай по отношение на „лице, за което преди това е установено, че може да има връзка с [терористична] заплаха“. Също така според тази

разпоредба, „когато са налице сериозни основания да се счита, че едно или повече лица от обкръжението на лицето, за което се отнася разрешението, могат да предоставят данни, свързани с целта, за която е издадено разрешението, то може също да бъде предоставено за всяко от тези лица поотделно“.

184 Данните, които са предмет на мярка от такова естество, позволяват на компетентните национални органи през периода на разрешението да наблюдават непрекъснато и в реално време събеседниците, с които се свързват съответните лица, използваните от тях средства, продължителността на осъществяваните от тях комуникации, както и мястото им на пребиваване и техните пътувания. Освен това те явно биха могли да разкрият естеството на информацията, до която е осъществяван достъп в интернет. Както следва от точка 117 от настоящото решение, от тези данни, разгледани в съвкупност, е възможно да се изведат много точни заключения за личния живот на съответните лица и те предоставят средства да се установи профилът им — информация, която с оглед на правото на зачитане на личния живот е също толкова чувствителна, колкото е и самото съдържание на съобщенията.

185 Що се отнася до предвиденото в член L. 851-4 от CSI събиране на данни в реално време, тази разпоредба разрешава събирането на технически данни за местонахождението на крайните устройства и предаването в реално време на подчинена на министър-председателя служба. Изглежда, тези данни позволяват на компетентната служба по всяко време през периода на разрешението непрекъснато и в реално време да установяват местонахождението на използваните крайни устройства, като например мобилни телефони.

186 Национална правна уредба, която разрешава такова събиране в реално време, подобно на уредбата, която разрешава автоматизирания анализ на данните, обаче съставлява изключение от предвиденото в член 5 от Директива 2002/58 принципно задължение да се гарантира поверителността на електронните съобщения и свързаните с тях данни. При това положение тя съставлява също намеса в основните права, закрепени в членове 7 и 8 от Хартата, и може да има възпиращо действие върху упражняването на гарантираната в член 11 от Хартата свобода на изразяване на мнение.

187 Следва да се подчертае, че намесата, която включва събирането в реално време на данните, позволяващи да се установи местонахождението на крайно устройство, изглежда особено сериозна, тъй като тези данни предоставят на компетентните национални органи средство за точно и постоянно проследяване на придвижването на лицата, които ползват мобилни телефони. Доколкото по посочените причини тези данни трябва да се считат за особено чувствителни, достъпът на компетентните органи до такива данни в реално време трябва да се разграничава от отложения във времето достъп до тях, тъй като първият представлява още по-интензивна намеса, защото позволява почти пълно наблюдение на тези потребители (вж. по аналогия относно член 8 от ЕКПЧ, ЕСПЧ, решение от 8 февруари 2018 г., Ben Faiza с/у Франция, CE:ECHR:2018:0208JUD003144612, § 74). Освен това интензивността на тази намеса се увеличава, когато събирането в реално време обхваща също данните за трафика на съответните лица.

188 Макар с оглед на важността си целта за предотвратяване на тероризма, преследвана от разглежданата в главното производство национална правна уредба, да може да обоснове намесата, която включва събирането в реално време на данни за трафик и на данни за местонахождение, предвид характера ѝ на особено сериозна намеса такава мярка може да се приложи само по отношение на лицата, за които съществува основателна причина да се

подозира, че участват по един или друг начин в терористични дейности. Що се отнася до данните на лицата, които не попадат в тази категория, те могат да бъдат предмет само на отложен във времето достъп, който съгласно практиката на Съда може да се осъществява само в особени случаи, като такива, в които става въпрос за терористични действия, и ако съществуват обективни обстоятелства, позволяващи да се приеме, че в случая тези данни действително биха могли да подпомогнат борбата с тероризма (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 119 и цитираната съдебна практика).

189 Освен това решението, с което се разрешава събиране в реално време на данни за трафик и на данни за местонахождение, трябва да се основава на обективни критерии, предвидени в националното законодателство. По-специално в съответствие с цитираната в точка 176 от настоящото решение съдебна практика това законодателство трябва да определи обстоятелствата и условията, при които може да бъде разрешено подобно събиране, и да предвиди, както бе уточнено в предходната точка, че могат да бъдат обхванати само лицата, които имат връзка с целта за предотвратяване на тероризма. Освен това решението, с което се разрешава събиране в реално време на данни за трафик и на данни за местонахождение, трябва да се основава на обективни и недискриминационни критерии, предвидени в националното законодателство. За да се гарантира на практика спазването на тези условия, от съществено значение е прилагането на мярката за разрешаване на събиране в реално време да подлежи на предварителен контрол, осъществяван от юрисдикция или от независима административна структура, чието решение има обвързващо действие, като тази юрисдикция или структура трябва по-специално да се увери, че подобно събиране в реално време е разрешено само в границите на строго необходимото (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 120). В надлежно обосновани спешни случаи контролът трябва да бъде осъществен в кратък срок.

По уведомяването на лицата, чиито данни са били събрани или анализирани

190 Важно е компетентните национални органи, които събират данни за трафик и данни за местонахождение в реално време, да уведомят за това засегнатите лица в рамките на приложимите национални процедури, при условие че и едва след като това не може да попречи на изпълнението на задачите на тези органи. Всъщност тази информация е фактически необходима, за да се позволи на тези лица да упражнят правата си, произтичащи от членове 7 и 8 от Хартата, да поискат достъп до техните лични данни, които са предмет на тези мерки, и евентуално тяхното поправяне или заличаване, както и в съответствие с член 47, първа алинея от Хартата да подадат ефективна жалба пред съда, като това право впрочем е изрично гарантирано в член 15, параграф 2 от Директива 2002/58 във връзка с член 79, параграф 1 от Регламент 2016/679 (вж. в този смисъл решение от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 121 и цитираната съдебна практика и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 219 и 220).

191 Що се отнася до информацията, която се изисква при автоматизиран анализ на данни за трафик и на данни за местонахождение, компетентният национален орган е длъжен да публикува обща информация относно този анализ, без да е длъжен да предоставя индивидуална информация на съответните лица. За сметка на това, когато данните отговарят на параметрите, уточнени в мярката, с която се разрешава автоматизирания анализ, и този орган идентифицира съответното лице, за да анализира по-задълбочено

отнасящите се до него данни, е необходимо индивидуално уведомяване на това лице. Подобна информация трябва да се дава обаче, при условие че и едва след като това вече не може да попречи на изпълнението на задачите на въпросния орган (вж. по аналогия становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 222—224).

192 С оглед на всички гореизложени съображения на втория и третия въпрос по дело C-511/18 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 допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги, от една страна, да използват автоматизиран анализ, както и да събират в реално време по-специално данни за трафик и данни за местонахождение, и от друга страна, да събират в реално време технически данни за местонахождението на използваните крайни устройства, ако

– използването на автоматизирания анализ се ограничава до положения, при които държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, като прибягването до този анализ трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, обосноваващи въпросната мярка, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени, и

– прибягването до събиране в реално време на данни за трафик и на данни за местонахождение се ограничава до лицата, за които съществува основателна причина да се подозира, че участват по един или друг начин в терористични дейности, и подлежи на предварителен контрол, осъществяван от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се увери, че такова събиране в реално време е разрешено само в границите на строго необходимото. В надлежно обосновани спешни случаи контролът трябва да бъде осъществен в кратък срок.

По втория въпрос по дело C-512/18

193 С втория въпрос по дело C-512/18 запитващата юрисдикция иска по същество да се установи дали разпоредбите на Директива 2000/31 във връзка с членове 6—8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкуват в смисъл, че не допускат национална правна уредба, която налага на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги задължение за общо и неизбирателно запазване по-специално на лични данни, свързани с тези услуги.

194 Макар да счита, че такива услуги попадат в приложното поле на Директива 2000/31, а не на Директива 2002/58, запитващата юрисдикция изразява мнение, че член 15, параграфи 1 и 2 от Директива 2000/31 във връзка с членове 12 и 14 от нея не въвежда сам по себе си принципна забрана за запазване на данни, свързани със създаването на съдържание, от която може само в краен случай да се допуска изключение. Тази юрисдикция обаче иска да се установи дали тази преценка може да се възприеме предвид необходимостта да се зачитат основните права, закрепени в членове 6—8 и 11 от Хартата.

195 Освен това запитващата юрисдикция уточнява, че нейният въпрос се отнася до задължението за запазване, предвидено в член 6 от LCEN във връзка с Декрет № 2011-219. Данните, които съответните доставчици на услуги трябва да съхраняват на това основание, включват по-специално данните за самоличността на лицата, които са използвали тези услуги, като име, фамилно име, съответните им пощенски адреси, свързаните с тях адреси за електронна поща или адреси на профил, паролите им, а когато сключването на договора или създаването на профила е срещу заплащане — вида на плащането, референция на плащането, данните за размера, датата и часа на трансакцията.

196 Освен това данните, обхванати от задължението за запазване, включват идентификаторите на абонатите, свързванията с интернет и използваните крайни устройства, идентификаторите, дадени на съдържанието, датата и часа на начало и край на свързването и на действията, както и видовете протоколи, използвани за свързването към услугата и за прехвърлянето на съдържанието. Достъпът до тези данни, периодът на запазване на които е една година, може да бъде поискан в рамките на наказателни и граждански производства, за да се осигури спазването на правилата относно гражданската или наказателната отговорност, както и в рамките на мерки за събиране на разузнавателна информация, към които се прилага член L. 851-1 от CSI.

197 В това отношение следва да се отбележи, че съгласно член 1, параграф 2 от Директива 2000/31 тя сближава някои приложими към услугите на информационното общество национални разпоредби, посочени в член 2, буква а) от нея.

198 Такива услуги действително обхващат услугите, предоставяни на разстояние посредством електронно оборудване за обработка и съхраняване на данни, при индивидуално поискване от страна на получателя на услугите, обикновено срещу заплащане, като услугите за предоставяне на достъп до интернет или до съобщителна мрежа и услугите за съхраняване на информация (вж. в този смисъл решения от 24 ноември 2011 г., Scarlet Extended, C-70/10, EU:C:2011:771, т. 40, от 16 февруари 2012 г., SABAM, C-360/10, EU:C:2012:85, т. 34, от 15 септември 2016 г., Mc Fadden, C-484/14, EU:C:2016:689, т. 55 и от 7 август 2018 г., SNB-REACT, C-521/17, EU:C:2018:639, т. 42 и цитираната съдебна практика).

199 При все това член 1, параграф 5 от Директива 2000/31 предвижда, че тя не се прилага за въпроси, които се отнасят до услуги на информационното общество, които са предмет на директиви 95/46 и 97/66. В това отношение от съображения 14 и 15 от Директива 2000/31 следва, че защитата на поверителността на съобщенията, както и на физическите лица при обработването на лични данни в рамките на услугите на информационното общество, се урежда единствено от Директива 95/46 и Директива 97/66, като последната забранява, с оглед на защитата на поверителността на съобщенията, в член 5 всяка форма на прихващане или наблюдение на съобщенията.

200 Така въпросите, свързани със защитата на поверителността на съобщенията и на личните данни, трябва да се преценяват с оглед на Директива 2002/58 и на Регламент 2016/679, тъй като те са заменили съответно Директива 97/66 и Директива 95/46, като следва да се уточни, че защитата, която Директива 2000/31 цели да осигури, при всички положения не може да засяга изискванията, произтичащи от Директива 2002/58 и от Регламент 2016/679 (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 57).

201 Следователно, както по същество отбелязва генералният адвокат в точка 141 от заключението си по съединени дела La Quadrature du Net и др. (C-511/18 и C-512/18, EU:C:2020:6), задължението, наложено с посочената в точка 195 от настоящото решение национална правна уредба на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги, да запазват лични данни, свързани с тези услуги, трябва да се преценява с оглед на Директива 2002/58 или на Регламент 2016/679.

202 Така в зависимост от това дали предоставянето на услугите, обхванати от тази национална правна уредба, попада в приложното поле на Директива 2002/58, то се урежда или от тази директива, и по-специално от член 15, параграф 1 от нея във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, или от Регламент 2016/679, и по-специално от член 23, параграф 1 от посочения регламент във връзка със същите разпоредби от Хартата.

203 В случая не може да се изключи, както отбелязва Европейската комисия в писменото си становище, че някои услуги, към които се прилага посочената в точка 195 от настоящото решение национална правна уредба, съставляват електронни съобщителни услуги по смисъла на Директива 2002/58, което запитващата юрисдикция следва да провери.

204 В това отношение следва да се отбележи, че Директива 2002/58 обхваща електронните съобщителни услуги, които отговарят на условията по член 2, буква в) от Директива 2002/21, към който препраща член 2 от Директива 2002/58 и който определя електронната съобщителна услуга като „услуга, осигурявана обикновено срещу заплащане, която се състои изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи, включително далекосъобщителни услуги и предавателни услуги в мрежи, използвани за разпръскване“. Що се отнася до услугите на информационното общество, като посочените в точки 197 и 198 от настоящото решение и обхванати от Директива 2000/31, те представляват електронни съобщителни услуги, при положение че се състоят изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи (вж. в този смисъл решение от 5 юни 2019 г., Skype Communications, C-142/18, EU:C:2019:460, т. 47 и 48).

205 В този смисъл, услугите за достъп до интернет, които, изглежда, са обхванати от посочената в точка 195 от настоящото решение национална правна уредба, представляват електронни съобщителни услуги по смисъла на Директива 2002/21, както се потвърждава от съображение 10 от нея (вж. в този смисъл решение от 5 юни 2019 г., Skype Communications, C-142/18, EU:C:2019:460, т. 37). Такъв е и случаят с услугите за електронна поща по интернет, за които не може да се изключи, че също са обхванати от тази национална правна уредба, доколкото в технически план включват изцяло или главно пренасянето на сигнали по електронни съобщителни мрежи (вж. в този смисъл решение от 13 юни 2019 г., Google, C-193/18, EU:C:2019:498, т. 35 и 38).

206 Що се отнася до изискванията, произтичащи от член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, следва да се препрати към всички съображения и изводи, направени в рамките на отговора на първите въпроси по дела C-511/18 и C-512/18, както и на първия и втория въпрос по дело C-520/18.

207 Що се отнася до произтичащите от Регламент № 2016/679 изисквания, следва да се припомни, че той има за цел по-специално, както личи от съображение 10 от него, да гарантира високо ниво на защита на физическите лица в Съюза и за целта да гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на

основните права и свободи на тези лица във връзка с обработването на лични данни (вж. в този смисъл решение от 16 юли 2020 г., Facebook Ireland и Schrems, C-311/18, EU:C:2020:559, т. 101).

208 За тази цел, при спазване на допустимите съгласно член 23 от Регламент 2016/679 изключения, всяко обработване на лични данни трябва да зачита принципите, уреждащи обработването на личните данни, както и правата на субекта на данните, установени съответно в глави II и III от този регламент. По-конкретно всяко обработване на лични данни, от една страна, трябва да е в съответствие с принципите, прогласени в член 5 от посочения регламент, и от друга страна, да отговаря на изискванията за законосъобразност, изброени в член 6 от същия (вж. по аналогия, що се отнася до Директива 95/46, решение от 30 май 2013 г., Worten, C-342/12, EU:C:2013:355, т. 33 и цитираната съдебна практика).

209 Що се отнася по-специално до член 23, параграф 1 от Регламент 2016/679, следва да се отбележи, че подобно на предвиденото в член 15, параграф 1 от Директива 2002/58, той позволява на държавите членки да ограничат обхвата на посочените в него задължения и права с оглед на целите, които предвижда, и посредством законодателни мерки, „когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира“ преследваната цел. Всяка приета на това основание законодателна мярка трябва по-специално да отговаря на специалните изисквания, предвидени в член 23, параграф 2 от този регламент.

210 Така член 23, параграфи 1 и 2 от Регламент 2016/679 не може да се тълкува в смисъл, че може да предостави на държавите членки правомощието в нарушение на член 7 от Хартата да накърняват зачитането на личния живот, както и другите предвидени в нея гаранции (вж. по аналогия, що се отнася до Директива 95/46, решение от 20 май 2003 г., Österreichischer Rundfunk и др., C-465/00, C-138/01 и C-139/01, EU:C:2003:294, т. 91). По-конкретно, подобно на това, което важи за член 15, параграф 1 от Директива 2002/58, правомощието, което член 23, параграф 1 от Регламент 2016/679 предоставя на държавите членки, може да се упражнява само при спазване на изискването за пропорционалност — дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото (вж. по аналогия, що се отнася до Директива 95/46, решение от 7 ноември 2013 г., IPI, C-473/12, EU:C:2013:715, т. 39 и цитираната съдебна практика).

211 От това следва, че констатациите и изводите, направени в рамките на отговора на първите въпроси по дела C-511/18 и C-512/18, както и на първия и втория въпрос по дело C-520/18, се прилагат mutatis mutandis към член 23 от Регламент 2016/679.

212 С оглед на изложените по-горе съображения на втория въпрос по дело C-512/18 следва да се отговори, че Директива 2000/31 трябва да се тълкува в смисъл, че не е приложима в областта на защитата на поверителността на съобщенията и на физическите лица при обработването на лични данни в рамките на услугите на информационното общество, тъй като тази защита според случая се урежда от Директива 2002/58 или от Регламент 2016/679. Член 23, параграф 1 от Регламент 2016/679 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 налага на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги задължение за общо и неизбирателно запазване по-специално на лични данни, свързани с тези услуги.

По третия въпрос по дело C-520/18

213 С третия въпрос по дело C-520/18 запитващата юрисдикция иска по същество да се установи дали национална юрисдикция може да приложи разпоредба от националното си право, която я оправомощава да ограничи във времето действието на обявяването на незаконосъобразността — възложено ѝ по силата на това право по отношение на национално законодателство, което налага на доставчиците на електронни съобщителни услуги, с оглед, наред с другото, на преследването на целите за опазване на националната сигурност и за борба с престъпността, общо и неизбирателно запазване на данни за трафик и на данни за местонахождение — която произтича от несъвместимостта на това законодателство с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

214 Принципът на предимство на правото на Съюза утвърждава върховенството на правото на Съюза над правото на държавите членки. Този принцип съответно задължава всички институции на държавите членки да осигурят пълното действие на различните норми на Съюза, като правото на държавите членки не може да накърнява признатото действие на тези различни норми на територията на посочените държави (решения от 15 юли 1964 г., Costa, 6/64, EU:C:1964:66, стр. 1159 и 1160 и от 19 ноември 2019 г., A. K. и др. (Независимост на Дисциплинарната колегия на Върховния съд), C-585/18, C-624/18 и C-625/18, EU:C:2019:982, т. 157 и 158 и цитираната съдебна практика).

215 По силата на принципа на предимство, при липса на правомощие да тълкува националната правна уредба в съответствие с изискванията на правото на Съюза, националният съд, натоварен в рамките на своята компетентност с прилагането на разпоредбите от правото на Съюза, е длъжен да гарантира пълното им действие, като при необходимост по собствена инициатива оставя без приложение противоречащите им разпоредби от националното законодателство, дори да са по-късни, без да е необходимо да иска или да изчаква тяхната предварителна отмяна по законодателен път или по какъвто и да било друг ред, предвиден в конституцията (решения от 22 юни 2010 г., Melki и Abdeli, C-188/10 и C-189/10, EU:C:2010:363, т. 43 и цитираната съдебна практика, от 24 юни 2019 г., Popławski, C-573/17, EU:C:2019:530, т. 58 и от 19 ноември 2019 г., A. K. и др. (Независимост на Дисциплинарната колегия на Върховния съд), C-585/18, C-624/18 и C-625/18, EU:C:2019:982, т. 160).

216 Единствено Съдът може по изключение и поради императивни съображения за правна сигурност временно да отложи последиците, изразяващи се в неприлагането на национално право, противоречащо на норма на правото на Съюза. Такова ограничение във времето на действието на даденото от Съда тълкуване на това право се допуска единствено в самото решение по искането за тълкуване (вж. в този смисъл решения от 23 октомври 2012 г., Nelson и др., C-581/10 и C-629/10, EU:C:2012:657, т. 89 и 91, от 23 април 2020 г., Herst, C-401/18, EU:C:2020:295, т. 56 и 57 и от 25 юни 2020 г., A и др. (Вятърни генератори в Алтер и Невеле), C-24/19, EU:C:2020:503, т. 84 и цитираната съдебна практика).

217 Ако националните юрисдикции бяха оправомощени, дори и временно, да дадат предимство пред правото на Съюза на противоречащи му национални разпоредби, това би застрашило предимството и еднаквото прилагане на правото на Съюза (вж. в този смисъл решение от 29 юли 2019 г., Inter-Environnement Wallonie и Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, т. 177 и цитираната съдебна практика).

218 При все това по дело, отнасящо се до законосъобразността на мерки, приети в нарушение на установеното от правото на Съюза задължение за извършване на предварителна оценка на въздействието на проект върху околната среда и върху дадена защитена територия, Съдът е постановил, че ако вътрешното право позволява това, националната юрисдикция може по изключение да запази последиците на такива мерки, когато това запазване е обосновано от императивни съображения, свързани с необходимостта да се отстрани реална и сериозна заплаха от прекъсване на електроснабдяването на съответната държава членка, на която не би могло да се противодейства с други средства и алтернативи, по-специално в рамките на вътрешния пазар, като посоченото запазване може да бъде само за периода, строго необходим за отстраняването на нередността (вж. в този смисъл решение от 29 юли 2019 г., Inter-Environnement Wallonie и Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, т. 175, 176, 179 и 181).

219 За разлика обаче от неизпълнението на процедурно задължение като изготвянето на предварителна оценка на въздействието на проект в специфичната област на опазването на околната среда, неизпълнението на член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата не може да бъде отстранено чрез процедура, сравнима с посочената в предходната точка. Всъщност запазването на последиците от национално законодателство като разглежданото в главното производство би означавало, че това законодателство продължава да налага на доставчиците на електронни съобщителни услуги задължения, които противоречат на правото на Съюза и които предполагат сериозна намеса в основните права на лицата, чиито данни са запазени.

220 Следователно запитващата юрисдикция не може да приложи разпоредба от националното си право, която я оправомощава да ограничи във времето последиците на възложено ѝ по силата на това право обявяване на незаконосъобразността на разглежданото в главното производство национално законодателство.

221 При това положение в представените пред Съда становища VZ, WY и XX изтъкват, че третият въпрос повдига имплицитно, но неминуемо въпроса дали правото на Съюза допуска използването в рамките на наказателно производство на информацията и доказателствата, получени чрез несъвместимо с това право общо и неизбирателно запазване на данни за трафик и на данни за местонахождение.

222 В това отношение и за да се даде полезен отговор на запитващата юрисдикция, следва да се припомни, че при сегашното състояние на правото на Съюза по принцип само националното право, в рамките на наказателно производство, образувано срещу заподозрени в тежки престъпления лица, може да определи правилата относно допустимостта и преценката на информацията и доказателства, получени чрез подобно запазване на данни в разрез с правото на Съюза.

223 Всъщност съгласно постоянната съдебна практика при липсата на правила на Съюза в тази област, въз основа на принципа на процесуална автономия вътрешният правен ред на всяка държава членка трябва да уреди процесуалните правила за съдебните производства, предназначени да гарантират защитата на правата, които страните в процеса черпят от правото на Съюза, при условие обаче те да не са по-неблагоприятни от правилата, които уреждат подобни положения, подчинени на вътрешното право (принцип на равностойност), и да не правят практически невъзможно или прекомерно трудно упражняването на правата, предоставени от правото на Съюза (принцип на ефективност)

(вж. в този смисъл решения от 6 октомври 2015 г., Târşia, C-69/14, EU:C:2015:662, т. 26 и 27, от 24 октомври 2018 г., XC и др., C-234/17, EU:C:2018:853, т. 21 и 22 и цитираната съдебна практика и от 19 декември 2019 г., Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, т. 33).

224 Що се отнася до принципа на равностойност, националният съд, пред който е образувано наказателно производство, основано на информация или доказателства, получени в нарушение на произтичащите от Директива 2002/58 изисквания, трябва да провери дали националното право, уреждащо това производство, предвижда по-неблагоприятни правила по отношение на допустимостта и използването на такива данни и доказателства от правилата относно данните и доказателствата, получени в нарушение на вътрешното право.

225 Що се отнася до принципа на ефективност, следва да се отбележи, че националните правила относно допустимостта и използването на данните и доказателствата имат за цел съгласно избора, направен от националното право, да се избегне възможността неправомерно придобити данни и доказателства да нанесат неоснователно вреди на лице, заподозряно в извършване на престъпления. Според националното право обаче тази цел може да бъде постигната не само със забрана за използване на такива данни и доказателства, но и с национални правила и практики, регламентиращи преценката и претеглянето на данните и доказателствата, дори чрез отчитане на техния неправомерен характер, при определяне на наказанието.

226 Независимо от това от практиката на Съда следва, че необходимостта от изключване на данните и доказателствата, получени в нарушение на предписанията на правото на Съюза, трябва да се преценява с оглед по-специално на опасността, която допустимостта на такива данни и доказателства представлява за спазването на принципа на състезателност, а следователно и на правото на справедлив съдебен процес (вж. в този смисъл решение от 10 април 2003 г., Steffensen, C-276/01, EU:C:2003:228, т. 76 и 77). Юрисдикция, която счита, че дадена страна не може да обсъди ефикасно доказателствено средство от област, в която са необходими специални познания, каквито съдът няма, и което може да повлияе съществено на преценката на фактите и обстоятелствата, трябва да констатира нарушение на правото на справедлив съдебен процес и да изключи това доказателствено средство, за да се избегне подобно нарушение (вж. в този смисъл решение от 10 април 2003 г., Steffensen, C-276/01, EU:C:2003:228, т. 78 и 79).

227 Следователно принципът на ефективност налага на националния наказателен съд да не взема предвид данни и доказателства, получени чрез несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик и на данни за местонахождение, в рамките на наказателно производство, образувано срещу заподозрени в престъпни деяния лица, ако тези лица не са в състояние да обсъдят ефективно тези данни и доказателства от област, в която са необходими специални познания, каквито съдът няма, и които данни и доказателства могат да повлияят съществено на преценката на фактите и обстоятелствата.

228 С оглед на гореизложените съображения на третия въпрос по дело C-520/18 следва да се отговори, че национална юрисдикция не може да прилага разпоредба от националното си право, която я оправомощава да ограничи във времето последиците на възложено ѝ по силата на това право обявяване на незаконосъобразността на национално законодателство, което налага на доставчиците на електронни съобщителни услуги с оглед по-специално на опазването на националната сигурност и борбата с престъпността общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в разрез с член 15,

параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата. Този член 15, параграф 1, тълкуван в светлината на принципа на ефективност, изисква националният наказателен съд да не взема предвид данни и доказателства, получени чрез несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в рамките на наказателно производство, образувано срещу заподозрени в престъпни деяния лица, ако тези лица не са в състояние да обсъдят ефективно тези данни и доказателства от област, в която са необходими специални познания, каквито съдът няма, и които данни и доказателства могат да окажат съществено влияние върху преценката на фактите и обстоятелствата.

По съдебните разноски

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

По изложените съображения Съдът (голям състав) реши:

1) **Член 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 законодателни мерки, които предвиждат превантивно общо и неизбирателно запазване на данни за трафик и на данни за местонахождение за целите, предвидени в посочения член 15, параграф 1. Обратно, член 15, параграф 1 от Директива 2002/58, изменена с Директива 2009/136, във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права допуска законодателни мерки:**

   – **позволяващи с оглед опазването на националната сигурност да се разпореди на доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно запазване 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, предвиждащо това разпореждане, трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, обосноваващи въпросната мярка, 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,**

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

– **предвиждащи общо и неизбирателно запазване на данни относно самоличността на ползвателите на електронни съобщителни средства за целите на опазването на националната сигурност, на борбата с престъпността и на опазването на обществената сигурност, 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 чрез решение на компетентния орган, подлежащо на ефективен съдебен контрол, да извършват за определен период бързо запазване 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 запазването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби.

2) **Член 15, параграф 1 от Директива 2002/58, изменена с Директива 2009/136, във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права трябва да се тълкува в смисъл, че допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги, от една страна, да използват автоматизиран анализ, както и да събират в реално време по-специално данни за трафик и данни за местонахождение, и от друга страна, да събират в реално време технически данни за местонахождението на използваните крайни устройства, ако:**

– **използването на автоматизирания анализ се ограничава до положения, при които държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, като прибягването до този анализ трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се провери за наличието на едно от тези положения, обосноваващи въпросната мярка, както и за спазването на условията и гаранциите, които трябва да бъдат предвидени, и**

– **прибягването до събиране в реално време на данни за трафик и на данни за местонахождение се ограничава до лицата, за които съществува основателна причина да се подозира, че участват по един или друг начин в терористични дейности, и подлежи на предварителен контрол, осъществяван от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се увери, че подобно събиране в реално време е разрешено само в границите на строго необходимото. В надлежно обосновани спешни случаи контролът трябва да бъде осъществен в кратък срок.**

3) **Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) трябва да се тълкува в смисъл, че не е приложима в областта на защитата на поверителността на съобщенията и на физическите лица при обработването на лични данни в рамките на услугите на информационното общество, като тази защита според случая се урежда от Директива 2002/58, изменена с Директива 2009/136, или от 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. Член 23, параграф 1 от Регламент 2016/679 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права трябва да се тълкува в смисъл, не допуска национална правна уредба, която налага на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги задължение за общо и неизбирателно запазване по-специално на лични данни, свързани с тези услуги.**

4) **Национална юрисдикция не може да прилага разпоредба от националното си право, която я оправомощава да ограничи във времето последиците на възложено ѝ по силата на това право обявяване на незаконосъобразността на национално законодателство, което налага на доставчиците на електронни съобщителни услуги с оглед по-специално на опазването на националната сигурност и борбата с престъпността общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в разрез с член 15, параграф 1 от Директива 2002/58, изменена с Директива 2009/136, във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права. Този член 15, параграф 1, тълкуван в светлината на принципа на ефективност, изисква националният наказателен съд да не взема предвид данни и доказателства, получени чрез несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в рамките на наказателно производство, образувано срещу заподозрени в престъпни деяния лица, ако тези лица не са в състояние да обсъдят ефективно тези данни и доказателства от област, в която са необходими специални познания, каквито съдът няма, и които данни и доказателства могат да окажат съществено влияние върху преценката на фактите и обстоятелствата.**

Подписи