Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

2 март 2021 година *

„Преюдициално запитване — Обработка на лични данни в сектора на електронните съобщения — Директива 2002/58/ЕО — Доставчици на електронни съобщителни услуги — Поверителност на съобщенията — Ограничения — Член 15, параграф 1 — Членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз — Правна уредба, предвиждаща общо и неизбирателно запазване на данни за трафика и данни за местонахождението от доставчиците на електронни съобщителни услуги — Достъп на националните органи до запазените данни за целите на разследвания — Борба с престъпността като цяло — Разрешение от прокуратурата — Използване на данните като доказателства в наказателното производство — Допустимост“

По дело C-746/18

с предмет преюдициално запитване, отправено на основание член 267 ДФЕС от Riigikohus (Върховен съд, Естония) с акт от 12 ноември 2018 г., постъпил в Съда на 29 ноември 2018 г., в рамките на наказателно производство срещу

H. K.,

в присъствието на:

Prokuratuur,

СЪДЪТ (голям състав),

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

генерален адвокат: G. Pitruzzella,

секретар: C. Strömholm, администратор,

предвид изложеното в писмената фаза на производството и в съдебното заседание от 15 октомври 2019 г.,

като има предвид становищата, представени:

– за H. K., от S. Reinsaar, vandeadvokaat,

– за Prokuratuur, от T. Pern и M. Voogma, в качеството на представители,

* Език на производството: естонски.

– за естонското правителство, от N. Grünberg, в качеството на представител,

– за датското правителство, от J. Nymann-Lindegren и M. S. Wolff, в качеството на представители,

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

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

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

– за унгарското правителство, от M. Z. Fehér и A. Pokoraczki, в качеството на представители,

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

– за португалското правителство, от L. Inez Fernandes, P. Barros da Costa, L. Medeiros и I. Oliveira, в качеството на представители,

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

– за правителството на Обединеното кралство, от S. Brandon и Z. Lavery, в качеството на представители, подпомагани от G. Facenna, QC, и de C. Knight, barrister,

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

след като изслуша заключението на генералния адвокат, представено в съдебното заседание от 21 януари 2020 г.,

постанови настоящото

Решение

1 Преюдициалното запитване се отнася 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, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“).

2 Запитването е отправено в рамките на наказателно производство, образувано срещу H. K. с обвинения за кражба, използване на банковата карта на трето лице и насилие по отношение на лица, участващи в съдебно производство.

Правна уредба

Правото на Съюза

3 Съображения 2 и 11 от Директива 2002/58 гласят:

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

[…]

(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 [Съюза]. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 15, параграф 1 от настоящата директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право. Следователно, настоящата директива не засяга възможността на държавите членки да провеждат законно прихващане на електронни комуникации или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с Европейската конвенция за защита на човешките права и основните свободи [подписана в Рим на 4 ноември 1950 г.], съгласно тълкуването на решенията на Европейския съд за човешките права. Такива мерки трябва да бъдат уместни, строго пропорционални на предвидената цел и необходими в едно демократично общество, и следва да бъдат предмет на съответна защита в съответствие с Европейската конвенция за защита на човешките права и основните свободи“.

4 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 обща[та регулаторна рамка за електронните съобщителни] мрежи и услуги (Рамкова директива) [ОВ L 108, 2002 г., стр. 33; Специално издание на български език, 2007 г., глава 13, том 35, стр. 195)].

Прилагат се също следните дефиниции:

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

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

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

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

[…]“.

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

„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“.

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

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

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

3. С цел маркетинг на електронни съобщителни услуги или за предоставянето на услуги с добавена стойност, доставчикът на обществено достъпна електронна съобщителна услуга може да обработва данните, упоменати в параграф 1, до степен и продължителност, необходими за

такива услуги или маркетинг, ако абонатът или ползвателят, за когото се отнасят данните, е дал предварително съгласието си. На ползватели или абонати трябва да бъде дадена възможността да оттеглят по всяко време съгласието си за обработка на данни за трафика.

[…]

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

[…]“.

7 Член 9 от Директива 2002/58 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. […]“.

8 Член 15 от посочената директива е озаглавен „Приложение на някои разпоредби от Директива [95/46]“ и параграф 1 от него предвижда:

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

Естонското право

Закон за електронните съобщения

9 Член 111[1] от elektroonilise side seadus (Закон за електронните съобщения, RT I 2004, 87, 593; RT I, 22.5.2018 г., 3) в редакцията му, приложима към фактите по главното производство (наричан по-нататък „Законът за електронните съобщения“), озаглавен „Задължение за запазване на данните“, предвижда:

„[…]

(2) Доставчиците на фиксирани и мобилни телефонни услуги, както и на мрежа за фиксирани и мобилни телефонни услуги са длъжни да запазват следните данни:

1) телефонния номер, от който се извършва повикването, името и адреса на абоната;

2) телефонния номер, към който е насочено повикването, името и адреса на абоната;

3) при ползването на допълнителна услуга като прехвърляне или пренасочване на повикване — номера, към който е пренасочено и ли прехвърлено повикването, името и адреса на абоната;

4) датата и часа на началото и края на повикването;

5) ползваната фиксирана или мобилна телефонна услуга;

6) международен идентификатор на викащия и на повикания мобилния абонат (International Mobile Subscriber Identity IMSI);

7) международен идентификатор на мобилното крайно устройство (International Mobile Equipment Identity — IMEI) на викащия и за повикания;

8) идентификатор на клетката в началото на повикването;

9) данни, идентифициращи географското местоположение на клетките чрез съотнасяне с идентификатора на клетката през периода, в който се запазват данните;

10) в случай на предплатени анонимни услуги — датата и часа на първоначалното активиране на услугата и знака за местоположение, откъдето е била активирана услугата.

[…]

(4) Данните по параграфи 2 и 3 от този член се запазват в продължение на една година от осъществяването на връзката, когато тези данни са създадени или обработени в процеса на предоставянето на съобщителната услуга. […]

[…]

(11) Данните по параграфи 2 и 3 от този член се предават:

1) по реда и условията на kriminaalmenetluse seadustik [Наказателно-процесуален кодекс] — на разследващия орган, на органа, упълномощен да извършва надзор, на прокуратурата или на съда;

[…]“.

Наказателно-процесуален кодекс

10 Член 17 от Наказателно-процесуалния кодекс (kriminaalmenetluse seadustik, RT I 2003, 27, 166; RT I, 31.5.2018 г., 22) гласи:

„(1) Страни в съдебното производство са прокуратурата […].

[…]“.

11 Член 30 от този кодекс има следното съдържание:

„(1) Прокуратурата ръководи производството по разследване, за чиято законосъобразност и ефективност трябва да следи, и представлява държавното обвинение пред съда.

(2) Правомощията на прокуратурата в наказателното производство се упражняват от нейно име от прокурор, който действа като независим орган и се подчинява само на закона“.

12 Член 90^1 от посочения кодекс предвижда:

„[…]

(2) Разследващият орган може да изиска — с разрешението на прокурора в производството по разследване, съответно с разрешението на съда в съдебното производство — от доставчика на електронни съобщителни услуги предаване на данните, изброени в член 111^1, параграфи 2 и 3 от Закона за електронните съобщения, извън посочените в параграф 1 от настоящия член. В разрешението се посочва периодът, за който може да се изисква предаване на данни, заедно с точните дати.

(3) Изискването на данни при условията на настоящия член е допустимо само ако е абсолютно необходимо за постигането на целта на наказателното производство“.

13 Член 211 от същия кодекс гласи:

„(1) Производството по разследване има за цел събиране на доказателства и изпълнение на другите условия за откриване на съдебното производство.

(2) В производството по разследване разследващият орган и прокурорът установяват фактите, които оневиняват или уличават заподозряното лице или обвиняемия“.

Закон за прокуратурата

14 Член 1 от prokuratuuriseadus (prokuratuuriseadus (Закон за прокуратурата, RT I 1998, 41, 625; RT I, 6.7.2018 г., 20) в редакцията му, приложима към фактите по главното производство, предвижда:

„(1) Прокуратурата е орган към Justiitsministeeriumi [Министерство на правосъдието], който участва в планирането на мерките за наблюдение, необходими за борба с престъпленията и за тяхното разкриване, ръководи производството по разследване, за чиято законосъобразност и ефективност трябва да следи, представлява държавното обвинение пред съда и изпълнява други възложени ѝ от закона функции.

(1[1]) Прокуратурата е независима при изпълнението на възложените ѝ от закона функции и действа по реда и при условията на този закон, други закони и на приетите въз основа на тях правни актове.

[…]“.

15 Член 2, параграф 2 от този закон гласи:

„Прокурорът е независим при изпълнението на възложените му задачи и действа единствено съгласно закона и по собствено убеждение“.

Спорът в главното производство и преюдициалните въпроси

16 С присъда на Viru Maakohus (Първоинстанционен съд на Виру, Естония) от 6 април 2017 г. H. K. е осъдена на две години лишаване от свобода за това, че в периода от 17 януари 2015 г. и 1 февруари 2016 г. е извършила няколко кражби на вещи (на стойност от 3 EUR до 40 EUR) и на парични суми (в размер от 5,20 EUR до 2100 EUR), използвала е банковата карта на трето лице, причинявайки на това лице вреда от 3941,82 EUR, и е упражнила насилие спрямо лица, участващи в съдебно производство, отнасящо се до нея.

17 За да осъди H. K. за тези престъпления, Viru Maakohus (Първоинстанционен съд Виру) се основава на доказателства, сред които няколко протокола, изготвени въз основа на данни за електронни съобщения по смисъла на член 111[1], параграф 2 от Закона за електронните съобщения, които разследващият орган е събрал от доставчик на електронни съобщителни услуги в хода на производството по разследване, след като на основание член 90 от Наказателно-процесуалния кодекс е получил няколко разрешения за тази цел от Viru Ringkonnaprokuratuur (районна прокуратура на Виру, Естония). Тези разрешения, предоставени на 28 януари, 2 февруари 2015 г., 2 ноември 2015 г. и 25 февруари 2016 г., се отнасят до данните относно няколко телефонни номера на H. K. и различни международни идентификационни номера на нейния мобилен апарат за периода от 1 януари до 2 февруари 2015 г., от 21 септември 2015 г., както и за периода от 1 март 2015 г. до 19 февруари 2016 г.

18 H. K. обжалва решението на Viru Maakohus (Първоинстанционен съд Виру) пред Tartu Ringkonnakohus (Апелативен съд Тарту, Естония), който отхвърля жалбата с решение от 17 ноември 2017 г.

19 H. K. подава касационна жалба срещу последното решение пред Riigikohus (Върховен съд, Естония), като оспорва по-специално допустимостта на протоколите, изготвени въз основа на данни, получени от доставчика на електронни съобщителни услуги. Според нея от решение от 21 декември 2016 г., Tele2 Sverige и Watson и др. (C-203/15 и C-698/15, наричано по-нататък „решение Tele2“, EU:C:2016:970) следва, че разпоредбите на член 111[1] от Закона за електронните съобщения, които предвиждат задължение за доставчиците на услуги да съхраняват данни за съобщенията, както и използването на тези данни за целите на осъждането ѝ противоречат на член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

20 Според запитващата юрисдикция възниква въпросът дали протоколите, изготвени въз основа на данните, посочени в член 111[1], параграф 2 от Закона за електронните съобщения, могат да се считат за допустими доказателства. Тази юрисдикция отбелязва, че допустимостта на разглежданите в главното производство протоколи като доказателствени средства зависи от въпроса доколко данните, въз основа на които са изготвени тези протоколи, са събрани в съответствие с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

21 Тази юрисдикция счита, че отговорът на този въпрос предполага да се определи дали член 15, параграф 1 във връзка с Хартата трябва да се тълкува в смисъл, че достъпът на държавните органи до данни, позволяващи идентифициране на източника и на адресата на телефонна комуникация, осъществена чрез фиксиран или мобилен телефон на заподозряно лице, определяне на нейната дата, час, продължителност и тип, използваното крайно устройство и мястото на използване на мобилно крайно устройство, представлява толкова тежка намеса в разглежданите основни права, че този достъп трябва да бъде ограничен до борбата с тежката престъпност, независимо за кой период от време се отнасят запазените данни, до които националните органи са поискали достъп.

22 Запитващата юрисдикция обаче счита, че продължителността на този период е съществен елемент за преценката на тежестта на намесата, каквато представлява достъпът до данните за трафик и до данните за местонахождение. Така, когато посоченият период е много кратък или обемът на събраните данни е много ограничен, следвало да се постави въпросът дали целта за борба с престъпността като цяло, а не само за борба с тежката престъпност може да обоснове подобна намеса.

23 Накрая, запитващата юрисдикция има съмнения относно възможността естонската прокуратура да се счита за независим административен орган по смисъла на точка 120 от решение от 21 декември 2016 г., Tele2 (C-203/15 и C-698/15, EU:C:2016:970), който може да разреши достъпа на разследващия орган до данни относно електронните съобщения като посочените в член 111[1], параграф 2 от Закона за електронните съобщения.

24 Прокуратурата ръководела производството по събиране на доказателства, като същевременно гарантирала неговата законосъобразност и ефективност. Тъй като целта на това производство е по-специално събирането на доказателства, разследващият орган и прокуратурата проверявали уличаващите и оневиняващите доказателства, събрани срещу всеки заподозрян или обвиняем. Ако прокуратурата е убедена, че са събрани всички необходими доказателства, тя предявявала обвинението срещу обвиняемия. Правомощията на прокуратурата се упражнявали от нейно име от прокурор, който е независим при изпълнението на възложените му функции, което е видно от член 30, параграфи 1 и 2 от Наказателно-процесуалния кодекс, както и от членове 1 и 2 от Закона за прокуратурата.

25 В този контекст запитващата юрисдикция отбелязва, че съмненията ѝ относно изискваната от правото на Съюза независимост се дължат главно на факта, че прокуратурата не само ръководи производството по събиране на доказателства, но и представлява държавното обвинение в съдебното производство, тъй като съгласно националното право този орган е страна в наказателното производство.

26 При тези обстоятелства Riigikohus (Върховен съд) решава да спре производството и да постави на Съда следните преюдициални въпроси:

1) Трябва ли член 15, параграф 1 от Директива [2002/58] във връзка с членове 7, 8 и 11 и член 52, параграф 1 от [Хартата] да се тълкува в смисъл, че в наказателно производство достъпът на държавни органи до данни, позволяващи идентифициране на източника и на адресата на комуникационната връзка, нейната дата, час, продължителност и тип, използваното крайно устройство и мястото на използване на мобилно крайно устройство във връзка с фиксирана или мобилна телефонна комуникационна връзка, осъществена от заподозряното лице, представлява толкова тежка намеса в неговите основни права, закрепени в посочените разпоредби на Хартата, че този достъп трябва да бъде ограничен — в рамките на предотвратяването, разследването, разкриването и преследването на престъпления — до целите на борбата с тежката престъпност, независимо за кой период от време се отнасят запазените данни, до които имат достъп държавни органи?

2) Трябва ли член 15, параграф 1 от Директива [2002/58], като се вземе предвид принципът на пропорционалност, откроен от Съда на Европейския съюз в точки 55—57 на [решение от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788)], да се тълкува в смисъл, че когато посочените в първия въпрос данни, до които имат достъп държавни органи, нямат голям обхват (както с оглед на техния вид, така и на времето, за което се отнасят), произтичащата от този достъп намеса в основни права по принцип може да бъде обоснована с целите на предотвратяване, разследване, разкриване и преследване на престъпления и че колкото по-голям е обхватът на достъпните за държавните органи данни, толкова по-тежки трябва да бъдат престъпленията, чието преследване обосновава намесата в основни права?

3) Означава ли установеното от Съда на Европейския съюз в точка 2 от диспозитива на (решение от 21 декември 2016 г.,Tele2 (C-203/15 и C-698/15, EU:C:2016:970) изискване, съгласно което достъпът на компетентните държавни органи до данните трябва да е подчинен на предварителен контрол от юрисдикция или от независима административна структура, че член 15, параграф 1 от Директива [2002/58] следва да се тълкува в смисъл, че прокуратурата като орган, който ръководи производството по разследване, задължен е по закон да действа независимо, подчинява се само на закона, длъжен е да установи в производството по разследване както уличаващите, така и оневиняващите обвиняемия факти, но и представлява държавното обвинение в съдебното производство, може да се счита за независима административна структура?“.

По преюдициалните въпроси

По първия и втория въпрос

27 С първия и втория си преюдициален въпрос, които следва да се разгледат заедно, запитващата юрисдикция иска по същество да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, позволяваща достъпа на публични органи до съвкупност от данни за трафик или данни за местонахождение, които могат да предоставят информация за комуникациите, извършени от ползвател на средство за електронна комуникация, или относно данните за местонахождението на използваните от него крайни устройства и да позволят да се направят точни изводи относно неговия личен живот за целите на предотвратяването, разследването, разкриването и преследването на престъпления, без този достъп да е ограничен до производствата за борба с тежката престъпност, независимо от продължителността на периода, за който е поискан достъпът до посочените данни, обема, както и естеството на наличните данни за подобен период.

28 В тази връзка от акта за преюдициално запитване следва, както естонското правителство потвърждава в хода на съдебното заседание, че данните, до които натовареният да извърши разследването национален орган е имал достъп в делото по главното производство са тези, събрани по силата на член 111^1, параграфи 2 и 4 от Закона за електронните съобщения, който налага на доставчиците на електронни комуникационни услуги задължение за общо и неизбирателно запазване на данните за трафика и за местонахождението, що се отнася до фиксираните и мобилни телефони в продължение на една година. Тези данни позволяват по-конкретно откриване и идентифициране на източника и на адресата на телефонна връзка, осъществена чрез фиксиран или мобилен телефон на дадено лице, да се определи нейната дата, час, продължителност и тип, използваното средство за комуникация, както и да се локализира мобилният телефон, без да е необходимо той да е бил използван. Нещо повече, те дават възможност да се определи честотата на комуникациите на ползвателя с определени лица през

определен период. Освен това, както потвърждава естонското правителство в съдебното заседание, в областта на борбата с престъпността достъпът до посочените данни може да се иска за всеки вид престъпление.

29 Що се отнася до условията, при които достъпът до запазените от доставчиците на електронни съобщителни услуги данни за трафик и данни за местонахождение може да се предостави с цел предотвратяване, разследване, разкриване и преследване на престъпления, на публични органи в изпълнение на мярка, приета на основание член 15, параграф 1 от Директива 2002/58, Съдът е постановил, че такъв достъп може да се предостави само ако тези данни са били запазени от доставчиците в съответствие с посочения член 15, параграф 1 (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 167).

30 В това отношение Съдът е постановил също, че посоченият член 15, параграф 1, разглеждан в светлината на членове 7, 8 и 11 и член 52, параграф 1 от Хартата, не допуска законодателни мерки, предвиждащи за тази цел превантивно общо и неизбирателно запазване на данни за трафик и на данни за местонахождение (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 168).

31 Що се отнася до целите, които могат да обосноват достъпа на публичните органи до запазените от доставчиците на електронни съобщителни услуги данни въз основа на съответстваща на тези разпоредби мярка, от една страна, от практиката на Съда следва, че такъв достъп може да бъде обоснован само с целта от общ интерес, за която това запазване е наложено на тези доставчици на услуги (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 166).

32 От друга страна, Съдът е постановил, че възможността за държавите членки да обосноват ограничение на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58, трябва да се прецени, като се измери тежестта на намесата, до която води това ограничение, и като се провери дали значението на преследваната с това ограничение цел от общ интерес е свързано с тази тежест (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 131 и цитираната съдебна практика).

33 Що се отнася до целта за предотвратяване, разследване, разкриване и преследване на престъпления, преследвана от разглежданата в главното производство правна уредба, в съответствие с принципа на пропорционалност единствено борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност могат да обосноват сериозна намеса в основните права, закрепени в членове 7 и 8 от Хартата, като тази, която предполага запазването на данни за трафик и на данни за местонахождение, независимо дали е общо, неизбирателно или целенасочено. При това положение само когато намесата в посочените основни права не е сериозна, тя може да бъде обоснована от целта, преследвана с разглежданата в главното производство правна уредба, за предотвратяване, разследване, разкриване и преследване общо на престъпления (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 140 и 146).

34 Във връзка с това е постановено по-конкретно, че законодателните мерки, насочени към обработването на данните за самоличността на ползвателите на електронни съобщителни средства като такива, и по-специално тяхното запазване и достъпът до тях единствено с цел да се установи самоличността на съответния потребител, без посочените данни да могат да се свържат с информация за извършените комуникации, могат да бъдат обосновани от целта за предотвратяване, разследване, разкриване и преследване общо на престъпления, посочена в член 15, параграф 1, първо изречение от Директива 2002/58. Всъщност сами по себе си тези данни не позволяват да се установи нито датата, часът, продължителността и адресатите на съобщенията, нито местата, на които те са осъществени, или тяхната честота с определени лица

през даден период, така че, освен координатите на ползвателите на електронни съобщителни средства, като техните адреси, те не предоставят никаква информация относно дадените комуникации и следователно относно техния личен живот. Поради това намесата, до която води мярка, насочена към тези данни, по принцип не може да бъде квалифицирана като „тежка“ (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 157 и 158 и цитираната съдебна практика).

35 При това положение само целите за борба с тежката престъпност или предотвратяването на сериозни заплахи за обществената сигурност са от естество да обосноват достъпа на публичните органи до съвкупност от данни за трафика или данни за местонахождението, които могат да дадат информация за извършените комуникации от даден ползвател на средство за електронна комуникация или за местонахождението на използваните от него крайни устройства и позволяват да се направят точни изводи относно личния живот на засегнатите лица (вж. в този смисъл решение от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 54), без други фактори, свързани с пропорционалността на подобно искане за достъп, като продължителността на периода, за който се иска достъп до подобни данни, да могат да имат за последица целта за предотвратяване, разследване, разкриване и преследване общо на престъпления да оправдае подобен достъп.

36 Следва да се отбележи, че достъпът до съвкупност от данни за трафик или данни за местонахождение като запазените по силата на член 111^1 от Закона за електронните съобщения действително може да позволи да се направят точни и дори много точни изводи относно личния живот на лицата, чиито данни са запазени, като навиците им в ежедневния живот, местата 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. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 117).

37 Несъмнено, както предлага запитващата юрисдикция, колкото по-дълъг е периодът, за който е поискан достъпа, толкова по принцип е по-голямо количеството данни, които могат да бъдат съхранявани от доставчиците на електронни съобщителни услуги относно извършените електронни комуникации, местата на престой и пътуванията на ползвателя на средство за електронна комуникация, позволявайки по този начин въз основа на консултираните данни да се направят повече изводи относно личния живот на този потребител. Аналогична констатация може да се направи относно категориите поискани данни.

38 Следователно, за да изпълнят изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото (решение от 6 октомври 2020 г., La Qurature и др., C-511/18 C-512/18 и C-520/18, EU:C:2020:791, т. 130 и цитираната съдебна практика), компетентните национални органи трябва да гарантират във всеки конкретен случай, че както визираните категории данни, така и продължителността, за която се иска достъп до тях, са ограничени, в зависимост от обстоятелствата по случая, до строго необходимото за целите на въпросното разследване.

39 При все това намесата в основните права, закрепени в членове 7 и 8 от Хартата, която предполага достъпът на публичен орган до съвкупност от данни за трафик или данни за местонахождение, които могат да предоставят информация за извършените комуникации от ползвател на средство за електронна комуникация или за местонахождението на използваните от него крайни устройства, при всички положения е сериозна, независимо от продължителността на периода, за който се иска достъп до тези данни, и от обема или вида на наличните данни за този период, когато, както е в делото по главното производство, от тази съвкупност от данни може да се направят точни изводи относно личния живот на засегнатото лице или лица.

40 В това отношение дори достъпът до ограничен обем данни за трафик или данни за местонахождение или достъпът до данни за кратък период може да предостави точна информация за личния живот на ползвател на средство за електронна комуникация. Освен това обемът налични данни и произтичащата от тях конкретна информация за личния живот на съответното лице са обстоятелства, които могат да се преценят едва след запознаване с посочените данни. Разрешението за достъп, предоставено от компетентната юрисдикция или от компетентния независим орган, обаче по необходимост се дава, преди да може да се направи справка с тези данни и информация. В този смисъл преценката на тежестта на намесата, която представлява достъпът, се извършва по необходимост в зависимост от риска, който обикновено се свързва с категорията поискани данни за личния живот на съответните лица, без освен това да има значение това дали произтичащата от тях информация за личния живот има конкретно чувствителен характер.

41 Накрая, като се има предвид, че запитващата юрисдикция е сезирана с искане за обявяване на недопустимостта на протоколи, изготвени въз основа на данни за трафик и данни за местонахождение, поради това че разпоредбите на член 111^1 от Закона за електронните съобщения противоречат на член 15, параграф 1 от Директива 2002/58 както по отношение на съхраняването на данните, така и по отношение на достъпа до тях, следва да се припомни, че при сегашното състояние на правото на Съюза в рамките на образувано наказателно производство срещу заподозрени в извършването на престъпления лица по принцип само националното право следва да определи правилата относно допустимостта и преценката на данни и на доказателства, които са били получени посредством общо и неизбирателно съхранение на тези данни в разрез с правото на Съюза (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 222) или още посредством достъп на националните органи до тези данни в разрез с това право.

42 Всъщност съгласно постоянната съдебна практика при липсата на правила на Съюза в тази област въз основа на принципа на процесуална автономия вътрешният правен ред на всяка държава членка трябва да уреди процесуалните правила за съдебните производства, предназначени да гарантират защитата на правата, които страните в процеса черпят от правото на Съюза, при условие обаче че те не са по-неблагоприятни от правилата, които уреждат подобни вътрешноправни положения (принцип на равностойност), и не правят практически невъзможно или прекомерно трудно упражняването на правата, предоставени от правото на Съюза (принцип на ефективност) (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 223 и цитираната съдебна практика).

43 Що се отнася по-специално до принципа на ефективност, следва да се припомни, че националните правила относно допустимостта и използването на данните и доказателствата имат за цел, съгласно направения от националното право избор, да се избегне неправомерно придобити данни и доказателства да нанесат неоснователно вреди на лице, заподозряно в извършване на престъпления. Съгласно националното право обаче тази цел може да бъде постигната не само със забрана за използване на такива данни и доказателства, но и чрез национални правила и практики, уреждащи преценката и претеглянето на данните и доказателствата, дори чрез отчитане на техния неправомерен характер, при определяне на наказанието (решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 225).

44 Необходимостта от изключване на данни и доказателства, получени в нарушение на предписанията на правото на Съюза, трябва да се преценява с оглед по-специално на опасността, която допустимостта на такива данни и доказателства представлява за спазването на принципа на състезателност, а следователно и на правото на справедлив съдебен процес. Юрисдикция, която счита, че дадена страна не може да обсъди ефикасно доказателствено средство от област, в която са необходими специални познания, които съдът няма, което може да повлияе съществено на преценката на фактите, трябва да констатира нарушение на правото

на справедлив съдебен процес и да изключи това доказателствено средство, за да се избегне подобно нарушение. Следователно принципът на ефективност налага на националния наказателен съд да не взема предвид данни и доказателства, които са били получени посредством несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик и на данни за местонахождение или още посредством достъп на компетентния орган до тези данни в нарушение на това право, в рамките на наказателно производство, образувано срещу заподозрени в престъпни деяния лица, ако тези лица не са в състояние да обсъдят ефективно тези данни и доказателства от област, в която са необходими специални познания, които съдът няма и които могат да повлияят съществено на преценката на фактите (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 226 и 227).

45 С оглед на гореизложените съображения на първия и втория въпрос следва да се отговори, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, позволяваща достъпа на публични органи до съвкупност от данни за трафик или данни за местонахождение, които могат да предоставят информация за комуникациите, извършени от ползвател на средство за електронна комуникация, или за местонахождението на използваните от него крайни устройства и да позволят да се направят точни изводи относно неговия личен живот, за целите на предотвратяването, разследването, разкриването и преследването на престъпления, без този достъп да е ограничен до производствата за борба с тежката престъпност или за предотвратяване на сериозни заплахи за обществената сигурност, независимо от продължителността на периода, за който е поискан достъпът до посочените данни, и от обема или вида на наличните данни за подобен период.

По третия въпрос

46 С третия си преюдициален въпрос запитващата юрисдикция по същество иска да се установи дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която оправомощава прокуратурата, чиято задача е да ръководи производството по разследване и евентуално да представлява държавното обвинение в последващо производство, за да разреши достъпа на публичен орган до данните за трафик и до данните за местонахождение за целите на събиране на доказателства в наказателно производство.

47 В това отношение запитващата юрисдикция уточнява, че макар съгласно националното право естонската прокуратура да е длъжна да действа независимо, е подчинена единствено на закона и трябва да разглежда уличаващите и оневиняващи доказателства в хода на производството по събиране на доказателства, това не променя факта, че целта на това производство остава събирането на доказателства, както и наличието на останалите необходими условия за провеждането на производството. Именно този орган представлява държавното обвинение и следователно е също страна в производството. Освен това от преписката, с която Съдът разполага, както потвърждават също естонското правителство и Prokuratuur в съдебното заседание, е видно, че естонската прокуратура е организирана йерархично и че за исканията за достъп до данни за трафик и до данни за местонахождение не се изисква особена форма и могат да бъдат подадени от самия прокурор. Накрая, лицата, до чиито данни може да се предостави достъп, не са само тези, заподозрени в участие в престъпление.

48 Вярно е, както Съдът вече е постановил, че националното право трябва да определи условията, при които доставчиците на електронни съобщителни услуги са длъжни да предоставят на компетентните национални органи достъп до данните, с които разполагат. При все това, за да изпълни изискването за пропорционалност, подобна правна уредба трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да налагат

минимални изисквания, така че лицата, чиито лични данни са засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на тези данни срещу рискове от злоупотреби. Тази уредба трябва да е задължителна по вътрешното право и да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на подобни данни, като по този начин гарантира ограничаването на намесата до строго необходимото (вж. в този смисъл решения от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 117 и 118, от 6 октомври 2020 г., Privacy International, C-623/17, EU:C:2020:790, т. 68 и от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 132 и цитираната съдебна практика).

49 По-специално приета на основание член 15, параграф 1 от Директива 2002/58 национална правна уредба, която урежда достъпа на компетентните органи до запазените данни за трафик и данни за местонахождение, не може да се ограничи до изискването достъпът на органите до данните да отговаря на преследваната с тази правна уредба цел, а трябва да предвижда също материални и процесуални условия за това използване (решения от 6 октомври 2020 г., Privacy International, C-623/17, EU:C:2020:790, т. 77 и от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 176 и цитираната съдебна практика).

50 В този смисъл, тъй като 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 въпросните данни. В това отношение във връзка с целта за борба с престъпността подобен достъп може по принцип да се предостави само до данните на лица, които са заподозрени, че подготвят, извършват или са извършили тежко престъпление или още че по някакъв начин са участвали в такова престъпление. При все това в някои изключителни случаи като тези, при които жизнено важните интереси на националната сигурност, отбраната или обществената сигурност са застрашени от терористични дейности, достъп до данните на други лица също би могъл да се предостави, ако съществуват обективни обстоятелства, позволяващи да се приеме, че в случая тези данни действително биха могли да подпомогнат борбата с такива дейности (вж. в този смисъл решения от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 119 и от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 188).

51 За да се гарантира на практика пълното спазване на тези условия, от съществено значение е достъпът на компетентните национални органи до запазените данни да се предоставя 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. В надлежно обосновани спешни случаи контролът трябва да бъде осъществен в кратък срок (вж. в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 189 и цитираната съдебна практика).

52 Както по същество отбелязва генералният адвокат в точка 105 от заключението си, този предварителен контрол изисква, наред с останалото, юрисдикцията или административната структура, натоварена с извършването на посочения предварителен контрол, да разполага с всички правомощия и да представи всички необходими гаранции, за да осигури съвместяване на различните разглеждани интереси и права. Що се отнася по-специално до наказателно разследване, подобен контрол изисква тази юрисдикция или структура да е в състояние да осигури справедливо равновесие между, от една страна, интересите, свързани с нуждите на

разследването в рамките на борбата с престъпността, и от друга страна, основните права на зачитане на личния живот и на защита на личните данни на лицата, чиито данни са засегнати от достъпа.

53 Когато този контрол се извършва не от юрисдикция, а от независима административна структура, същата трябва да се ползва със статут, който ѝ позволява при упражняването на нейните функции да действа по обективен и безпристрастен начин и да бъде за тази цел защитена от всякакво външно влияние (вж. в този смисъл решение от 9 март 2010 г., Комисия/Германия, C-518/07, EU:C:2010:125, т. 25 и становище 1/15 (Споразумение PNR ЕС—Канада) от 26 юли 2017 г., EU:C:2017:592, т. 229 и 230).

54 От изложените по-горе съображения следва, че изискването за независимост, на което трябва да отговаря административната структура, натоварена с упражняването на предварителния контрол, припомнен в точка 51 от настоящото решение, налага тази структура да има качеството на трето лице по отношение на лицето, което иска достъп до данните, така че първата да е в състояние да упражнява този контрол обективно и безпристрастно, без каквото и да било външно влияние. По-специално в наказателноправната област изискването за независимост предполага, както по същество отбелязва генералният адвокат в точка 126 от заключението си, структурата, на която е възложен този предварителен контрол, от една страна, да не участва в провеждането на въпросното наказателно разследване и от друга страна, да заема неутрално положение по отношение на страните в наказателното производство.

55 Не е такъв случаят на прокуратура, която ръководи производството по разследване и евентуално представлява държавното обвинение. Всъщност задачата на прокуратурата не е да решава напълно самостоятелно даден спор, а евентуално да го отнесе до компетентната юрисдикция в качеството си на страна в процеса, действаща в рамките на наказателното преследване.

56 Обстоятелството, че в съответствие с правилата относно функциите и статута ѝ прокуратурата е длъжна да провери уличаващите и оневиняващите доказателства, да гарантира законосъобразността на производството по събиране на доказателства и да действа единствено по силата на закона и на убеждението си, не е достатъчно, за да ѝ се предостави статут на трето лице спрямо разглежданите интереси в смисъла, описан в точка 52 от настоящото решение.

57 От това следва, че прокуратурата не е в състояние да осъществи посочения в точка 51 от настоящото решение предварителен контрол.

58 Освен това, тъй като запитващата юрисдикция повдига въпроса дали липсата на контрол, извършван от независима структура, може да се компенсира чрез последващ контрол, упражняван от юрисдикция за законосъобразността на достъпа на национален орган до данните за трафик и до данните за местонахождение, важно е да се отбележи, че независимият контрол трябва да се осъществи, както изисква припомнената в точка 51 от настоящото решение съдебна практика, преди всеки достъп, освен в надлежно обосновани спешни случаи, когато контролът трябва да се извърши в кратки срокове. Както отбелязва генералният адвокат в точка 128 от заключението си, такъв последващ контрол не би позволил да се отговори на целта за предварителен контрол, а именно да се предотврати разрешаването на достъп до разглежданите данни, който надхвърля границите на строго необходимото.

59 При тези условия на третия преюдициален въпрос следва да се отговори, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която оправомощава прокуратурата, чиято задача е да ръководи наказателното разследване и евентуално да

представлява държавното обвинение в последващо производство, да разреши достъпа на публичен орган до данните за трафик и до данните за местонахождение за целите на наказателно разследване.

По съдебните разноски

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

По изложените съображения Съдът (голям състав) реши:

1) **Член 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, позволяваща достъпа на публични органи до съвкупност от данни за трафик или данни за местонахождение, които могат да предоставят информация за комуникациите, извършени от ползвател на средство за електронна комуникация, или за местонахождението на използваните от него крайни устройства и да позволят да се направят точни изводи относно неговия личен живот, за целите на предотвратяването, разследването, разкриването и преследването на престъпления, без този достъп да е ограничен до производствата за борба с тежката престъпност или за предотвратяване на сериозни заплахи за обществената сигурност, независимо от продължителността на периода, за който е поискан достъпът до посочените данни, и от обема или вида на наличните данни за подобен период.**

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 оправомощава прокуратурата, чиято задача е да ръководи наказателното разследване и евентуално да представлява държавното обвинение в последващо производство, да разреши достъпа на публичен орган до данните за трафик и до данните за местонахождение за целите на наказателно разследване.**

Подписи