Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

21 декември 2016 година*

[Текст, поправен с определение от 16 март 2017 г.]

„Преюдициално запитване — Електронни съобщения — Обработка на лични данни — Поверителност на електронните съобщения — Защита — Директива 2002/58/ЕО — Членове 5, 6 и 9, както и член 15, параграф 1 — Харта на основните права на Европейския съюз — Членове 7, 8 и 11 и член 52, параграф 1 — Национална правна уредба — Доставчици на електронни съобщителни услуги — Задължение за общо и неизбирателно запазване на данни за трафика и на данни за местонахождението — Национални органи — Достъп до данните — Липса на предварителен контрол от юрисдикция или независим административен орган — Съвместимост с правото на Съюза“

По съединени дела C-203/15 и C-698/15

с предмет преюдициални запитвания, отправени на основание член 267 ДФЕС от Kammarrätten i Stockholm (Административен апелативен съд Стокхолм, Швеция) и от Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение, Обединено кралство) с решения съответно от 29 април 2015 г. и от 9 декември 2015 г., постъпили в Съда на 4 май 2015 г. и на 28 декември 2015 г., в рамките на производства

Tele2 Sverige AB (C-203/15)

срещу

Post- och telestyrelsen,

и

Secretary of State for the Home Department (C-698/15)

срещу

Tom Watson,

Peter Brice,

Geoffrey Lewis,

в присъствието на:

Open Rights Group,

* Езици на производството: английски и шведски.

Privacy International,

The Law Society of England and Wales,

СЪДЪТ (голям състав),

състоящ се от: K. Lenaerts, председател, A. Tizzano, заместник-председател, R. Silva de Lapuerta, T. von Danwitz (докладчик), J. L. da Cruz Vilaça, E. Juhász и M. Vilaras, председатели на състави, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, Ал. Арабаджиев, S. Rodin, F. Biltgen и C. Lycourgos, съдии,

генерален адвокат: H. Saugmandsgaard Øe,

секретар: C. Strömholm, администратор,

предвид решението на председателя на Съда от 1 февруари 2016 г. за разглеждане на дело C-698/15 по реда на бързото производство, предвидено в член 105, параграф 1 от Процедурния правилник на Съда,

предвид изложеното в писмената фаза на производството и в съдебното заседание от 12 април 2016 г.,

като има предвид становищата, представени:

— за Tele2 Sverige AB, от M. Johansson и N. Torgerzon, advokater, както и от E. Lagerlöf и S. Backman,

— за г-н Watson, от J. Welch и E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, както и от D. Rose, QC,

— за г-н Brice и г-н Lewis, от A. Suterwalla и R. de Mello, barristers, R. Drabble, QC, както и от S. Luke, solicitor,

— за Open Rights Group и Privacy International, от D. Carey, solicitor, както и от R. Mehta и J. Simor, barristers,

— за The Law Society of England and Wales, от T. Hickman, barrister, както и от N. Turner,

— за шведското правителство, от A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren и L. Swedenborg, в качеството на представители,

— за правителството на Обединеното кралство, от S. Brandon, L. Christie и V. Kaye, в качеството на представители, подпомагани от D. Beard, G. Facenna и J. Eadie, QC, както и от S. Ford, barrister,

— за белгийското правителство, от J.-C. Halleux, S. Vanrie и C. Pochet, в качеството на представители,

— за чешкото правителство, от M. Smolek и J. Vláčíl, в качеството на представители,

— за датското правителство, от C. Thorning и M. Wolff, в качеството на представители,

— за германското правителство, от T. Henze, M. Hellmann и J. Kemper, в качеството на представители, подпомагани от M. Kottmann и U. Karpenstein, Rechtsanwalte,

— за естонското правителство, от K. Kraavi-Käerdi, в качеството на представител,

— за Ирландия, от E. Creedon, L. Williams и A. Joyce, в качеството на представители, подпомагани от D. Fennelly, BL,

— за испанското правителство, от A. Rubio González, в качеството на представител,

— за френското правителство, от G. de Bergues, D. Colas, F.-X. Bréchot и C. David, в качеството на представители,

— за кипърското правителство, от K. Kleanthous, в качеството на представител,

— за унгарското правителство, от M. Fehér и G. Koós, в качеството на представители,

— за нидерландското правителство, от M. Bulterman, M. Gijzen и J. Langer, в качеството на представители,

— за полското правителство, от B. Majczyna, в качеството на представител,

— за финландското правителство, от J. Heliskoski, в качеството на представител,

— за Европейската комисия, от H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira и J. Vondung, в качеството на представители,

след като изслуша заключението на генералния адвокат, представено в съдебното заседание от 19 юли 2016 г.,

постанови настоящото

Решение

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

2 Запитванията са отправени по два спора, първият от които е между Tele2 Sverige AB и Post- och telestyrelsen (Комитет по пощи и далекосъобщения на Швеция, наричан по-нататък „PTS“) и се отнася до разпореждане на последния за запазване от Tele2 Sverige на данните за трафика и на данните за местонахождението на абонатите му и регистрираните ползватели (дело C-203/15), а вторият — между г-н Tom Watson, г-н Peter Brice и г-н Geoffrey Lewis, от една страна, и Secretary of State for the Home Department (министъра на вътрешните работи на Обединено кралство Великобритания и Северна Ирландия), от друга страна, относно съвместимостта с правото на Съюза на член 1 от Data Retention and Investigatory Powers Act 2014 (Закон от 2014 г. относно запазването на данните и правомощията по разследване, наричан по-нататък „DRIPA“) (дело C-698/15).

Правна уредба

Правото на Съюза

Директива 2002/58

3 Съображения 2, 6, 7, 11, 21, 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-конкретно тя се стреми да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от [същата].

[…]

(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/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)], настоящата директива не се отнася до въпросите за защита на основните права и свободи свързани с дейности, които не се управляват от законодателството на Общността. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 15, параграф 1 от настоящата директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право. Следователно, настоящата директива не засяга възможността на държавите членки да провеждат законно прихващане на електронни комуникации или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с Европейската конвенция за защита на човешките права и основните свободи, 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 [подходящи гаранции] в съответствие с Европейската конвенция за защита на човешките права и основните свободи.

[…]

(21) Трябва да се вземат мерки, за да се предотврати неоторизираният достъп до съобщения, за да се защити конфиденциалният характер на комуникациите, включително както на съдържанията, така и на всякакви данни, свързани с такива съобщения, посредством публични комуникационни мрежи и налични електронни комуникационни услуги. Националното законодателство в някои държави членки забранява само преднамерения неразрешен достъп до съобщения.

(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. […]

[…]

(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. […]“.

4 Член 1 от Директива 2002/58 е озаглавен „Обхват и цел“ и 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 Общността.

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

3. Настоящата директива не се прилага за дейности, които попадат извън обхвата на Договора за създаване на Европейската общност, като тези обхванати от дялове V и VI от Договора за Европейския съюз, 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“.

5 Член 2 от Директива 2002/58 е озаглавен „Дефиниции“ и гласи:

„Освен ако не е предвидено друго, се прилагат дефинициите от Директива [95/46] и от Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно общата регулаторна [рамка] за електронни[те 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].

Прилагат се също следните дефиниции:

[…]

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;

[…]“.

6 Член 3 от Директива 2002/58 е озаглавен „Обхванати услуги“ и предвижда:

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

7 Член 4 от същата директива е озаглавен „Сигурност на обработката“ и гласи:

„1. Доставчикът на публично достъпни електронни комуникационни услуги трябва да вземе подходящи технически и организационни мерки, за да защити сигурността на неговите услуги, ако е необходимо заедно с доставчика на публични комуникационни мрежи по отношение на сигурността на мрежата. Като се вземе предвид състоянието на науката и разходите за тяхното изпълнение, тези мерки трябва да осигуряват ниво на сигурност, съответстващо на риска, който е налице.

1а. Без да се засягат разпоредбите на Директива [95/46], мерките, посочени в параграф 1, най-малкото:

— гарантират, че достъп до личните данни може да има само упълномощен персонал за законно разрешени цели,

— защитават съхраняваните или предавани лични данни от инцидентно или незаконно унищожаване, инцидентна загуба или промяна и неразрешено или незаконно съхраняване, обработка, достъп или разкриване, както и

— гарантират осъществяването на политика на сигурност по отношение на обработката на лични данни.

[…]“.

8 Член 5 от Директива 2002/58 е озаглавен „Конфиденциалност на комуникациите“ и гласи:

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

[…]

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

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

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

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

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

[…]

5. Обработка на данни за трафик, в съответствие с параграфи 1, 2, 3 и 4, трябва да бъде ограничена до лица, действащи под ръководството на доставчиците на публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, които отговарят за изготвянето на сметки или управлението на трафика, за запитванията на клиенти,

за разкриването на измами, за търговията с електронни комуникационни услуги или за обезпечаването на услуга с добавена стойност и трябва да бъде ограничена до това, което е необходимо за целите на тези дейности“.

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

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

11 Член 15 от споменатата директива е озаглавен „Приложение на някои разпоредби от Директива [95/46]“ и 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 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 криминални нарушения 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 [запазването] на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф. Всички мерки, упоменати в настоящия параграф, трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф 1 и 2 от Договора за Европейския съюз.

[…]

1б. Доставчиците установяват вътрешни процедури за удовлетворяване на исканията за достъп до личните данни на ползвателите въз основа на националните разпоредби, приети съгласно параграф 1. При поискване от страна на компетентния национален орган те му предоставят информация относно посочените процедури, броя на получените искания, посочената правна обосновка и техния отговор.

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.

[…]“.

Директива 95/46

12 Член 22 от Директива 95/46, който се съдържа в глава III от същата, гласи:

„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 2006/24/ЕО

13 Член 1 от 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) е озаглавен „Предмет и обхват“ и в параграф 2 предвижда:

„Настоящата директива се прилага за данни за трафик и данни за местоположението, както за юридически, така и за физически лица, и на свързаните с тях данни, необходими за идентифицирането на абонат или регистриран ползвател. Тя не се прилага по отношение съдържанието на електронните съобщения, включително и по отношение на информацията, ползвана за справка посредством използване на електронна съобщителна мрежа“.

14 Член 3 от същата директива е озаглавен „Задължение за запазване на данни“ и предвижда:

„1. Чрез дерогация от разпоредбите на членове 5, 6 и 9 от Директива [2002/58] държавите членки приемат мерки, за да гарантират, че данните, посочени в член 5 от настоящата директива, са запазени в съответствие с нейните разпоредби до степента, до която тези данни са създадени или обработени от доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи, попадащи под тяхната юрисдикция в процеса на предоставяне на съответните съобщителни услуги.

2. Задължението за запазване на данни, предвидено в параграф 1, включва запазването на данните, посочени в член 5, свързани с неуспешни опити за повикване, когато тези данни са създадени или обработени и съхранени (по отношение на данните за телефония), или записани (по отношение на интернет данни) от доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи, попадащи под юрисдикцията на съответната държава членка, в процеса на предоставяне на съответните съобщителни услуги. Настоящата директива не изисква запазването на данни за повиквания, където не е била установена връзка“.

Шведското право

15 Видно от акта за преюдициално запитване по дело C-203/15, шведският законодател транспонира Директива 2006/24 в националното право, като изменя lagen (2003:389) om elektronisk kommunikation (Закон (2003:389) за електронните съобщения) и förordningen (2003:396) om elektronisk kommunikation (Наредба (2003:396) за електронните съобщения). И двата посочени акта в редакцията им, приложима към спора в главното производство, съдържат правни норми относно запазването на данни за електронните съобщения и относно достъпа на националните органи до тези данни.

16 Достъпът до споменатите данни е уреден и в lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Закон (2012:278) за предоставяне на данни за електронни съобщения в хода на разузнавателни действия на правоприлагащи органи, наричан по-нататък „Закон 2012:278“) и в rättegångsbalken (Съдопроизводствен кодекс, наричан по-нататък „RB“).

По задължението за запазване на данни за електронните съобщения

17 Според запитващата юрисдикция по дело C-203/15 разпоредбите на глава 6, член 16a от LEK във връзка с глава 2, член 1 от същия закон налагат задължение на доставчиците на електронни съобщителни услуги да запазват данните, предвидени в Директива 2006/24. Такива са данните за абонати и за всички електронни съобщения, необходими за откриване и идентифициране на източника и местоназначението на съобщението с цел определяне на датата, часа, продължителността и естеството му, както и установяване на използваното съобщително оборудване и локализиране на местонахождението на използваното в началото и в края на съобщението мобилно съобщително оборудване. Задължението за запазване на данни се прилага за данни, създадени или обработени при предоставянето на телефонни услуги, мобилна телефония, система за изпращане на електронни съобщения, достъп до интернет, както и при предоставянето на услуги за достъп до интернет (начин на свързване). Задължението се отнася и за данните за неуспешни повиквания. То обаче не касае съдържанието на съобщенията.

18 В членове 38—43 от Наредбата (2003:396) за електронните съобщения са посочени подлежащите на запазване категории данни. По отношение на телефонните услуги подлежат на запазване по-специално данните за телефонни повиквания и набрани номера, както и за проследими дати и часове за начало и край на съобщението. По отношение на мобилната телефония са наложени допълнителни задължения, като например за запазване на данните за местонахождението в началото и края на съобщението. По отношение на телефонните услуги, при които се използват IP пакети, трябва по-специално да се запазват, освен посочените по-горе данни, и тези за IP адресите на набиращия и на набрания. По отношение на системите за изпращане на електронни съобщения трябва по-специално да се запазват данните за номерата на изпращачите и получателите, IP адресите или всеки друг електронен адрес. По отношение на услугите за достъп до интернет трябва например да се запазват данните за IP адресите на ползвателите, както и проследимите дати и часове за начало и край на ползване на услугата за достъп до интернет.

По периода за запазване на данните

19 Съгласно глава 6, член 16d от LEK доставчиците на електронни съобщителни услуги трябва да запазват данните по член 16a от същата глава шест месеца, считано от деня на прекратяване на съобщението. След това те трябва да ги унищожат незабавно, освен ако в член 16d, втора алинея от същата глава не е предвидено друго.

По достъпа до запазените данни

20 Достъпът на националните органи до запазените данни се урежда от разпоредбите на Закон 2012:278, LEK и RB.

– Закон 2012:278

21 В рамките на разузнавателните действия националната полиция, Säkerhetspolisen (Полиция по сигурността, Швеция) и Tullverket (Митническа администрация, Швеция) могат — на основание на член 1 от Закон 2012:278 и при условията, предвидени от същия закон, без да уведомяват

доставчика на електронната съобщителна мрежа или на разрешената по LEK електронна съобщителна услуга, — да събират данни за изпратените по електронната съобщителна мрежа съобщения, за намиращото се в определена географска зона оборудване за електронни съобщения, както и за географската зона или географските зони, където се намира или се е намирало оборудването за електронни съобщения.

22 Съгласно членове 2 и 3 от Закон 2012:278 данните могат по принцип да се събират, ако с оглед на обстоятелствата мярката е особено необходима за предотвратяване, възпрепятстване или разкриване на престъпна дейност по осъществяване на едно или няколко престъпления, за които е предвидено наказание лишаване от свобода не по-малко от две години, или престъпления по член 3 от същия закон, за някои от които е предвидено наказание лишаване от свобода до две години. Причините, налагащи мярката, трябва да надделяват над съображенията за засягането или увреждането на адресата ѝ или за друг противоречащ на прилагането ѝ интерес. Съгласно член 5 от споменатия закон продължителността на мярката не трябва да надвишава един месец.

23 Решението за предприемане на такава мярка се взема от ръководителя на съответния орган или от служител, на когото той е делегирал правомощия за целта. То не подлежи на предварителен контрол от съдебен орган или от независим административен орган.

24 Член 6 от Закон 2012:278 предвижда, че за всяко решение за разрешаване на събирането на данни трябва да се уведоми Säkerhets- och integritetsskyddsnämnden (Комисията по сигурността и защитата на интегритета, Швеция). Съгласно член 1 от lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Закон (2007:980) за надзор върху някои дейности по правоприлагане) този орган трябва да упражнява надзор върху прилагането на закона от страна на правоприлагащите органи.

– LEK

25 По силата на глава 6, член 22, първа алинея, точка 2 от LEK всеки доставчик на електронни съобщителни услуги е длъжен при поискване да предаде данните за съответния абонат на прокуратурата, националната полиция, полицията по сигурността или друг правоприлагащ орган, ако въпросните данни са свързани с подозрение за извършено престъпление. Съгласно посоченото от запитващата юрисдикция по дело C-203/15 за целта не е необходимо да става въпрос за тежко престъпление.

– RB

26 RB регламентира съобщаването на запазените данни на националните органи в хода на предварителното разследване. Съгласно глава 27, член 19 от RB „поставянето под наблюдение на електронни съобщения“ без знанието на трети лица принципно се разрешава в хода на предварителни разследвания по-специално на престъпления, за които се предвижда наказание лишаване от свобода най-малко шест месеца. Глава 27, член 19 от RB предвижда, че „поставяне под наблюдение на електронни съобщения“ означава получаване без знанието на трети лица на данни за съобщения, изпратени чрез електронна съобщителна мрежа, за оборудване за електронни съобщения, което е налично или е било налично в определена географска зона, както и за географската зона или географските зони, където дадено електронно съобщително оборудване е или е било налично.

27 Запитващата юрисдикция по дело C-203/15 посочва, че глава 27, член 19 от RB не може да послужи като основание за получаване на сведения за съдържанието на съобщение. По принцип разпореждане за поставяне под наблюдение на електронни съобщения на основание глава 27, член 20 от RB е възможно само когато има достатъчно основания да се предполага, че дадено

лице е извършило престъпление, и когато мярката е изключително необходима за нуждите на разследването, като последното трябва да се отнася до престъпление, за което се предвижда наказание лишаване от свобода най-малко две години, или до опит, подготовка или съучастие в извършването на такова престъпление. Съгласно глава 27, член 21 от RB прокурорът трябва, освен при спешни случаи, да поиска от компетентния съдия разрешение за поставянето под наблюдение на електронни съобщения.

По сигурността и защитата на запазените данни

28 Съгласно глава 6, член 3a от LEK доставчиците на електронни съобщителни услуги, на които е възложено задължение за запазване на данни, трябва да предприемат подходящи технически и организационни мерки, за да гарантират защитата на данните в хода на тяхната обработка. Запитващата юрисдикция по дело C-203/15 обаче посочва, че шведското право не съдържа разпоредби относно мястото на запазване на данните.

Правото на Обединеното кралство

DRIPA

29 Член 1 от DRIPA е озаглавен „Правомощия за запазване на данни за релевантните съобщения при спазване на съответните гаранции“ и гласи:

„(1) [Министърът на вътрешните работи] може с акт („акт за разпореждане на запазване“) да наложи на обществен далекосъобщителен оператор да запазва релевантни данни за съобщения, ако прецени, че такова изискване е необходимо и пропорционално с оглед на една или няколко от целите по член 22, параграф 2, букви a)—h) от Regulation of Investigatory Powers Act 2000 [Закон от 2000 г. за уреждане на правомощията по разследване] (цели, които обосновават получаването на данни за съобщения).

(2) Актът за разпореждане на запазване може:

(a) да се отнася до конкретен оператор или до определена категория оператори;

(b) да налага запазване на всички данни или на определена категория данни;

(c) да определя период или периоди на запазване на данните;

(d) да налага други изисквания или ограничения във връзка със запазването на данните;

(e) да предвижда различни разпоредби за различни цели;

(f) да се отнася до данни, които съществуват или не към момента на издаване или влизане в сила на акта за разпореждане на запазването.

(3) [Министърът на вътрешните работи] може с наредба да приема допълнителни разпоредби относно запазването на релевантни данни за съобщенията.

(4) Тези разпоредби могат по-специално да уреждат:

(a) изискванията до приемането на акта за разпореждане на запазване;

(b) максималния период, за който трябва да се пазят данните съгласно акт за разпореждане на запазване;

(c) съдържанието, приемането, влизането в сила, обжалването, изменението или отмяната на акта за разпореждане на запазване;

(d) неприкосновеността, сигурността или защитата на запазените съгласно настоящия член данни, достъпа до тях, както и разкриването или унищожаването им;

(e) прилагането на релевантните изисквания или ограничения и проверяването дали тези изисквания или ограничения се спазват;

(f) кодекс за добри практики относно релевантните изисквания, ограничения или правомощия,

(g) възстановяването от [министъра на вътрешните работи] (при определени условия или безусловно) на разходите на обществените далекосъобщителни оператори за изпълнение на релевантните изисквания или ограничения;

(h) прекратяването на действието на [Data Retention (EC Directive) Regulations 2009 (Наредба от 2009 г. за запазването на данни по смисъла на Директивата на ЕО)] и преминаването към запазване на данни съгласно настоящия член.

(5) Максималният период по параграф 4, буква b) не трябва да надвишава 12 месеца, считано от датата, посочена за съответните данни в наредбите по параграф 3.

[…]“.

30 Член 2 от DRIPA определя понятието „релевантни данни за съобщенията“ като „релевантни данни за съобщения от вида, посочен в приложението към Наредбата от 2009 г. за запазването на данни по смисъла на Директивата ЕО, доколкото тези данни са създадени или обработени в Обединеното кралство от обществени далекосъобщителни оператори в хода на доставката на съответните далекосъобщителни услуги“.

RIPA

31 Член 21 от Закона от 2000 г. за уреждане на правомощията по разследване (наричан по-нататък „RIPA“) се съдържа в глава II от същия закон, озаглавен е „Получаване и разкриване на данни за съобщения“ и в параграф 4 уточнява:

„За целите на тази глава „данни за съобщения“ са:

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

(b) всяка информация, която не включва никаква част от съдържанието на съобщението (освен информацията по буква а) и показва как дадено лице използва:
(i) пощенска или далекосъобщителна услуга или
(ii) част от далекосъобщителна система във връзка с доставката или използването от всяко лице на всякаква далекосъобщителна услуга;

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

32 Съгласно посоченото в акта за преюдициално запитване по дело C-698/15 тези данни включват „данните за местонахождението на ползвателя“, но не и такива за съдържанието на съобщението.

33 По отношение на достъпа до запазените данни член 22 от RIPA предвижда:

„(1) Този член се прилага в случаите, когато отговорно лице по настоящата глава счита за необходимо да получи данни за съобщения по съображения, посочени в параграф 2 от настоящия член.

(2) Получаването на данни за съобщения е необходимо, когато се налага по следните съображения:

(a) в интерес на националната сигурност;

(b) за предотвратяване или разкриване на престъпления или предотвратяване на нарушения на обществения ред;

(c) в интерес е на икономическото благосъстояние на Обединеното кралство;

(d) в интерес е на обществената безопасност;

(e) за защита на общественото здраве;

(f) за определяне на данъчната основа или за събиране на данъци, мита, такси или други дължими на публичната администрация налози, вноски или суми;

(g) за предотвратяване в спешни случаи на смърт, нараняване или друго увреждане на физическото или психическото здраве на лице или за ограничаване на нараняване или увреждане на физическото или психическото здраве на лице;

(h) за други цели (извън посочените в букви a)—g), посочени в заповед на [министъра на вътрешните работи].

(4) При условията на параграф 5 съответното отговорно лице може, ако счита, че даден далекосъобщителен или пощенски оператор разполага, би могъл да разполага или би могъл да направи така, че да разполага с определени данни, да предяви искане пред този далекосъобщителен или пощенски оператор:

(a) да получи данните, ако вече не разполага с тях, и

(b) да му разкрие всички данни, с които разполага или които е получил впоследствие.

(5) Съответното отговорно лице дава разрешение по параграф 3 или предявява искане по параграф 4 само ако счита, че получаването на въпросните данни — в резултат на разрешени действия или на изискване в разрешение или искане — е пропорционално на преследваната с получаването на данните цел“.

34 Член 65 от RIPA предвижда възможност за подаване на жалба пред Investigatory Powers Tribunal (Специализиран съд по въпросите на разузнавателните средства, Обединено кралство), ако има основание да се счита, че данните са получени по ненадлежен начин.

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (Наредба от 2014 г. за запазване на данни) е приета на основание на DRIPA и е разделена на три части, втората от които включва членове 2—14. Член 4 е озаглавен „Искания за запазване“ и предвижда:

„(1) искането за запазване трябва да посочва:

(a) обществения далекосъобщителен оператор (или съответните му характеристики), пред когото се предявява,

(b) подлежащите на запазване данни за релевантни съобщения,

(c) периода или периодите, за който или които данните трябва да се запазят;

(d) други изисквания или ограничения във връзка със запазването на данните;

(2) Искането за запазване не може да налага запазване на данни за повече от 12 месеца, считано:

(a) по отношение на данните за трафик или за използване на услуга — от деня на съответното съобщение, и

(b) по отношение на данните за абонатите — от деня, когато съответното лице прекратява разглежданата съобщителна услуга, или от датата на промяна на данните (ако тя е по-ранна).

[…]“.

36 Член 7 от споменатата наредба е озаглавен „Неприкосновеност и сигурност на данните“ и гласи:

„(1) Обществен далекосъобщителен оператор, който запазва данни на основание на член 1 от [DRIPA], трябва:

(a) да гарантира същата неприкосновеност и поне същото равнище на сигурност и защита на данните като тези на системите, от които те са извлечени,

(b) да гарантира с подходящи технически и организационни мерки достъп до данните само на тези лица от персонала, които са получили специално разрешение за това, и

(c) да осигури с подходящи технически и организационни мерки защита на данните срещу неправомерно унищожаване, загуба или случайно повреждане, както и срещу неправомерно или неразрешено запазване, обработване, достъп или разкриване.

(2) Обществен далекосъобщителен оператор, който запазва данни на основание на член 1 от [DRIPA], трябва да ги унищожи, когато разрешението за запазването им по този член или по друга разпоредба от закона отпадне.

(3) Изискването по параграф 2 за унищожаване на данните налага те да бъдат трайно заличени по начин, който прави достъпа до тях невъзможен.

(4) Достатъчно е операторът да предприема мерки за заличаване на данните ежемесечно или на по-кратки интервали според възможностите, с които практически разполага“.

37 Член 8 от споменатата наредба е озаглавен „Разкриване на запазените данни“ и гласи:

„(1) Общественият далекосъобщителен оператор трябва да установи подходящи системи за сигурност (включващи технически и организационни мерки) при определяне на достъпа до данните за съобщения, които са запазени по силата на член 1 от [DRIPA], с оглед предотвратяване на всяко разкриване извън случаите по член 1, параграф 6, буква а) от [DRIPA].

(2) Обществен далекосъобщителен оператор, който запазва данни на основание член 1 от [DRIPA], трябва да го прави по начин, позволяващ му без неоправдано закъснение да ги предоставя при предявени за това искания“.

38 Член 9 от същата наредба е озаглавен „Контрол от комисаря по информацията“ и гласи:

„Комисарят по информацията контролира спазването на изискванията или ограниченията, предвидени в тази част във връзка с неприкосновеността, сигурността и унищожаването на данните, запазени по силата на член 1 от [DRIPA]“.

Кодексът за добри практики

39 Acquisition and Disclosure of Communications Data Code of Practice (Кодекс за добри практики относно получаването и разкриването на данни за съобщения, наричан по-нататък „Кодексът за добри практики“) съдържа в параграфи 2.5—2.9 и 2.36—2.45 насоки във връзка с необходимостта и пропорционалността при получаване на данни за съобщения. Запитващата юрисдикция по дело C-698/15 пояснява, че параграфи 3.72—3.77 от посочения кодекс налагат да се обърне особено внимание на необходимостта и пропорционалността в случаите, когато поисканите данни за съобщения се отнасят до лице, чиято професия го задължава да спазва професионална тайна или друго изискване за поверителност.

40 Съгласно параграфи 3.78—3.84 от споменатия кодекс, за да се предяви искане на данни за съобщения с цел разкриване на журналистически източник, се изисква постановено за тази цел съдебно решение. Съгласно параграфи 3.85—3.87 от същия кодекс, за да се поиска достъп от органи на местната власт, се изисква съответно одобрение от съда. Не се изисква обаче каквото и да било разрешение от съдебен или друг независим орган, за да се предяви искане на достъп до данни за съобщения, защитени с адвокатската тайна, лекарска тайна или тайна поради качество на лицето на член на парламента или свещенослужител.

41 Параграф 7.1 от Кодекса за добри практики предвижда, че данните за съобщения, събрани или получени по силата на разпоредбите на RIPA, както и всички откъси, резюмета и копия на такива данни трябва да се обработват и съхраняват по сигурен начин. Освен това трябва да се спазват и изискванията на Data Protection Act (Закон за защита на данните).

42 Параграф 7.18 от Кодекса за добри практики предвижда, че при преценката дали данни за съобщения могат да се разкрият на чуждестранни органи, съответният публичен орган на Обединеното кралство трябва да установи по-специално дали тези данни ще бъдат надлежно защитени. Видно обаче от параграф 7.22 от посочения кодекс, когато причини от важен обществен интерес го налагат, предаването на данни към трети страни е възможно дори и когато съответната трета страна не гарантира подходящо равнище на тяхната защита. Във връзка с това запитващата юрисдикция по дело C-698/15 отбелязва, че министърът на

вътрешните работи може да издаде удостоверение относно националната сигурност, с което да изключи необходимостта от спазване на определени законови разпоредби по отношение на някои данни.

43 В параграф 8.1 от споменатия кодекс се напомня, че с RIPA се създава институтът на Interception of Communications Commissioner (Комисар по засичане на съобщения, Обединено кралство), чиято роля по-специално е да контролира независимото упражняване и прилагане на правомощията и задълженията по част I, глава II от RIPA. Видно от параграф 8.3 от същия кодекс, този комисар има право, когато „установи, че дадено физическо лице е пострадало вследствие от нарушение, извършено умишлено или поради небрежност“, да уведоми това лице, че съществуват подозрения за неправомерно използване на компетентност.

Споровете в главните производства и преюдициалните въпроси

Дело C-203/15

44 На 9 април 2014 г. Tele2 Sverige, доставчик на електронни съобщителни услуги, установен в Швеция, съобщава на PTS, че предвид 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), с което Директива 2006/24 се обявява за невалидна, ще преустанови, считано от 14 април 2014 г., запазването на данни за електронните съобщения, посочени в LEK, и ще унищожи запазените до тази дата данни.

45 На 15 април 2014 г. Rikspolisstyrelsen (Генерална дирекция на националната полиция, Швеция) подава жалба пред PTS, че Tele2 Sverige е преустановило съобщаването на разглежданите данни.

46 На 29 април 2014 г. justitieminister (министър на правосъдието, Швеция) определя специален докладчик, на когото възлага да анализира съответната шведска правна уредба от гледна точка на решение Digital Rights. В доклад от 13 юни 2014 г., озаглавен „Datalagring, EU-rätten och svensk rätt, nº Ds 2014:23“ („Запазване на данни — правото на Съюза и шведското право“, наричан по-нататък „докладът от 2014 г.“), специалният докладчик стига до извода, че националната правна уредба относно запазването на данни, която се съдържа в членове 16a—16f от LEK, не противоречи нито на правото на Съюза, нито на Европейската конвенция за защита на правата на човека и основните свободи, подписана в Рим на 4 ноември 1950 г. (наричана по-нататък „ЕКПЧ“). Специалният докладчик отбелязва, че решение Digital Rights не би трябвало да се тълкува в смисъл, че отхвърля самия принцип на общо и неизбирателно запазване на данни. То според него не трябва да се разбира и в смисъл, че с него Съдът установява набор от критерии, които трябва да са изпълнени, за да може дадена правна уредба да се счита за пропорционална. За да се прецени дали шведската правна уредба е в съответствие с правото на Съюза, трябвало да се вземат предвид всички обстоятелства, като например обхватът на запазването на данни с оглед на разпоредбите за достъпа до данни, периода на запазване, защитата и сигурността им.

47 Въз основа на това на 19 юни 2014 г. PTS уведомява Tele2 Sverige, че като не запазва посочените в LEK данни за целите на борбата с престъпността от шест месеца, не изпълнява наложените му съгласно националната правна уредба задължения. След това със заповед от 27 юни 2014 г. PTS му разпорежда най-късно до 25 юли 2014 г. да започне да запазва данните.

48 Тъй като счита, че докладът от 2014 г. се основава на неправилно тълкуване на решение Digital Rights и че задължението за запазване на данни противоречи на гарантирани от Хартата основни права, Tele2 Sverige обжалва заповедта от 27 юни 2014 г. пред Förvaltningsrätten i Stockholm (Административен съд Стокхолм, Швеция). Последният отхвърля жалбата с решение от 13 октомври 2014 г., което Tele2 Sverige обжалва пред запитващата юрисдикция.

49 Според запитващата юрисдикция съвместимостта на шведската правна уредба с правото на Съюза трябва да се прецени с оглед на член 15, параграф 1 от Директива 2002/58. Всъщност, макар да налага принципа, че данните за трафик и данните за местонахождение трябва да се изтриват или да се правят анонимни, когато вече не са необходими за целите на предаване на съобщения, споменатата директива допуска с член 15, параграф 1 дерогиране на този принцип, като разрешава на държавите членки, когато поради някой от посочените в същия член мотиви се налага, да ограничават задължението за изтриване или за анонимизиране или също да предвиждат запазване на данни. В този смисъл според запитващата юрисдикция правото на Съюза в някои случаи допуска запазване на данни за електронни съобщения.

50 При все това запитващата юрисдикция иска да се установи дали, като се има предвид решение Digital Rights, задължение за общо и неизбирателно запазване на данни за електронни съобщения като разглежданото в главното производство е съвместимо с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7 и 8 и член 52, параграф 1 от Хартата. Предвид различните становища на страните в това отношение Съдът би следвало еднозначно да се произнесе по въпроса дали, както счита Tele2 Sverige, общото и неизбирателното запазване на данни за електронни съобщения само по себе си е несъвместимо с членове 7 и 8 и член 52, параграф 1 от Хартата, или, както следва от доклада от 2014 г., съвместимостта на такова запазване на данни трябва да се прецени с оглед на разпоредбите за достъпа до данните, както и за тяхната защита, сигурност и период на запазване.

51 При тези условия запитващата юрисдикция решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) Съвместимо ли е общо задължение за запазване на данни — което се отнася до всички лица, всички електронни съобщителни средства и всички данни за трафик без никакво разграничаване, ограничаване или изключение за целите на борбата с престъпността […] — с член 15, параграф 1 от Директива 2002/58 с оглед на членове 7 и 8 и член 52, параграф 1 от Хартата?

2) При отрицателен отговор на първия въпрос, може ли все пак такова задължение за запазване да бъде разрешено, при условие че:
   а) достъпът на националните органи до запазените данни е установен съгласно уточнения в точки 19—36 [от акта за преюдициално запитване] начин и
   б) изискванията за защита и сигурност на данните са уредени съгласно уточнения в точки 38—43 [от акта за преюдициално запитване] начин, и
   в) всички релевантни данни се запазват за срок от шест месеца, считано от датата на прекратяване на съобщението, и впоследствие се изтриват съгласно изложеното в точка 37 [от акта за преюдициално запитване]?“.

Дело C-698/15

52 Г-н Watson, г-н Brice и г-н Lewis са подали поотделно жалби пред High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Върховен съд (Англия и Уелс), общо гражданско отделение (административен състав), за контрол за законосъобразност на член 1 от DRIPA, твърдейки по-специално, че посоченият член е несъвместим с членове 7 и 8 от Хартата и член 8 от ЕКПЧ.

53 В решение от 17 юли 2015 г. High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) (Върховен съд (Англия и Уелс), общо гражданско отделение (административен състав) приема, че решение Digital Rights установява „императивни изисквания на правото на Съюза“ за правните уредби на държавите членки в областта на запазването на данни за съобщения и на достъпа до тях. Тази юрисдикция счита, че след като в споменатото решение Съдът приема Директива 2006/24 за несъвместима с принципа на пропорционалност, то национална правна уредба с идентично на нейното съдържание също не би могла да е съвместима с него. От логиката, на която било основано решение Digital Rights, следвало, че законодателство, което установява общ режим за запазване на данни за съобщения, нарушава гарантираните с членове 7 и 8 от Хартата права, освен ако не предвижда също и предоставящ достатъчно гаранции за запазване на тези права режим за достъп до данните. В този смисъл член 1 от DRIPA бил несъвместим с членове 7 и 8 от Хартата, тъй като не установявал ясни и точни правила за достъп и използване на запазените данни и не налагал изискване достъпът до тях да подлежи на предварителен контрол от страна на юрисдикция или на независима административна структура.

54 Министърът на вътрешните работи обжалва решението пред Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение), Обединено кралство).

55 Последната юрисдикция отбелязва, че член 1, параграф 1 от DRIPA оправомощава министъра на вътрешните работи да приема, без каквото и да било предварително разрешение от юрисдикция или от независима административна структура, общ режим за налагане на задължение на обществените далекосъобщителни оператори за запазване на всички данни за всякакви пощенски или далекосъобщителни услуги за максимален период от дванадесет месеца, ако счита, че такова изискване е необходимо и пропорционално за постигане на целите, посочени в правната уредба на Обединеното кралство. Независимо че не включвали съдържанието на съобщението, тези данни можели да доведат до значителна намеса в личния живот на ползвателите на съобщителни услуги.

56 В акта за преюдициално запитване и в постановеното в хода на производството по обжалване решение от 20 ноември 2015 г., с което решава да отправи до Съда настоящото преюдициално запитване, запитващата юрисдикция приема, че националните правни норми относно запазването на данни логично попадат в приложното поле на член 15, параграф 1 от Директива 2002/58, поради което следователно трябва да отговарят на произтичащите от Хартата изисквания. Съгласно обаче член 1, параграф 3 от същата директива законодателят на Съюза не бил хармонизирал правилата относно достъпа до запазени данни.

57 По отношение на отражението, което решение Digital Rights има върху разрешаването на повдигнатите в спора в главното производство въпроси, запитващата юрисдикция отбелязва, че по споменатото дело Съдът бил сезиран с искане за установяване на валидността на Директива 2006/24, а не на национална правна уредба. Предвид по-специално тясната връзка между запазването на данни и достъпа до тях се налагало посочената директива задължително да включва и съответни гаранции, като, за да установи законосъобразността на предвидения в нея режим за запазване на данни, решение Digital Rights трябвало да анализира правилата за достъп до данните. Ето защо с това си решение Съдът не целял да приеме императивни изисквания за национални законодателства в областта на достъпа до данни, с които не се прилагало правото на Съюза. Освен това съображенията на Съда били тясно свързани с преследваните със същата директива цели. Докато преценката на национална правна уредба трябвало да направи с оглед на преследваните от нея цели и нейния контекст.

58 Във връзка с необходимостта от отправяне на преюдициално запитване до Съда запитващата юрисдикция отбелязва факта, че към момента на приемане на акта за преюдициално запитване шест юрисдикции на други държави членки, пет от които действащи като последна инстанция,

били отменили национални законодателства на основание решение Digital Rights. Отговорът на поставените въпроси следователно не бил очевиден, а бил необходим за разрешаване на споровете, с които тази юрисдикция била сезирана.

59 При тези условия Court of Appeal (England & Wales) (Civil Division) (Апелативен съд на Англия и Уелс (гражданско отделение) решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) Установява ли решение Digital Rights (и конкретно точки 60—62) императивни изисквания на правото на Съюза, приложими по отношение на националния режим на държава членка относно достъпа до запазени в съответствие с националното законодателство данни, за да бъде този режим в съответствие с членове 7 и 8 от Хартата?

2) Разширява ли решение Digital Rights обхвата на членове 7 и/или 8 от Хартата отвъд границите на приложение на член 8 от ЕКПЧ, определени в практиката на Европейския съд по правата на човека?“.

Производството пред Съда

60 С определение от 1 февруари 2016 г., Davis и др. (C-698/15, непубликувано, EU:C:2016:70) председателят на Съда решава да уважи искането на Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение) за разглеждане на дело C-698/15 по реда на бързото производство, предвиден в член 105, параграф 1 от Процедурния правилник на Съда.

61 С решение на председателя на Съда от 10 март 2016 г. дела C-203/15 и C-698/15 са съединени за целите на устната фаза на производството и на решението.

По преюдициалните въпроси

По първия въпрос по дело C-203/15

62 С първия си въпрос по дело C-203/15 Kammarrätten i Stockholm (Апелативен административен съд Стокхолм) иска по същество да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 7 и 8 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба като тази, предмет на главното производство, предвиждаща за целите на борбата с престъпността общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства.

63 Въпросът възниква по-специално поради факта, че Директива 2006/24 — която разглежданата в главното производство национална правна уредба има за цел да транспонира — е обявена за невалидна с решение Digital Rights, но страните имат различни становища за обхвата на това решение и за отражението му върху посочената правна уредба, която регламентира запазването на данни за трафик и на данни за местонахождение и достъпа на националните органи до тези данни.

64 Най-напред следва да се установи дали национална правна уредба като разглежданата в главното производство попада в приложното поле на правото на Съюза.

По приложното поле на Директива 2002/58

65 Държавите членки, които са представили писмени становища пред Съда, изразяват различни становища по въпроса дали и в каква степен национални правни уредби, които регламентират запазването на данни за трафик и на данни за местонахождение и достъпа на националните органи до тези данни за целите на борбата с престъпността, попадат в приложното поле на Директива 2002/58. Всъщност, докато белгийското, датското, германското, естонското правителство, Ирландия и нидерландското правителство считат, че на такъв въпрос би следвало да се отговори положително, то чешкото правителство предлага да му се отговори отрицателно, като отбелязва, че единствената цел на споменатите правни уредби е борбата с престъпността. Правителството на Обединеното кралство пък счита, че в приложното поле на посочената директива попадат само правните уредби, които регламентират запазването на данни, но не и тези, които регламентират достъпа на националните правоприлагащи органи до тези данни.

66 Що се отнася накрая до Комисията, в писменото си становище, което представя на Съда по дело C-203/15, тя поддържа, че разглежданата в главното производство национална правна уредба попада в приложното поле на Директива 2002/58, а в писменото си становище по дело C-698/15 посочва, че в посоченото ѝ приложно поле попадат само националните правни норми относно запазването на данни, но не и тези относно достъпа на националните органи до тези данни. Според нея обаче последните норми би трябвало да се вземат предвид при преценката дали дадена национална правна уредба, която регламентира запазването на данни от доставчици на електронни съобщителни услуги, представлява пропорционална намеса в гарантираните с членове 7 и 8 от Хартата основни права.

67 В това отношение следва да се отбележи, че обхватът на приложното поле на Директива 2002/58 трябва да се прецени, като се вземе предвид по-специално нейната структура.

68 Съгласно член 1, параграф 1 от Директива 2002/58 същата предвижда по-специално хармонизиране на националните разпоредби, необходими за осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по отношение на обработката на лични данни в сектора на електронните съобщения.

69 Член 1, параграф 3 от същата директива изключва от приложното ѝ поле „дейностите на държавата“ в определени области, а именно в тези на наказателното право, обществената сигурност, отбраната, сигурността на държавата, включително икономическото благосъстояние на държавата, когато дейностите се отнасят до проблемите за сигурността на държавата (вж. по аналогия, що се отнася до член 3, параграф 2, първо тире от Директива 95/46, решения от 6 ноември 2003 г., Lindqvist, C-101/01, EU:C:2003:596, т. 43 и от 16 декември 2008 г., Satakunnan Markkinapörssi и Satamedia, C-73/07, EU:C:2008:727, т. 41).

70 Член 3 от Директива 2002/58 предвижда, че същата се прилага при обработката на лични данни във връзка с предоставянето на публично достъпни електронни съобщителни услуги в публични комуникационни 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.

71 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

[този] директива“. Като пример за мерки, които държавите членки могат да приемат, член 15, параграф 1, второ изречение от споменатата директива посочва мерките, „предвиждащи [запазването] на данни“.

72 Вярно е наистина, че законодателните мерки по член 15, параграф 1 от Директива 2002/58 се отнасят до дейности, които са присъщи на държавите или на държавните органи и са чужди на областите на дейност на частноправните субекти (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 51). Освен това целите, които трябва да се преследват с такива мерки съгласно посочената разпоредба, а именно гарантиране на националната сигурност, отбраната, обществената безопасност, както и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна съобщителна система, по същество съвпадат с целите, които се преследват с дейностите по член 1, параграф 3 от тази директива.

73 Като се има предвид обаче общата структура на Директива 2002/58, изложените в предходната точка от настоящото решение съображения не позволяват да се направи изводът, че законодателните мерки по член 15, параграф 1 от Директива 2002/58 са изключени от приложното ѝ поле, тъй като в противен случай посочената разпоредба би била лишена от смисъл. Всъщност споменатата разпоредба логично предполага, че посочените в нея национални мерки, като например тези, свързани със запазването на данни за целите на борбата с престъпността, попадат в приложното поле на същата директива, тъй като тя изрично допуска държавите членки да ги приемат само при спазване на предвидените в нея условия.

74 Освен това законодателните мерки по член 15, параграф 1 от Директива 2002/58 регламентират — за посочените в същата разпоредба цели — дейността на доставчиците на електронни съобщителни услуги. Следователно член 15, параграф 1 във връзка с член 3 от споменатата директива трябва да се тълкува в смисъл, че такива законодателни мерки попадат в приложното поле на същата директива.

75 В приложното ѝ поле по-специално попада законодателна мярка като разглежданата в главното производство, с която на посочените доставчици се налага задължение за запазване на данни за трафик и на данни за местонахождение, тъй като една такава дейност логично предполага обработване на лични данни.

76 В приложното ѝ поле попада и законодателна мярка, която също като тази в главното производство се отнася до достъпа на националните органи до запазените от доставчиците на електронни съобщителни услуги данни.

77 Всъщност гарантираната с член 5, параграф 1 от Директива 2002/58 защита на поверителността на електронните съобщения и на свързаните с тях данни за трафик се отнася за мерки, приети от всяко различно от ползвателите лица, независимо дали става въпрос за частноправни субекти, или образувания, или пък за държавни структури. Както се потвърждава в съображение 21 от посочената директива, същата има за цел да се предотврати „неоторизираният достъп“ до съобщения, включително и до „всякакви данни, свързани с такива съобщения“, за да се защити поверителността на електронните съобщения.

78 При тези обстоятелства законодателна мярка — с която на основание член 15, параграф 1 от Директива 2002/58 държава членка налага на доставчиците на електронни съобщителни услуги да предоставят за посочените от същата разпоредба цели и при предвидените с такава мярка условия достъп на националните органи до запазените от доставчиците данни — се отнася до обработката на лични данни от последните и попада в приложното поле на тази директива.

79 Освен това, след като налага запазване на данни единствено за целите на предоставянето при необходимост на достъп до тях на компетентните национални органи, национална правна уредба относно запазване на данни по принцип логично съдържа разпоредби, свързани с достъпа на компетентните национални органи до запазените от доставчиците на електронни съобщителни услуги данни.

80 Това тълкуване се потвърждава от член 15, параграф 1 от Директива 2002/58, съгласно който доставчиците установяват вътрешни процедури за удовлетворяване на исканията за достъп до личните данни на ползвателите въз основа на националните разпоредби, приети съгласно член 15, параграф 1 от същата директива.

81 От изложеното следва, че национална правна уредба като разглежданата в главното производство по дела C-203/15 и C-698/15 попада в приложното поле на Директива 2002/58.

По тълкуването на член 15, параграф 1 от Директива 2002/58 с оглед на членове 7, 8 и 11 и член 52, параграф 1 от Хартата

82 Следва да се отбележи, че съгласно член 1, параграф 2 от Директива 2002/58 разпоредбите на същата „конкретизират и допълват“ Директива 95/46. Както се посочва в съображение 2 от Директива 2002/58, същата се стреми по-специално 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]

83 За тази цел Директива 2002/58 съдържа специални разпоредби, които, както се посочва в съображения 6 и 7 от същата, целят да защитят ползвателите на електронни съобщителни услуги срещу рисковете за техните лични данни и за неприкосновеността на личния им живот в резултат на новите технологии и увеличаващата се способност за автоматизирано съхранение и обработка на данни.

84 Член 5, параграф 1 от споменатата директива по-специално предвижда, че в националното си законодателство държавите членки трябва да гарантират поверителността на съобщенията, направени чрез публични комуникационни мрежи и публично достъпни електронни съобщителни услуги, и на свързаните с тях данни за трафик.

85 Видно от член 5, параграф 1, второ изречение от Директива 2002/58, установеният от същата директива принцип на поверителност на съобщенията означава, че по правило е забранено лица, различни от потребителите, да съхраняват без съгласието на последните свързани с електронните им съобщения данни за трафика. Единственото изключение е предвидено за лицата, законно упълномощени в съответствие с член 15, параграф 1 от тази директива, и за техническото съхранение, което е необходимо за пренасяне на съобщение (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 47).

86 В този смисъл и както се потвърждава от съображения 22 и 26 от Директива 2002/58, член 6 от същата директива предвижда, че обработването и съхраняването на данни за трафик се разрешава само ако и докато те са необходими за целите на фактурирането на услугите, пускането им на пазара, доставката им или облагането им с данък върху добавената стойност (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 47 и 48).

По отношение в частност на фактурирането на услугите такова обработване е допустимо само до края на периода, през който фактурата може законно да се оспори или да се претендира плащане по съответния ред. 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.

87 Обхватът на разпоредбите на членове 5 и 6 и на член 9, параграф 1 от Директива 2002/58, с които се цели да се гарантира поверителността на съобщенията и на свързаните с тях данни, както и да се намалят до минимум рисковете от злоупотреби, трябва също да се прецени от гледна точка на съображение 30 от тази директива, съгласно което „[с]истемите за обезпечаване на електронни комуникационни мрежи и услуги трябва да бъдат направени, така че да ограничават количеството на необходимите лични данни до точен минимум“.

88 Вярно е наистина, че член 15, параграф 1 от Директива 2002/58 допуска държавите членки да въвеждат изключения от принципното задължение по член 5, параграф 1 от същата директива за гарантиране на поверителността на личните данни, както и на съответните задължения, посочени по-специално в членове 6 и 9 от споменатата директива (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 50).

89 Тъй като обаче допуска държавите членки да ограничат обхвата на принципното задължение за гарантиране на поверителността на съобщенията и на свързаните с тях данни за трафика, член 15, параграф 1 от Директива 2002/58 следва съгласно практиката на Съда да се тълкува стриктно (вж. по аналогия решение от 22 ноември 2012 г., Probst, C-119/12, EU:C:2012:748, т. 23). Една такава разпоредба не би могла следователно да послужи като основание дерогирането по принцип на това задължение, и в частност на забраната за съхраняване на данни по член 5 от тази директива, да се превърне в правило, без при това да изпразни до голяма степен от смисъл последната разпоредба.

90 В това отношение следва да се отбележи, че съгласно член 15, параграф 1, първо изречение от Директива 2002/58 законодателните мерки, които същият посочва и които дерогират принципа на поверителност на съобщенията и на свързаните с тях данни за трафик, трябва да имат за цел да се „гарантира национална сигурност (т.е държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна комуникационна система“ или трябва да преследват други цели по член 13, параграф 1 от Директива 95/46, към който член 15, параграф 1, първо изречение от Директива 2002/58 препраща (вж. в този смисъл решение от 29 януари 2008 г., Promusicae, C-275/06, EU:C:2008:54, т. 53). Изброяването на целите е изчерпателно, след като в член 15, параграф 1, второ изречение от тази директива се посочва, че законодателните мерки трябва да бъдат оправдани на „основанията, изложени“ в член 15, параграф 1, първо изречение от споменатата директива. Ето защо държавите членки не могат да приемат такива мерки с цели, различни от изброените в последната разпоредба.

91 Освен това член 15, параграф 1, трето изречение от Директива 2002/58 предвижда, че „[в]сички мерки, упоменати в [член 15, параграф 1 от същата директива], трябва да бъдат в съответствие с общите принципи на законодателството [на Съюза], включително онези, упоменати в член 6, параграф[и] 1 и 2 от [ДЕС]“, сред които са гарантираните вече с Хартата общи принципи и основни права. Предвид това споменатият член 15, параграф 1 от Директива 2002/58 трябва да се тълкува с оглед на основните права, гарантирани с Хартата (вж. по аналогия, що се отнася до Директива 95/46, решения от 20 май 2003 г., Österreichischer Rundfunk и др., C-465/00, C-138/01 и C-139/01, EU:C:2003:294, т. 68, от 13 май 2014 г., Google Spain и Google, C-131/12, EU:C:2014:317, т. 68 и от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 38).

92 В това отношение следва да се подчертае, че задължението, наложено на доставчиците на електронни съобщителни услуги с национална правна уредба като разглежданата в главното производство, 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, свързани не само с изрично посочените в преюдициалните въпроси членове 7 и 8 от Хартата, но и със зачитането на свободата на изразяване на мнение, гарантирана от член 11 от Хартата (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 25 и 70).

93 С оглед на това 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 (в този смисъл вж. решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 39 и цитираната съдебна практика). Същото се отнася и за свободата на изразяване на мнение, като се има предвид особено голямото ѝ значение във всяко демократично общество. Това основно право, гарантирано с член 11 от Хартата, 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 12 юни 2003 г., Schmidberger, C-112/00, EU:C:2003:333, т. 79 и от 6 септември 2011 г., Patriciello, C-163/10, EU:C:2011:543, т. 31).

94 В това отношение следва да се напомни, че съгласно член 52, параграф 1 от Хартата всяко ограничаване на упражняването на правата и свободите, признати от Хартата, трябва да бъде предвидено в закон и да зачита основното им съдържание. При спазване на принципа на пропорционалност ограничения за упражняването на тези права и свободи могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора (решение от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 50).

95 Във връзка с последното член 15, параграф 1, първо изречение от Директива 2002/58 предвижда, че държавите членки могат да приемат мерки, с които да дерогират принципа на поверителност на съобщенията и на свързаните с тях данни за трафик, когато това представлява „необходима, подходяща и пропорционална мярка в рамките на демократично общество“ с оглед на посочените в същата разпоредба цели. В съображение 11 от тази директива пък се уточнява, че такива мерки трябва да бъдат „строго“ пропорционални на предвидената цел. Що се отнася в частност до запазването на данни, член 15, параграф 1, второ изречение от споменатата директива налага то да е „за ограничен период“ и да е „оправдан[о]“ с оглед на някоя от целите по член 15, параграф 1, първо изречение от същата директива.

96 Спазването на принципа на пропорционалност се налага също и от установената практика на Съда, съгласно която защитата на основното право на зачитане на личния живот на равнище на Съюза изисква дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото (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. 77, Digital Rights, т. 52 и от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 92).

97 По въпроса дали национална правна уредба като разглежданата по дело C-203/15 отговаря на посочените условия, следва да се отбележи, че тя предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства и че задължава доставчиците на електронни съобщителни услуги систематично и непрекъснато да запазват тези данни без каквото и да било изключение. Видно от акта за преюдициално запитване, визираните с посочената правна уредба категории данни по същество са същите като тези, за които Директива 2006/24 предвижда запазване.

98 Данните, които доставчиците на електронни съобщителни услуги трябва да запазват, позволяват да се проследи и идентифицира източникът на съобщението и неговото местоназначение, да се определи датата, времето, продължителността и видът на съобщението, съобщителното оборудване на ползвателите, както и да се локализира мобилното съобщително оборудване. Сред тези данни по-специално са и името и адресът на абоната или на регистрирания ползвател, телефонният номер на викащата страна и номерът на виканата страна, както и IP адрес за интернет услугите. Тези данни по-специално дават възможност да се установи лицето, с което даден абонат или регистриран ползвател се е свързал и по какъв начин, като същевременно се определят времето на съобщението и мястото, от което то е направено. Освен това те дават възможност да се разбере честотата на съобщенията на абоната или на регистрирания ползвател с определени лица през определен период (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 26).

99 Разгледани заедно, от тези данни 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 (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 27). Както се отбелязва в точки 253, 254 и 257—259 от заключението на генералния адвокат, посочените данни предоставят по-специално 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.

100 Произтичащата от такава правна уредба намеса в основните права, провъзгласени в членове 7 и 8 от Хартата, се оказва силно изразена и трябва да се счита за особено тежка. Обстоятелството, че запазването на данните се осъществява, без ползвателите на електронни съобщителни услуги да са информирани за това, може да породи усещане в съзнанието на съответните лица, че личният им живот е обект на постоянно наблюдение (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 37).

101 Макар такава правна уредба да не допуска запазване на данни за съдържанието на съобщенията и следователно да не може да засегне същественото съдържание на споменатите права (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 39), запазването на данни за трафик и на данни за местонахождение все пак би могло да даде отражение върху използването на електронните съобщителни средства и следователно върху упражняваната от тях свобода на изразяване на мнение, гарантирана от член 11 от Хартата (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 28).

102 Предвид тежестта на намесата в разглежданите основни права, каквато представлява национална правна уредба, предвиждаща за целите на борбата с престъпността запазване на данни за трафик и на данни за местонахождение, само борбата с тежките престъпления може да обоснове такава мярка (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 60).

103 Освен това, дори ефективността на борбата с тежката, и особено с организираната престъпност и тероризма, да може до голяма степен да зависи от използването на модерни техники на разследване, сама по себе си подобна цел от общ интерес не би могла по никакъв начин да обоснове приемането като необходима за целите на тази борба на национална правна уредба, предвиждаща общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 51).

104 Във връзка с това следва да се отбележи, от една страна, че предвид характеристиките си, описани в точка 97 от настоящото решение, такава правна уредба прави от запазването на данни за трафик и на данни за местонахождение правило, докато с установената с Директива 2002/58 система се изисква то да бъде изключение.

105 От друга страна, национална правна уредба като разглежданата в главното производство, която се отнася общо за всички абонати и регистрирани ползватели, като визира всички средства за електронни съобщения, както и всички данни за трафик, не предвижда каквото и да било диференциране, ограничение или изключение в зависимост от преследваната цел. Тя 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 извършени тежки престъпления. Освен това тя не предвижда никакво изключение, поради което се прилага и за лица, чиито съобщения според националното право представляват професионална тайна (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 57 и 58).

106 Такава правна уредба не изисква никаква връзка между данните, които се предвижда да бъдат запазвани, и наличието на заплаха за обществената сигурност. По-специално тя 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 престъпността (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 59).

107 Националната правна уредба като разглежданата в главното производство следователно 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.

108 При все това обаче 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, при условие че запазването на данни е ограничено до строго необходимото, що се отнася до подлежащите на запазване данни, визираните съобщителни средства, съответните лица, както и установения период на запазване.

109 За да отговори на изискванията, посочени в предходната точка от настоящото решение, тази национална правна уредба трябва, на първо място, да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито данни са запазени, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби. Тя трябва в частност да посочва обстоятелствата и условията, при които превантивно може да се приложи мярка за запазване на данни, като по този начин гарантира ограничаването ѝ до строго необходимото (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 54 и цитираната съдебна практика).

110 На второ място, по отношение на материалните условия, на които трябва да отговаря национална правна уредба, позволяваща в рамките на борбата с престъпността превантивно запазване на данни за трафик и на данни за местонахождение, за да се гарантира, че тя се ограничава до строго необходимото, следва да се отбележи, че макар условията да могат да варират в зависимост от мерките, които се вземат за целите на превенцията, разследването,

разкриването и преследването на тежки престъпления, то запазването на данни трябва да отговаря винаги на обективни критерии, установяващи връзка между подлежащите на запазване данни и преследваната с това цел. Такива условия трябва по-специално да се явяват на практика реално ограничаващи обхвата на мярката, а следователно и засегнатите лица.

111 [Поправено с определение от 16 март 2017 г.] Що се отнася до ограничаването на такава мярка по отношение на лицата и случаите, за които тя евентуално може да се приложи, националната правна уредба трябва да е основана на обективни обстоятелства, които да правят възможно с нея да се визират лица, чиито данни могат да имат връзка, макар и непряка, с тежки престъпления, да допринася по един или друг начин за борбата с тежката престъпност или да предотвратява сериозен риск за обществената сигурност. Такова ограничаване може да се постигне с географски критерий, когато въз основа на обективни обстоятелства компетентните национални органи установят, че в една или в няколко географски зони съществува повишен риск от подготвяне или извършване на такива престъпления.

112 С оглед на всички изложени съображения на първия въпрос по дело C-203/15 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 национална правна уредба, която за целите на борбата с престъпността предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства.

По втория въпрос по дело C-203/15 и по третия въпрос по дело C-698/15

113 Най-напред следва да се отбележи, че Kammarrätten i Stockholm (Апелативен административен съд Стокхолм) поставя втория си въпрос по дело C-203/15 само в случай на отрицателен отговор на първия въпрос по същото дело. Този втори въпрос обаче няма нищо общо с това дали запазването на данни е общо, или избирателно по смисъла, разгледан в точки 108—111 от настоящото решение. Ето защо на втория въпрос по дело C-203/15 и на първия въпрос по дело C-698/15 — поставен без оглед на обхвата на задължението за запазване на данни, което може да се наложи на доставчиците на електронни съобщителни услуги — следва да се даде общ отговор.

114 С втория въпрос по дело C-203/15 и първия въпрос по дело C-698/15 запитващите юрисдикции искат по същество да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 7 и 8 и член 52, параграф 1от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентни национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза.

115 По отношение на целите, които биха могли да обосноват национална правна уредба, с която се дерогира принципът на поверителност на електронните съобщения, следва да се напомни, че тези цели, както бе констатирано в точки 90 и 102 от настоящото решение, са изчерпателно изброени в член 15, параграф 1, първо изречение от Директива 2002/58, поради което следователно при достъп до запазените данни действително и строго трябва да се преследва някоя от тях. Освен това преследваната с такава правна уредба цел трябва да е свързана с тежестта на намесата в основните права, до която води достъпът до запазените данни, поради което същият би бил обоснован — що се отнася до превенцията, разследването, разкриването и преследването на престъпления — само в случаите на борба с тежката престъпност.

116 За да спазва принципа на пропорционалност, национална правна уредба относно условията, при които доставчиците на електронни съобщителни услуги са длъжни да предоставят на компетентните национални органи достъп до запазените данни, трябва да гарантира, че такъв достъп, както бе констатирано в точки 95 и 96 от настоящото решение, е допустим само в границите на строго необходимото.

117 Освен това, тъй като съгласно съображение 11 от Директива 2002/58 следва да бъдат „предмет на [подходящи гаранции]“, законодателните мерки по член 15, параграф 1 от същата директива трябва, както следва от цитирана в точка 109 от настоящото решение съдебна практика, да предвиждат ясни и точни правила при какви обстоятелства и при какви условия доставчиците на електронни съобщителни услуги са длъжни да предоставят на компетентните национални органи достъп до данните. Такива мерки трябва освен това да са задължителни по вътрешното право.

118 За да гарантира, че достъпът на компетентните национални органи до запазените данни е ограничен до строго необходимото, националното право следва действително да определя условията, при които доставчиците на електронни съобщителни услуги са длъжни да предоставят такъв достъп. При все това обаче съответната национална правна уредба не може да се ограничи до изискване достъпът да отговаря на някоя от целите по член 15, параграф 1 от Директива 2002/58, била тя и борбата с тежката престъпност. Всъщност такава национална правна уредба трябва да предвижда също и материални и процесуални условия за достъп на компетентните национални органи до запазените данни (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 61).

119 В този смисъл, тъй като един общ достъп до всички запазени данни — независимо дали те имат някаква, макар и непряка връзка с преследваната цел — не може да се счита за ограничен до строго необходимото, съответната национална правна уредба трябва да се основава на обективни критерии за определяне на обстоятелствата и условията, при които на компетентните национални органи трябва да се предоставя достъп до данните на абонатите или на регистрираните ползватели. В това отношение за целите на борбата с престъпността достъп може по принцип да се предостави само до данните на лица, които са заподозрени, че подготвят, извършват или са извършили тежко престъпление или че по някакъв начин са участвали в такова престъпление (вж. по аналогия ЕСПЧ, Решение по дело Захаров с/у Русия от 4 декември 2015 г., CE:ECHR:2015:1204JUD004714306, § 260). При все това в някои изключителни случаи като тези, при които жизнено важни интереси на националната сигурност, отбраната или обществената сигурност са застрашени от терористични действия, достъп до данните би могъл да се предостави и на други лица, ако съществуват обективни обстоятелства, позволяващи да се приеме, че в случая те действително биха могли да подпомогнат борбата с такива действия.

120 За да се гарантира на практика пълното спазване на тези условия, от съществено значение е достъпът на компетентните национални органи до запазените данни по принцип да се предоставя, освен в надлежно обосновани неотложни случаи, след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, и решението на тази юрисдикция или на тази структура да се постановява след мотивирана молба на тези органи, подадена по-специално в рамките на наказателни производства за предотвратяване, разкриване или наказателно преследване на престъпления (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 62; вж. също по аналогия, що се отнася до член 8 от ЕКПЧ, ЕСПЧ, Решение по дело Szabó и Vissy с/у Унгария от 12 януари 2016 г., CE:ECHR:2016:0112JUD003713814, §§ 77 и 80).

121 От значение е също компетентните национални органи, на които е предоставен достъп до запазените данни, да уведомят за това засегнатите лица в рамките на приложимите национални производства веднага щом това вече не може да попречи на водените от тези органи разследвания. Тази информация фактически е необходима, за да им се позволи да упражнят

правото си на възражение, изрично предвидено в член 15, параграф 2 от Директива 2002/58 във връзка с член 22 от Директива 95/46 в случай на нарушение на правата им (вж. по аналогия решения от 7 май 2009 г., Rijkeboer, C-553/07, EU:C:2009:293, т. 52 и от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 95).

122 Що се отнася до правилата за сигурност и защита на запазените данни от доставчиците на електронни съобщителни услуги, следва да се констатира, че член 15, параграф 1 от Директива 2002/58 не допуска държавите членки да дерогират член 4, параграф 1 и член 4, параграф 1а от същата директива. Последните разпоредби изискват от доставчиците да предприемат подходящи технически и организационни мерки, позволяващи да се гарантира ефикасна защита на запазените данни срещу рискове от злоупотреби и всякакъв незаконен достъп до тях. Предвид количеството на запазените данни, чувствителния им характер и риска от незаконен достъп до тях доставчиците на електронни съобщителни услуги, за да гарантират пълната неприкосновеност и поверителност на тези данни, трябва да осигурят особено завишено ниво на защита и на сигурност посредством подходящи технически и организационни мерки. В частност националната правна уредба трябва да предвижда, че данните следва да се запазват на територията на Съюза и безвъзвратно да се унищожават в края на периода за запазването им (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 66—68).

123 Във всички случаи държавите членки трябва да гарантират контрол от независим орган за спазването на равнището на защита, което правото на Съюза предвижда в областта на защитата на физическите лица при обработването на лични данни, тъй като член 8, параграф 3 от Хартата изрично изисква такъв контрол, представляващ съгласно установената практика на Съда съществен елемент от осигуряването на защита на лицата при обработването на лични данни. В противен случай лицата, чиито лични данни са били запазени, ще бъдат лишени от гарантираното в член 8, параграфи 1 и 3 от Хартата право да сезират националните надзорни органи с искане, за да защитят данните си (вж. в този смисъл решения Digital Rights, т. 68 и от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 41 и 58).

124 Запитващите юрисдикции следва да проверят дали и доколко разглежданите в главните производства национални правни уредби отговарят 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 и изяснени в точки 115—123 от настоящото решение, както по отношение на достъпа на компетентните национални органи до запазените данни, така и на защитата и равнището на сигурност на тези данни.

125 С оглед на всички изложени съображения на втория въпрос по дело C-203/15 и на първия въпрос по дело C-698/15 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 национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентни национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза.

По втория въпрос по дело C-698/15

126 С втория въпрос по дело C-698/15 Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение) иска по същество да се установи дали в решение Digital Rights Съдът тълкува членове 7 и/или 8 от Хартата в смисъл, който надхвърля тълкуването на член 8 от ЕКПЧ от Европейския съд по правата на човека.

127 Най-напред следва да се напомни, че макар признатите от ЕКПЧ основни права да са част от правото на Съюза като общи принципи, както потвърждава член 6, параграф 3 ДЕС, все пак, докато Съюзът не се присъедини към тази конвенция, тя не представлява юридически акт, формално интегриран в правния ред на Съюза (вж. в този смисъл решение от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 45 и цитираната съдебна практика).

128 Затова разглежданото в случая тълкуване на Директива 2002/58 трябва да се преценява единствено от гледна точка на основните права, гарантирани с Хартата (вж. в този смисъл решение от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 46 и цитираната съдебна практика).

129 Освен това следва да се напомни че разясненията по член 52 от Хартата сочат, че член 52, параграф 3 от същата има за цел да осигури необходимата последователност между Хартата и ЕКПЧ, „без това да засяга автономността на правото на Съюза и на Съда на Европейския съюз“ (решение от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 47). В частност, както изрично предвижда член 52, параграф 3, второ изречение от Хартата, член 52, параграф 3, първо изречение от същата не пречи правото на Съюза да предоставя по-широка защита, отколкото ЕКПЧ. Към това се прибавя накрая и фактът, че член 8 от Хартата се отнася до основно право, различно от това, за което се отнася член 7 от същата, като няма еквивалент в ЕКПЧ.

130 Съгласно постоянната практика на Съда обаче основанието на едно преюдициално запитване не е във формулирането на консултативни становища по общи или хипотетични въпроси, а в необходимостта от него за действителното решаване на спор, свързан с правото на Съюза (вж. в този смисъл решения от 24 април 2012 г., Kamberaj, C-571/10, EU:C:2012:233, т. 41, от 26 февруари 2013 г., Åkerberg Fransson, C-617/10, EU:C:2013:105, т. 42 и от 27 февруари 2014 г., Pohotovosť, C-470/12, EU:C:2014:101, т. 29).

131 В случая, като се имат предвид съображенията, изложени по-специално в точки 128 и 129 от настоящото решение, въпросът дали защитата по членове 7 и 8 от Хартата надхвърля тази по член 8 от ЕКПЧ, не може да окаже влияние върху тълкуването на Директива 2002/58 във връзка с Хартата, разглеждано в спора в главното производство по дело C-698/15.

132 В този смисъл отговорът на втория въпрос по дело C-98/15 явно не може да предостави тълкувателни критерии на правото на Съюза, които да са от полза за разрешаването на споменатия спор с оглед на същото това право.

133 Поради това вторият въпрос по дело C-698/15 е недопустим.

По съдебните разноски

134 С оглед на обстоятелството, че за страните по главното производство настоящото дело представлява отклонение от обичайния ход на производствата пред запитващите юрисдикции, последните следва да се произнесат 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 национална правна уредба, която за целите на борбата с престъпността предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства.

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 не допуска национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентни национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза.**

3) **Вторият въпрос на Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение), Обединено кралство) е недопустим.**

Подписи