



Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ

G. PITRUZZELLA

представено на 21 януари 2020 година¹

Дело C-746/18

**Н. К.
срещу
Prokuratuur**

(Преюдициално запитване, отправено от Riigikohus (Върховен съд, Естония))

„Преюдициално запитване — Обработката на лични данни в сектора на електронните съобщения — Поверителност на електронните съобщения — Доставчици на електронни съобщителни услуги — Общо и неизбирателно запазване на данни за трафика и данни за местонахождението — Наказателно разследване — Достъп на разследващия орган до запазените данни, отнасящи се за периоди от време от един ден до една година — Разрешение, издадено от прокуратурата — Използване на данните като доказателства в наказателното производство — Директива 2002/58/ЕО — Член 1, параграф 3, член 3 и член 15, параграф 1 — Харта на основните права на Европейския съюз — Членове 7, 8 и 11 и член 52, параграф 1“

I. Въведение

1. Настоящото преюдициално 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)², изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г.³, във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз⁴.

2. Запитването е отправено в рамките на наказателно производство, образувано срещу Н. К., предвид това, че последната е извършила няколко кражби, използвала е банкова карта, принадлежаща на друго лице, и е извършила действия на насилие спрямо участващо в съдебно производство лице.

3. Протоколите, въз основа на които се установява извършването на тези престъпления, са изготвени по-специално въз основа на лични данни, създадени при доставката на електронни съобщителни услуги. Riigikohus (Върховен съд, Естония) изразява съмнения относно съвместимостта с правото на Съюза на условията, при които разследващите органи са имали достъп до тези данни.

¹ Език на оригиналния текст: френски.

² ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63.

³ ОВ L 337, 2009 г., стр. 11, наричана по-нататък „Директива 2002/58“.

⁴ Наричана по-нататък „Хартата“.

4. Тези съмнения се отнасят, на първо място, до въпроса дали продължителността на периода, по отношение на който разследващите органи са имали достъп до данните, представлява критерий, позволяващ да се прецени тежестта на намесата в основните права на засегнатите лица, до която води този достъп.

5. На второ място, запитващата юрисдикция иска да се установи дали Prokuratuur (прокуратура, Естония), предвид различните функции, които са ѝ възложени от естонското законодателство, представлява „независима“ административна структура по смисъла на решение от 21 декември 2016 г., *Tele2 Sverige и Watson и др.*⁵

II. Правна уредба

A. Директива 2002/58

6. Съгласно член 1, параграф 3 от Директива 2002/58 същата „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“.

7. В допълнение, член 15, параграф 1 от тази директива гласи, че „[д]ържавите 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 криминални нарушения или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО⁶]. 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“.

Б. Естонското право

1. Закон за електронните съобщения

8. *Elektroonilise side seadus* (Закон за електронните съобщения)⁷ от 8 декември 2004 г. в редакцията му, приложима към спора по главното производство, в член 111¹, озаглавен „Задължение за запазване на данните“, гласи:

„[...]“

5 C-203/15 и C-698/15, наричано по-нататък „решение *Tele2 Sverige и Watson и др.*“, EU:C:2016:970 (т. 120 и диспозитив, подточка 2).

6 Директива 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 L281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10).

7 RT I 2004, 87, 593.

(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 или 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 викация и на повикания мобилния абонат (*International Mobile Subscriber Identity* IMSI);
- 7) международен идентификатор на мобилното крайно устройство (*International Mobile Equipment Identity* — IMEI) на викация 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 кодекс⁸] — на разследващия орган, на органа, упълномощен да извършва надзор, на прокуратурата или на съда;

[...]“.

2. Наказателно-процесуален кодекс

9. Член 17, параграф 1 от Наказателно-процесуалния кодекс, в редакцията му, приложима към спора по главното производство, озаглавен „Страни в съдебното производство“, гласи:

„Страни в съдебното производство са прокуратурата [...]“.

⁸ RT I 2003, 27, 166.

10. Съгласно член 30 от Наказателно-процесуалния кодекс, озаглавен „Прокуратурата в наказателното производство“:

„(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“.

11. Член 90¹ от Наказателно-процесуалния кодекс, озаглавен „Изискване за предаване на данни от предприятие за електронни съобщения“, предвижда в параграфи 2 и 3:

(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 111¹, 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“.

12. Член 211 от Наказателно-процесуалния кодекс, озаглавен „Цел на производството по разследване“, гласи следното:

„(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“.

3. Закон за прокуратурата

13. Prokuratuuriseadus (Закон за прокуратурата)⁹ от 22 април 1998 г. в редакцията си, приложима към спора по главното производство, в член 1, озаглавен „Прокуратура“, 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.

(1¹) 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.

[...]“.

⁹ RT I 1998, 41, 625.

14. Член 2 от Закона за прокуратурата, озаглавен „Прокурорът“, предвижда в параграф 2:

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

III. Фактите, главното производство и преюдициалните въпроси

15. С присъда на Viru Maakohus (Първоинстанционен съд Виру, Естония) от 6 април 2017 г. Н. К. е осъдена на две години лишаване от свобода за това, че в периода от 4 август 2015 г. до 1 февруари 2016 г. е извършила осем кражби на хранителни продукти и други движими 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 друго лице, за да тегли пари от банкомат, причинявайки на това лице вреда от 3941,82 EUR, и е упражнила насилие спрямо лице, участващо в съдебното производство¹⁰.

16. За да осъди Н. К. за тези престъпления, Viru Maakohus (Първоинстанционен съд Виру) се основава на доказателства, сред които няколко протокола, изготвени въз основа на данни за електронни съобщения, посочени в член 111¹, 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 90¹, параграф 2 от Наказателно-процесуалния кодекс е получил разрешения от прокурор от Viru Ringkonnaprokuratuur (районна прокуратура на Виру, Естония).

17. Така на 2 ноември 2015 г. прокурор от районната прокуратура на Виру издава на разследващия орган разрешение да изиска от предприятие за електронни съобщения предаването на данните, посочени в член 111¹, параграф 2 от Закона за електронните съобщения, за да определи чрез два мобилни телефонни номера на Н. К. осъществяването на 21 септември 2015 г. на телефонни разговори и текстови съобщения, продължителността и начина на предаването им, както и личните данни и местонахождението на повикващия/изпращащия и повикания/получателя.

18. На 4 ноември 2015 г. разследващият орган изготвя протокол за данните, получени от предприятието за електронни съобщения съгласно това разрешение, в който са отбелязани предавателните мачти, в обхвата на които на 21 септември 2015 г. след 19:00 ч. е използван абонатният номер на Н. К. Въз основа на този протокол, както и на други доказателства, прокуратурата иска да установи пред съда, че Н. К. е извършила кражбата от 21 септември 2015 г.

19. На 25 февруари 2016 г. прокурор от районната прокуратура на Виру издава за целите на разследването на престъпление по член 303, параграф 1 от Karistusseadustik (Наказателен кодекс)¹¹ разрешение разследващият орган да изиска от оператора на електронни съобщителни услуги предаване на данни по член 111¹, параграф 2 от Закона за електронните съобщения за седем абонатни номера, използвани от Н. К. в периода от 1 март 2015 г. до 19 февруари 2016 г.

¹⁰ Запитващата юрисдикция уточнява, че след присъединяването на това наказание към наказанието от четири години и седем месеца лишаване от свобода, наложено от Viru Maakohus (Първоинстанционен съд Виру) с присъда от 22 март 2016 г., на Н. К. е наложено окончателно общо наказание пет години и един месец лишаване от свобода.

¹¹ Става въпрос за престъпление, представляващо оказване на влияние върху правосъдието. Следва да се отбележи, че деянията, за които е обвинена Н. К., в това отношение са били преквалифицирани от Viru Maakohus (Първоинстанционен съд Виру) в съответствие с член 323, параграф 1 от Наказателния кодекс в упражняване на насилие спрямо лице, участващо в съдебно производство.

20. На 15 март 2016 г. разследващият орган изготвя протокол за данните, получени от предприятието за електронни съобщения съгласно това разрешение, в който са посочени датите, на които Н. К. е осъществила изходящи повиквания до другите подсъдими и е приела от тях входящи повиквания, и за датите, на които Н. К. им е изпратила и е получила от тях текстови съобщения. Въз основа на този протокол, както и на други доказателства, прокурорът иска да установи пред съда, че от пролетта на 2015 г. Н. К. няколкократно е отправяла по телефона заплахи до другите подсъдими.

21. На 20 април и 6 май 2016 г. разследващият орган изготвя още протоколи относно данните, получени от предприятието за електронни съобщения съгласно същото разрешение. В тези протоколи се посочват базовите станции, в чийто обхват на 4, 27 и 31 август 2015 г., както и от 1 до 3 септември 2015 г., са изпратени и получени телефонните повиквания чрез шест от използваните от Н. К. абонатни номера. Въз основа на тези протоколи и на всички други доказателства прокуратурата иска да докаже пред съда, че шестте кражби в посочените дни са извършени от Н. К.

22. На 20 април 2016 г. разследващият орган изготвя протокол, в който се съдържат данни за два от използваните от Н. К. абонатни номера. В протокола по-специално са отбелязани базовите станции, в чийто обхват в периода от 16 до 19 януари 2015 г. са осъществени изходящи и входящи повиквания от и до тези абонатни номера. Въз основа на този протокол, както и на други доказателства, прокурорът иска да установи, че тегленето на пари от банкомат с банковата карта на пострадалия в периода от 17 до 19 януари 2015 г. е извършено от Н. К.

23. Отразените в посочения протокол данни са получени от предприятието за електронни съобщения въз основа на разрешения, издадени на 28 януари и 2 февруари 2015 г. от прокурор от районната прокуратура на Виру по друго наказателно производство. Въпросното производство е било за престъпления по член 200, параграф 2, точки 7, 8 и 9 от Наказателния кодекс, а именно два грабежа, извършени на 23 и 27 януари 2015 г. от група с използване на оръжие и чрез проникване с взлом. Въз основа на тези разрешения за разследващия орган е било възможно да изиска от предприятието за електронни съобщения да предаде данните по член 111¹, параграф 2 от Закона за електронните съобщения, отнасящи се за използваните от Н. К. два абонатни номера и различните международни идентификатори на мобилните крайни устройства в периода от 1 януари до 2 февруари 2015 г.

24. От това описание на фактите по главното производство става ясно, че в съответствие с член 90¹, параграф 2 от Наказателно-процесуалния кодекс прокуратурата разрешава на разследващия орган да отправя искания за данни до предприятието за електронни съобщения в производството по разследване. Разрешенията се отнасят до данни за абонатните номера на подсъдимата и се издават за целите на разследването на различни престъпления, като обхващат периоди съответно от един ден, от около един месец и от около една година.

25. Н. К. подава въззивна жалба срещу решението на Viru Maakohus (Първоинстанционен съд Виру) пред Tartu Ringkonnakohtus (Апелативен съд Тарту, Естония), който отхвърля жалбата с решение от 17 ноември 2017 г. Н. К. подава касационна жалба до Riigikohtus (Върховен съд), като иска отмяната на присъдата на първата инстанция и решението на втората инстанция, прекратяването на наказателното производство срещу нея и постановяването на оправдателна присъда.

26. Н. К. поддържа, че протоколите с отразените данни, получени от предприятието за електронни съобщения, не са допустимо доказателствено средство и осъждането ѝ въз основа на тези доказателства е необосновано. Съгласно решение *Tele2 Sverige и Watson и др.*, правилата на член 111¹ от Закона за електронните съобщения, които предвиждат задължение за тези доставчици на услуги да съхраняват данни за съобщенията, както и използването на тези данни за целите на осъждането ѝ, били в противоречие с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

27. Според запитващата юрисдикция по този начин се поставя въпросът дали разглежданите протоколи, изготвени от разследващия орган въз основа на данните, посочени в член 111¹, параграф 2 от Закона за електронните съобщения, и изискани от предприятието за електронни съобщения с разрешение на прокуратурата, могат да се считат за допустими доказателства.

28. Сред данните, които доставчиците на електронни съобщителни услуги са длъжни да запазят за период от една година, се включват телефонният номер, от който се извършва повикването, и телефонният номер, до който е насочено повикването, името и адресът на абоната, датата и часът на началото и края на повикването, ползваната фиксирана или мобилна телефонна услуга, международният идентификатор на мобилния абонат, международният идентификатор на мобилното крайно устройство на викация и на повикания, както и идентификатор на клетката в началото на повикването и данните, идентифициращи географското местоположение на клетката. Запитващата юрисдикция отбелязва, че в случая става въпрос за данни, свързани с наличието на осъществена връзка под формата на повиквания и съобщения посредством фиксиран или мобилен телефон, както и с местоположението на мобилно крайно устройство, но че те не дават информация за съдържанието на съобщенията.

29. От решение *Tele2 Sverige и Watson и др.* и от решение от 2 октомври 2018 г., *Ministerio Fiscal*¹², следвало, че национална правна уредба, регулираща запазването на данни за трафика и на данни за местонахождението, както и достъпа до тези данни в рамките на наказателно производство като съдържащата се в член 111¹, параграфи 2 и 4 от Закона за електронните съобщения и член 90¹, параграф 2 от Наказателно-процесуалния кодекс, попадала в приложното поле на Директива 2002/58.

30. Допустимостта на доказателствата била обусловена от спазването на процесуалните разпоредби за събирането им. Следователно при преценката на допустимостта на разглежданите в главното производство протоколи като доказателствени средства запитващата юрисдикция трябва да разгледа въпроса доколко данните, въз основа на които са изготвени тези протоколи, са събрани от предприятие за електронни съобщения 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.

31. Предвид решения *Tele2 Sverige и Watson и др.*¹³ и *Ministerio Fiscal*¹⁴ запитващата юрисдикция 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 достъпът на държавните органи до данни, позволяващи откриване и идентифициране на източника и на адресата на телефонната връзка, осъществена чрез фиксиран или мобилен телефон на заподозряното лице, нейната дата, час, продължителност и тип, използваното крайно устройство и мястото на използване на мобилно крайно устройство, представлява толкова

¹² C-207/16, наричано по-нататък „решение *Ministerio Fiscal*“, EU:C:2018:788.

¹³ Диспозитив, подточка 2 от това решение.

¹⁴ Точки 53 и 57 от това решение.

тежка намеса в основните права, закрепени в посочените разпоредби на Хартата, че този достъп трябва да бъде ограничен до целите на борбата с тежката престъпност, независимо за кой период от време се отнасят запазените данни, до които тези национални органи са поискали достъп.

32. В това отношение запитващата юрисдикция счита, че периодът, за който се изискват въпросните данни, е обстоятелство от съществено значение за преценката за тежестта на намесата в основните права, до която би довел достъпът до разглежданите данни. Следователно било възможно тази намеса да не се счита за тежка, когато изискваните данни се отнасят само до много кратък период от време, както например един ден. В този случай по принцип не е възможно въз основа на тези данни да се направят точни заключения относно личния живот на съответното лице, така че достъпът на националните органи до посочените данни би могъл да се обоснове с целите на преследването и разследването на престъпленията като цяло.

33. Освен това запитващата юрисдикция иска да се установи дали с оглед на изводите, произтичащи от решение *Ministerio Fiscal*¹⁵, достъпът до данни като тези по главното производство, може да бъде обоснован със същата цел, когато количеството на данните, до които имат достъп компетентните органи, е ограничено и поради това намесата в разглежданите основни права не е толкова тежка. Що се отнася до обхвата на данните, съществено е да се вземе предвид техният вид (като данните, свързани с адресата на повикването или местоположението на крайното устройство) и времето, за което се отнасят (например за един ден, месец или година). Според тази юрисдикция колкото по-тежко е престъплението, толкова по-тежка може да бъде допустимата намеса в основни права за целите на наказателното производство, което означава, че толкова по-голям може да бъде обхватът на данните, до които държавните органи могат да имат достъп.

34. Накрая, запитващата юрисдикция иска да се установи дали прокуратурата може да се счита за „независима“ административна структура по смисъла на решение *Tele2 Sverige и Watson и др.*¹⁶. Тя отбелязва, че в Естония именно прокуратурата ръководи производството по разследване, чиято цел по-специално е събирането на доказателства. Подчертава също, че разследващият орган и прокуратурата установяват фактите, които уличават или оневиняват заподозряното лице. Накрая отбелязва, че правомощията на прокуратурата се упражняват 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 и от член 1, параграфи 1 и 1¹ и член 2, параграф 2 от Закона за прокуратурата.

35. В този контекст запитващата юрисдикция подчертава, че съмненията ѝ относно изискваната от правото на Съюза независимост се дължат преди всичко на обстоятелството, че след провеждане на производството по разследване прокуратурата повдига обвинение на съответното лице, ако счита, че са събрани всички необходими доказателства и е налице основание за това. Тази юрисдикция отбелязва, че в този случай прокуратурата повдига и поддържа обвинението пред съда и следователно също е страна в производството. Запитващата юрисдикция отбелязва също, че Европейският съд по правата на човека вече е приел, че при определени условия мерките за наблюдение могат да бъдат разрешени и без предварителен съдебен контрол, когато такъв контрол се осъществява *a posteriori*¹⁷.

¹⁵ Точки 55—57 от това решение.

¹⁶ Точка 120 и диспозитив, подточка 2 от това решение.

¹⁷ По този въпрос запитващата юрисдикция цитира решения на ЕСПЧ от 2 септември 2010 г., *Uzun c/y Германия* (СЕ:ЕCHR:2010:0902JUD003562305, § 71—74) и от 12 януари 2016 г., *Szabó и Vissy c/y Унгария* (СЕ:ЕCHR:2016:0112JUD003713814, § 77).

36. При тези условия Riigikohus (Върховен съд, Естония) 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 местоположението 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, открит от Съда на Европейския съюз в решение [Ministerio Fiscal], т. 55—57, 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 решение [Tele2 Sverige и Watson и др.], т. 2 от диспозитива, 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?“.

IV. Анализ

37. С първия и втория преюдициален въпрос запитващата юрисдикция по същество иска да се установи дали член 15, параграф 1 от Директива 2002/58, разглеждан във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата, трябва да се тълкува в смисъл, че сред критериите, които позволяват да се прецени тежестта на намесата в основните права, каквато представлява достъпът на компетентните национални органи до лични данни, които съгласно националната правна уредба доставчиците на електронни съобщителни услуги са длъжни да запазват, са категориите засегнати данни и продължителността на периода, за който се отнася поисканият достъп.

38. Преди да отговоря на този въпрос, ще изложа две предварителни бележки, които ще ми позволят, от една страна, да отговоря на доводите, повдигнати от някои държави членки по отношение на приложното поле на Директива 2002/58, и от друга страна, на предложението на Европейската комисия в настоящото преюдициално запитване да се разгледа съвместимостта с правото на Съюза на естонската правна уредба, доколкото тя задължава доставчиците на електронни съобщителни услуги да запазят няколко категории лични данни, създадени във връзка с тези услуги.

A. Предварителни бележки

1. По приложно поле на Директива 2002/58

39. Ирландското, унгарското и полското правителство повдигат въпроси относно приложното поле на Директива 2002/58.

40. Ирландското правителство изглежда приема, че съгласно член 1, параграф 3 от Директива 2002/58 национална правна уредба относно достъпа на компетентните органи по наказателни дела до запазените данни е изключена от приложното поле на тази директива.

41. Този довод трябва да се отхвърли въз основа на практиката на Съда, изведена от решения *Tele2 Sverige* и *Watson* и др. и *Ministerio Fiscal*.

42. В това отношение следва да се отбележи, че Съдът вече е приел, че законодателните мерки по член 15, параграф 1 от Директива 2002/58 „попадат в приложното поле на посочената директива, независимо че се отнасят до дейности, които са присъщи на държавите или на държавните органи и са чужди на областите на дейност на частноправните субекти, и независимо че целите, които трябва да се преследват с такива мерки, по същество съвпадат с целите, които се преследват с дейностите по член 1, параграф 3 от Директива 2002/58“¹⁸. Всъщност според Съда „член 15, параграф 1 от посочената директива логично предполага, че посочените в нея национални мерки 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. 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“¹⁹.

43. Съдът стига до заключението, че „посоченият член 15, параграф 1, във връзка с член 3 от Директива 2002/58 трябва да се тълкува в смисъл, че в приложното поле на посочената директива попадат не само законодателна мярка, с която на доставчиците на електронни съобщителни услуги се налага задължение за запазване на данни за трафик и на данни за местонахождение, а и законодателна мярка, която се отнася до достъпа на националните органи до запазените от тези доставчици данни“²⁰.

¹⁸ Решение *Ministerio Fiscal* (т. 34 и цитираната съдебна практика).

¹⁹ Пак там.

²⁰ Решение *Ministerio Fiscal* (т. 35 и цитираната съдебна практика).

44. Всъщност според Съда „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“²¹.

45. Към тези доводи Съдът добавя, че „законодателните мерки, които налагат на доставчиците на електронни съобщителни услуги задължението да запазват лични данни или да предоставят на компетентните национални органи достъп до тези данни, по необходимост предполагат обработване на посочените данни от доставчиците [...]. Доколкото тези мерки уреждат дейностите на посочените доставчици, те следователно не могат да се приравнят на присъщи на държавите дейности, посочени в член 1, параграф 3 от Директива 2002/58“²².

46. По аналогия с постановеното от Съда в решение *Ministerio Fiscal*²³ от всички тези доводи следва да се направи заключение, че искането за достъп до запазени от доставчици на електронни съобщителни услуги лични данни, отправено в рамките на производството по наказателно разследване, попада в приложното поле на Директива 2002/58.

47. Освен това унгарското и полското правителство изтъкват довода, че правото на Съюза не урежда въпроса за допустимостта на доказателствата в наказателното производство.

48. Макар да е вярно, че при сегашното си развитие това право не урежда правилата относно допустимостта на доказателствата в наказателно производство, запитващата юрисдикция все пак ясно подчертава защо поисканото от нея тълкуване на правото на Съюза е необходимо, за да може да се произнесе по допустимостта на доказателствата. Всъщност допустимостта зависи от спазването на условията и процесуалните правила, уреждащи събирането на тези доказателства. Така при преценката на допустимостта на разглежданите в главното производство протоколи като доказателства запитващата юрисдикция трябва да разгледа предварителния въпрос доколко събирането на данни от предприятието за електронни съобщения, въз основа на които са изготвени тези протоколи, е 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. Този предварителен въпрос обаче се отнася до аспект, който, както подчертах по-горе, се урежда от правото на Съюза. Следователно по този въпрос националните правила, приложими в областта на събирането на доказателства, трябва да спазват изискванията, произтичащи от гарантираните от правото на Съюза основни права²⁴. При тези условия доводът на унгарското и полското правителство според мен е ирелевантен.

2. По запазването на данните за трафика и на данните за местонахождението

49. Макар поставените от запитващата юрисдикция въпроси да се отнасят до условията за достъп до данните, Комисията приканва Съда в рамките на настоящото преюдициално запитване да се произнесе и по проблематиката, свързана със запазването на данните. В това отношение тя по същество отбелязва, че законосъобразен достъп до запазените данни изисква националната правна уредба, налагаща на доставчиците на електронни съобщителни услуги

21 Решение *Ministerio Fiscal* (т. 36 и цитираната съдебна практика).

22 Решение *Ministerio Fiscal* (т. 37 и цитираната съдебна практика).

23 Вж. решение *Ministerio Fiscal* (т. 38 и 39).

24 Вж. по-специално по аналогия решение от 10 април 2003 г., *Steffensen* (C-276/01, EU:C:2003:228, т. 71). В това решение Съдът разглежда тази проблематика и от гледна точка на принципа на ефективност като ограничение на процесуалната автономия на държавите членки (т. 66—68 от посоченото решение).

задължението за запазване на създадените във връзка с тези услуги данни, да отговаря на изискванията по член 15, параграф 1 от Директива 2002/58, разглеждан във връзка с Хартата, или въпросните данни да са били запазени от тези доставчици по тяхна собствена инициатива, по-специално за търговски цели, в съответствие със същата директива.

50. Що се отнася до главното производство, Комисията отбелязва, че данните, до които разследващият орган е имал достъп, са били запазени от доставчиците на електронни съобщителни услуги не по тяхна собствена инициатива за търговски цели, а въз основа на задължението за запазване, предвидено в член 111¹ от Закона за електронните съобщения. Отбелязва също, че Н. К. оспорва законосъобразността на националните правила, отнасящи се както до достъпа до данните, така и до запазването им²⁵.

51. С оглед на това отбелязвам, че подобно на случая в преюдициалното запитване, по което е постановено решение *Ministerio Fiscal*²⁶, формулираните от запитващата юрисдикция въпроси в преюдициалното запитване по настоящото дело нямат за цел да се установи дали разглежданите в главното производство лични данни са запазени от доставчиците на електронни съобщителни услуги при спазване на условията по член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата. Тези въпроси се отнасят единствено до съвместимостта с тези разпоредби на условията, при които достъпът на националните разследващи органи до такива данни е разрешен съгласно естонската правна уредба. Ето защо обсъждането пред Съда се отнася почти изключително до тези условия за достъп.

52. При всички положения запитващата юрисдикция може да се позове на съдебната практика, изведена от решение *Tele2 Sverige и Watson и др.*, ако за целите на решаването на спора по главното производство счете за необходимо да се произнесе по съвместимостта на член 111¹ от Закона за електронните съобщения с правото на Съюза.

53. В това отношение само ще припомня, че според Съда „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“²⁷.

54. Запитващата юрисдикция следва да провери, ако е необходимо, дали естонската правна уредба налага на доставчиците на електронни съобщителни услуги задължение за запазване на данни, което има такъв общ и неизбирателен характер, и да направи съответните изводи за разрешаването на спора по главното производство. Ако въведеният от Република Естония режим на запазване на данните трябва да се счита за несъответстващ на правото на Съюза, тъй като е непропорционален от гледна точка на преследваната цел, достъпът до така запазените данни не би могъл да се обоснове от същата тази цел.

55. Само ако задължението за запазване е съпроводено с подходящи ограничения, по-специално по отношение на категориите засегнати данни и срока на запазване, съгласно режим, който се различава в зависимост от преследваната цел и е строго необходим за постигането на тази цел, то може да премине успешно проверката за пропорционалност.

25 В този контекст Комисията подчертава, че настоящото дело се различава от делото, по което е постановено решение *Ministerio Fiscal*.

26 Вж. решение *Ministerio Fiscal* (т. 49 и 50).

27 Решение *Tele2 Sverige и Watson и др.* (т. 112).

56. В настоящото заключение няма да се спирам повече понятието „ограничено запазване на данни“, подробно разгледано от генералния адвокат Campos Sánchez-Bordona в заключението му, представено на 15 януари 2020 година по дело *Ordre des barreaux francophones et germanophone*²⁸.

Б. По достъпа на компетентните национални органи до запазените данни

*1. Изводите от решение *Tele2 Sverige и Watson и др.**

57. Съдът възприема проблематиката, свързана с достъпа на компетентните национални органи до запазените данни, „без оглед на обхвата на задължението за запазване на данни, което може да се наложи на доставчиците на електронни съобщителни услуги“, и по-специално независимо от това дали запазването на данни е общо или избирателно²⁹. Тази констатация е във връзка с факта, че Съдът счита запазването на данните и достъпа до тях за две отделни форми на намеса в основните права, защитени от Хартата.

58. С достъпа до запазените данни „действително и строго трябва да се преследва някоя от [целите]“, изброени в член 15, параграф 1, първо изречение от Директива 2002/58. Също така трябва да има съгласуваност между тежестта на намесата и преследваната цел. Ако намесата е квалифицирана като „тежка“, тя може да бъде обосновава само в случаите на борба с тежката престъпност³⁰.

59. Подобно на това, което важи за запазването на данните, достъпът до тях от компетентните национални органи е допустим само в границите на строго необходимото³¹. Нещо повече, законодателните мерки трябва „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“³². По-конкретно, националните правни уредби трябва „да предвижда[т] също и материални и процесуални условия за достъп на компетентните национални органи до запазените данни“³³.

60. От изложеното по-горе може да се направи извод, че „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“³⁴.

61. Според Съда „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“³⁵.

28 C-520/18, EU:C:2020:7. Вж. по-специално точки 72—107 от посоченото заключение.

29 Вж. решение *Tele2 Sverige и Watson и др.* (т. 113).

30 Вж. решение *Tele2 Sverige и Watson и др.* (т. 115).

31 Вж. решение *Tele2 Sverige и Watson и др.* (т. 116).

32 Вж. решение *Tele2 Sverige и Watson и др.* (т. 117).

33 Вж. решение *Tele2 Sverige и Watson и др.* (т. 118).

34 Вж. решение *Tele2 Sverige и Watson и др.* (т. 119).

35 Пак там.

62. С други думи, националната правна уредба, с която на компетентните национални органи се предоставя достъп до запазените данни, трябва да има достатъчно ограничен обхват, за да не може подобен достъп да се отнася до голям брой лица, и дори до всички лица и всички електронни съобщителни средства, както и до всички запазени данни. Следователно Съдът изтъква критерия за връзката между засегнатите лица и преследваната цел.

63. Освен това Съдът установява условията, на които трябва да отговаря всеки достъп на компетентните национални органи до запазените данни.

64. На първо място, този достъп трябва „по принцип да се предоставя, освен в надлежно обосновани неотложни случаи, след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура“³⁶. Решението на тази юрисдикция или на тази структура трябва 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“³⁷.

65. След това, според Съда е от значение „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“³⁸.

66. Накрая, държавите членки трябва да приемат правила за сигурност и защита на запазените данни от доставчиците на електронни съобщителни услуги, за да се избегнат злоупотреби и всякакъв незаконен достъп до данните³⁹.

2. Изводите от решение *Ministerio Fiscal*

67. По това дело Съдът е бил сезиран с въпроса за съвместимостта с член 15, параграф 1 от Директива 2002/58, разглеждан във връзка с членове 7 и 8 от Хартата, на национална правна уредба, която предвижда достъп на компетентните национални органи, като съдебната полиция, до данни за самоличността на притежателите на определени СИМ карти.

68. Що се отнася обаче до целта за превенция, разследване, разкриване и преследване на престъпления, текстът на член 15, параграф 1, първо изречение от Директива 2002/58 не ограничава тази цел до борбата само с тежките престъпления, а се отнася общо до „[престъпления]“⁴⁰.

69. Съображенията на Съда изясняват факта, че що се отнася до достъпа на компетентните национални органи до данните, трябва да съществува съответствие между тежестта на намесата и тежестта на разглежданите престъпления.

³⁶ Решение *Tele2 Sverige и Watson и др.* (т. 120).

³⁷ Пак там.

³⁸ Решение *Tele2 Sverige и Watson и др.* (т. 121).

³⁹ Вж. решение *Tele2 Sverige и Watson и др.* (т. 122).

⁴⁰ Вж. решение *Ministerio Fiscal* (т. 53).

70. В този смисъл Съдът припомня, като се позовава на точка 99 от решението си *Tele2 Sverige* и *Watson* и др., че безспорно е приел, че „що се отнася до превенцията, разследването, разкриването и преследването на престъпления, само в случаите на борба с тежката престъпност може да е обоснован достъпът на публичните органи до лични данни, запазени от доставчиците на съобщителни услуги, които в своята съвкупност позволяват да се направят точни изводи относно личния живот на лицата, чиито данни са засегнати“⁴¹.

71. Съдът обаче е уточнил, че „мотивираща това тълкуване с обстоятелството, че целта, преследвана с правна уредба, която регламентира този достъп, трябва да е свързана с тежестта на намесата в съответните основни права, до която води тази дейност“⁴².

72. Всъщност „съгласно принципа на пропорционалност в областта на превенцията, разследването, разкриването и преследването на престъпления тежка намеса може да бъде обоснована само от цел за борба с престъпността, която също трябва да е квалифицирана като „тежка“⁴³.

73. Когато обаче „намесата, до която води такъв достъп, не е тежка, този достъп може да бъде обоснован от целта за превенция, разследване, разкриване и преследване общо на „[престъпления]“⁴⁴.

74. Ето защо тези съображения изискват преценка дали с оглед на обстоятелствата по случая намесата в основните права, закрепени в членове 7 и 8 от Хартата, до която би довел достъп на съдебната полиция до разглежданите в главното производство данни, трябва да се счита за „тежка“.

75. За разлика обаче от решение *Tele2 Sverige* и *Watson* и др. намесата в правата, защитени от членове 7 и 8 от Хартата, която представлява достъпът до разглежданите данни, не е квалифицирана от Съда като „тежка“⁴⁵. Всъщност искането за достъп има „единствената цел [...] да се установят притежателите на СИМ карти, които са били активирани в рамките на дванадесетдневен период с кода [за международна идентификация на мобилното крайно устройство] на откраднатия мобилен телефон“⁴⁶. Става въпрос за достъп „само до телефонните номера, които съответстват на посочените СИМ карти, както и до данните за самоличността на притежателите на тези карти, като името и фамилията им, и според случая, техният адрес. [...] тези данни обаче не се отнасят да осъществяват комуникации с откраднатия мобилен телефон, нито до неговото местонахождение“⁴⁷.

76. От това Съдът е стигнал до извода, че „данните, за които се отнася разглежданото в главното производство искане за достъп, дават възможност само да се направи връзка през определен период между СИМ картата или картите, активирани с откраднатия мобилен телефон, и самоличността на притежателите на тези СИМ карти. Без да бъдат съпоставени с данните относно осъществяването с посочените СИМ карти комуникации и данните за местонахождение, посочените данни не дават възможност да се установи нито датата, часа,

41 Вж. решение *Ministerio Fiscal* (т. 54).

42 Вж. решение *Ministerio Fiscal* (т. 55).

43 Вж. решение *Ministerio Fiscal* (т. 56).

44 Вж. решение *Ministerio Fiscal* (т. 57).

45 Вж. решение *Ministerio Fiscal* (т. 61).

46 Вж. решение *Ministerio Fiscal* (т. 59).

47 Пак там.

продължителността и адресатите на комуникациите, осъществени с въпросната/въпросните СИМ карта или карти, нито местата, на които те са извършени, или тяхната честота с определени лица през даден период. Следователно посочените данни не дават възможност да се направят точни изводи относно личния живот на лицата, чиито данни са засегнати⁴⁸.

77. След като е отхвърлил квалификацията „тежка намеса“, Съдът е имал основание да приеме, че целта за превенция, разследване, разкриване и преследване общо на престъпления, без да е необходимо тези престъпления да са квалифицирани като „тежки“, може да обоснове разглежданата намеса⁴⁹.

78. С оглед на тази съдебна практика запитващата юрисдикция поставя първия и втория преюдициален въпрос, за да прецени тежестта на намесата, каквато представлява достъпът до данните в рамките на наказателното производство, разглеждано в главното производство. По-точно, тя иска да се установи дали съответните категории данни и продължителността на периода, за който е поискан достъп до тези данни, са релевантни критерии от тази гледна точка.

3. По критериите, които позволяват да се прецени тежестта на намесата

79. Както следва от практиката на Съда, колкото повече са категориите данни, до които е поискан достъп, в толкова по-голяма степен намесата може да се квалифицира като „тежка“.

80. При това положение първият и вторият въпрос, поставени от запитващата юрисдикция, изискват Съдът да уточни дали, освен засегнатите категории данни, продължителността на периода, за който се отнася този достъп, също има значение при определянето на тежестта на намесата.

81. Според мен той има значение. Отбелязвам впрочем, че в решението Ministerio Fiscal Съдът при преценката си взема предвид и продължителността на периода, за който се отнася достъпът, а именно дванадесет дни в конкретния случай⁵⁰.

82. Именно съчетанието между естеството на въпросните данни и продължителността на периода, за който се отнася достъпът, позволява да се прецени тежестта на намесата. Тези два аспекта позволяват всъщност да се провери дали е изпълнен критерият относно тежестта на намесата, т.е. дали достъпът до разглежданите данни може да позволи на компетентните национални органи да правят точни изводи относно личния живот на лицата, чиито данни са засегнати от този достъп. За да може обаче да се направи точен портрет на дадено лице, е необходимо не само да се предостави достъп до няколко категории данни, като например данни за идентифициране, за трафика и данни за местонахождението, но също и този достъп да обхваща достатъчно дълъг период от време, за да може да се разкрият достатъчно точно основните характеристики на живота на дадено лице.

83. Подобно на броя на засегнатите категории изисквани данни, продължителността на периода, за който те се отнасят съгласно разрешението за достъп, представлява съществен елемент при преценката на тежестта на намесата в основните права на засегнатите лица. Както посочва Комисията, натрупването на няколко искания за достъп, свързани с едно и също лице, трябва също да бъде взето предвид, макар и те да са с кратки периоди.

48 Вж. решение Ministerio Fiscal (т. 60).

49 Вж. решение Ministerio Fiscal (т. 62).

50 Вж. решение Ministerio Fiscal (т. 59). Вж. в същия смисъл заключението на генералния адвокат Saugmandsgaard Øe по дело Ministerio Fiscal (C-207/16, EU:C:2018:300), в което се отбелязва, че искането на полицейските органи се отнася „за ясно определен и ограничен във времето период, а именно около 12 дни“ (т. 33 и 84).

84. Както е видно от акта за преюдициално запитване, данните, до които разследващият орган е имал достъп, са посочените в член 111¹, параграф 2 от Закона за електронните съобщения. Тези данни позволяват откриване и идентифициране на местоположението на източника и на адресата на телефонна връзка, осъществена чрез фиксиран или мобилен телефон на дадено лице, нейната дата, час, продължителност и тип, използваното крайно устройство и мястото на използване на мобилно крайно устройство. Тези данни са предавани на разследващия орган за периоди от един ден, от един месец и от почти една година.

85. Преценката на степента на намеса в основните права, до която води достъпът на компетентните национални органи до запазените лични данни, произтича от конкретно проучване на специфичните обстоятелства във всеки отделен случай. Във всеки отделен случай запитващата юрисдикция е тази, която трябва да прецени дали данните, до които е разрешен достъпът, в зависимост от естеството и продължителността на периода, за който се отнася този достъп, позволят да се направят точни изводи за личния живот на засегнатите лица.

86. Ако случаят е такъв, намесата би трябвало да се квалифицира като „тежка“ по смисъла на практиката на Съда и следователно в областта на превенцията, разследването, разкриването и преследването на престъпления може да бъде обоснована само от цел за борба с престъпността, която също трябва да е квалифицирана като „тежка“⁵¹.

4. По съгласуваността между тежестта на намесата и преследваната цел

87. От практиката на Съда следва, че намеса в основните права, квалифицирана като „тежка“, включва изискване за засилена обосновка.

88. Що се отнася до тежестта на предполагаемите престъпления, по повод на които е предоставен достъп до данните, Комисията отбелязва, че разглежданата в главното производство национална правна уредба разрешава по-конкретно достъпа за борбата с престъпленията като цяло⁵².

89. Запитващата юрисдикция следва да провери в зависимост от обстоятелствата по случая дали достъпът до данни като разглежданите в главното производство действително и точно отговаря на някоя от целите, посочени в член 15, параграф 1 от Директива 2002/58. В това отношение следва да се припомни, че тази разпоредба не ограничава целта за предотвратяване, разследване, разкриване и преследване на престъпления до борбата само с тежките престъпления, а се отнася общо до „престъпленията“⁵³.

90. Ако запитващата юрисдикция стигне до извода, че намесата трябва да се квалифицира като „тежка“, тя трябва да прецени дали разглежданото престъпление също може да се квалифицира като „тежко“ съгласно националното наказателно право.

91. В това отношение считам, че определянето на това какво може да се квалифицира като „тежко престъпление“, трябва да се остави на преценката на държавите членки.

92. Всъщност съгласно националните правни системи едно и също престъпление може да бъде наказвано повече или по-малко строго. Определението на утежняващите вината обстоятелства също са различни в отделните държави членки.

⁵¹ Решение Ministerio Fiscal (т. 56).

⁵² Член 111¹, параграф 11 от Закона за електронните съобщения и член 90¹ от Наказателно-процесуалния кодекс.

⁵³ Вж. решение Ministerio Fiscal (т. 53).

93. Както основателно посочва естонското правителство, приложимото наказание не е единственият критерий за определянето тежестта на престъпленията. Следва да се вземе предвид и естеството на престъпленията, причинената от тях вреда на обществото, по какъв начин засягат правните интереси и общите им последици за националния правен ред и ценностите на демократичното общество. Историческият, икономическият и социалният контекст, специфичен за всяка държава членка, също е от значение в това отношение. Освен това във връзка с утежняващите вината обстоятелства следва да се постави въпросът дали престъпленията са извършени например многократно, или пък по отношение на група от уязвими лица.

94. За да се прецени пропорционалността на достъпа, следва също така да се вземе предвид, че съгласно член 90¹, параграф 3 от Наказателно-процесуалния кодекс „[и]зискването на данни [...] е допустимо само ако е абсолютно необходимо за постигането на целта на наказателното производство“. Както посочва естонското правителство, критерият за абсолютна необходимост⁵⁴ задължава както разследващите, така и лицата, на които е възложено издаването на разрешението, да съобразят и преценят какви данни са необходими за успешното провеждане на наказателното производство, без които в рамките на дадено дело не би било възможно да се достигне до установяване на истината или до задържането на нарушител или на предполагаем извършител на престъплението.

95. Добавям, че както френското правителство основателно подчертава, степента на тежест на дадено престъпление, а още повече точната му правна квалификация, не винаги могат да бъдат точно определени, когато разрешението за достъп до запазените данни се издава на ранен етап от разследването, така че би могло да изглежда преждевременно на този етап разглежданото престъпление да се причисли към категорията на тежките престъпления или към категорията на престъпления като цяло. Тази несигурност, която е присъща на наказателното разследване, чиято цел сама по себе си е да спомогне за установяване на истината, трябва да бъде взета предвид от запитващата юрисдикция при преценката ѝ относно пропорционалния характер на достъпа.

96. При това положение несигурността, която може да съществува в началото на наказателното разследване по тези въпроси, не може да премахне изискването всяко искане за достъп да бъде мотивирано от необходимостта да се търсят доказателства за конкретно деликтно или престъпно поведение, въз основа на подозрение, подкрепяно с обективни доказателства. В този смисъл искането за достъп не може да има за цел да разгледа през определен период всички факти и действия на дадено лице с оглед на търсенето на евентуални престъпления. Освен това, ако в хода на разследването се разкрият нови факти, достъпът до данните за доказване на последните трябва да бъде предмет на ново разрешение за достъп.

97. С оглед на изложените по-горе съображения предлагам на Съда да постанови, 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 сред критериите, които позволяват да се прецени тежестта на намесата в основните права, каквато представлява достъпът на компетентните национални органи до лични данни, които съгласно национална правна уредба доставчиците на електронни съобщителни услуги са длъжни да запазват, са категориите засегнати данни и продължителността на периода, за който е поискан този достъп. Запитващата юрисдикция следва да прецени в зависимост от тежестта на намесата дали посоченият достъп е строго необходим за постигане на целта да се гарантира предотвратяването, разследването, разкриването и преследването на престъпления.

⁵⁴ Определян също като „принцип на ultima ratio“.

В. Предварителен контрол от юрисдикция или независима административна структура

98. За да се гарантира, че достъпът на компетентните национални органи до запазените данни е ограничен до строго необходимото за постигане на преследваната цел, Съдът е приел, че е от съществено значение този достъп „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“⁵⁵.

99. С третия си преюдициален въпрос запитващата юрисдикция иска от Съда да уточни критериите, на които трябва да отговаря дадена административна структура, за да може да се счита за „независима“ по смисъла на решение *Tele2 Sverige и Watson* и др. По-конкретно, запитващата юрисдикция иска да се установи дали прокуратурата може да се счита за независима административна структура, като се има предвид обстоятелството, че ръководи производството по разследване и повдига и поддържа обвинението в съдебното производство.

100. За да се отговори на този въпрос, според мен е полезно да се вземат предвид две направления в практиката на Съда, а именно, от една страна, съдебната практика относно независимостта на националните надзорни органи за защита на личните данни, и от друга страна, съдебната практика относно независимостта на издаващия съдебен орган в рамките на европейската заповед за арест.

101. Според Съда независимостта представлява съществена характеристика, потвърдена по-специално в член 8, параграф 3 от Хартата, на органите, на които е възложено да контролират спазването на правилата на Съюза относно защитата на физическите лица при обработването на лични данни, за да се гарантира ефективността и надеждността на този надзор и да се засили защитата на засегнатите от решенията на тези органи лица⁵⁶.

102. Съдът вече е постановил по отношение на член 28, параграф 1, втора алинея от Директива 95/46, че „надзорните органи, компетентни да наблюдават обработването на лични данни, трябва да се ползват с независимост, която да им дава възможност да изпълняват функциите си без външно влияние. Тази независимост изключва по-специално всяко предписание и всяко друго външно влияние под каквато и да е форма, независимо дали последното е пряко или косвено, които биха могли да насочат решенията им и по този начин биха могли да застрашат изпълнението на задачата на посочените органи, състояща се в постигането на справедлив баланс между защитата на правото на личен живот и свободното движение на личните данни“⁵⁷.

103. Освен това Съдът е поставил акцент върху изискването, предвид ролята им на пазители на правото на личен живот, по отношение на тези надзорни органи „да бъде изключено всякакво подозрение за пристрастност“⁵⁸.

104. Тъй като третият поставен от запитващата юрисдикция въпрос се отнася до прокуратурата, следва да се вземат предвид и критериите, формулирани от Съда в практиката му относно независимостта на издаващия съдебен орган в рамките на европейската заповед за арест. Така според Съда контролът при приемането на заповед за арест „трябва да се упражнява обективно,

55 Решение *Tele2 Sverige и Watson* и др. (т. 120 и цитираната съдебна практика), курсивът е мой. Вж. в същия смисъл Становище 1/15 (Споразумение PNR ЕС—Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 202 и 208).

56 Вж. по-специално решение от 6 октомври 2015 г., *Schrems* (C-362/14, EU:C:2015:650, т. 40 и 41 и цитираната съдебна практика). Вж. също Становище 1/15 (Споразумение PNR ЕС—Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 229).

57 Решение от 8 април 2014 г., Комисия/Унгария (C-288/12, EU:C:2014:237, т. 51 и цитираната съдебна практика).

58 Решение от 8 април 2014 г., Комисия/Унгария (C-288/12, EU:C:2014:237, т. 53 и цитираната съдебна практика).

като се отчитат всички уличаващи и оневиняващи доказателства, и при условията на независимост, което предполага наличието на устройствени и организационни правила, които да могат да изключат всякакъв риск от това приемането на решение за издаване на такава заповед за арест да се подчинява на външни указания, по-специално от страна на изпълнителната власт⁵⁹. Важно е обаче да се има предвид, че конкретната преценка на Съда, във всеки отделен случай, по въпроса дали прокуратурата изпълнява тези критерии⁶⁰, се прави в конкретния контекст на издаване на европейска заповед за арест и поради това не може да бъде автоматично пренасяна към други области като тази относно защитата на личните данни.

105. С оглед на това уточнение двете направления на практиката на Съда се припокриват, като във всяка от съответните области се подчертава, че националният орган, компетентен да проверява спазването на правните норми на Съюза, трябва да е независим, което обхваща две изисквания⁶¹. От една страна, този орган не трябва да бъде подчинен на външни указания или натиск, които могат да повлияят на решенията му. От друга страна, по силата на своя статут и на поверените му задачи посоченият орган трябва да отговаря на изискването за обективност при упражнявания от него контрол, т.е. трябва да предоставя гаранции за безпристрастност. По-специално, преценката от административната структура на пропорционалния характер на достъпа до запазените данни изисква тя да е в състояние да постигне справедлив баланс между интересите, свързани с ефикасността на разследването в борбата с престъпността, и интересите, свързани със защитата на личните данни на засегнатите от достъпа лица. Предвид този последен аспект изискването за безпристрастност следователно е присъщо на понятието „независима административна структура“, подчертано от Съда в решение *Tele2 Sverige* и *Watson* и др.

106. Следва да се провери дали предвид различните функции, които са ѝ възложени от естонската правна уредба, прокуратурата изпълнява този критерий за независимост в нейните две измерения, когато трябва да осъществява контрол дали достъпът до данните е строго необходим. В този смисъл понятието „независимост“, с което трябва да се характеризира натоварената с такъв контрол административна структура, има функционално измерение в смисъл, че с оглед на конкретната цел на този контрол следва да се прецени дали тази структура може да действа без външна намеса или натиск, които могат да повлияят на решенията ѝ, както и при запазването на обективност и строгото прилагане на правната норма. Накратко, понятието „независима административна структура“ по смисъла на решение *Tele2 Sverige* и *Watson* и др. следва да гарантира обективността, надеждността и ефективността на този контрол.

107. Това налага да се провери дали естонската правна уредба, която регламентира статута и функциите на прокуратурата, може да породи оправдани съмнения в съзнанието на засегнатите лица относно неподатливостта на прокурорите на външни фактори и неутралността им по отношение на противопоставящите се интереси, когато трябва да осигуряват предварителен контрол за пропорционалност на достъпа до данните.

⁵⁹ Вж. решение от 9 октомври 2019 г., NJ (Прокуратура на Виена) (C-489/19 PPU, EU:C:2019:849, т. 38 и цитираната съдебна практика).

⁶⁰ Вж. последно решение от 12 декември 2019 г., JR и YC (Procureurs de Lyon et de Tours) (C-566/19 PPU и C-626/19 PPU, EU:C:2019:1077), в което Съдът по-специално приема, че представените обстоятелства са достатъчни, за да докажат, че „във Франция магистратите прокурори разполагат с правомощието да преценяват самостоятелно, по-специално по отношение на изпълнителната власт, необходимостта и пропорционалния характер на издаването на европейска заповед за арест и упражняват това правомощие по обективен начин, като вземат предвид всички уличаващи и оневиняващи доказателства (т. 55 от решението).

⁶¹ По двата аспекта на изискването за независимост вж. по аналогия, по отношение на националните юрисдикции, които трябва да се произнасят по въпроси, свързани с тълкуването и прилагането на правото на Съюза, решение от 5 ноември 2019 г., Комисия/Полша (Независимост на общите съдилища) (C-192/18, EU:C:2019:924, т. 108—110 и цитираната съдебна практика).

108. Прокуратурата изпълнява основна роля при провеждането на наказателното производство, тъй като ръководи производството по разследване и разполага с компетентност да провежда преследване срещу лице, заподозряно в извършването на престъпление, с цел то да бъде изправено пред съд. В това отношение трябва да се счита за орган, участващ в правораздаването на съответната държава членка⁶².

109. Както Съдът е посочил по отношение на Procura della Repubblica (прокурор на Републиката, Италия) и съгласно формулировка, която според мен може да бъде приложена в рамките на настоящото дело, прокурорът има „функцията не да постанови при пълна независимост решение по делото, а евентуално да отнесе делото пред компетентния съд в качеството си на страна в наказателния процес, легитимирана да внесе и поддържа обвинението“⁶³.

110. Макар по този начин прокуратурата да показва, що се отнася до статута, организацията и функциите си, особени характеристики, които я разграничават от юрисдикция и са основание тя да бъде определена като „орган, участващ в наказателното правораздаване в държавите членки“, това не променя обстоятелството, че от функционална гледна точка, когато националното право предвижда, че прокуратурата е органът, упражняващ предварителния контрол за пропорционалност на достъпа, който се изисква от решение Tele2 Sverige и Watson и др., тя трябва в това отношение да демонстрира степен на независимост, аналогична на тази на юрисдикция. Всъщност упражняването на тази функция от страна на административна структура, а не от юрисдикция, не трябва да засяга обективността, надеждността и ефективността на този контрол.

111. В това отношение следва да се припомни, че съгласно член 90¹, параграф 2 от Наказателно-процесуалния кодекс разследващият орган може, с разрешението на прокурора в производството по разследване или с разрешението на съда в съдебното производство пред него, да изиска от предприятие за електронни съобщения предаването на данните, изброени в член 111¹, параграфи 2 и 3 от Закона за електронните съобщения.

112. Освен това съгласно естонската правна уредба в рамките на наказателно производство прокуратурата ръководи производството по разследване, чиято цел е събирането на доказателства и изпълнение на другите условия за откриване на съдебното производство. Освен това в производството по разследване разследващият орган и прокуратурата установяват фактите, които уличават или оневиняват заподозряното лице или обвиняемия. Прокуратурата повдига обвинение на съответното лице, ако счита, че са събрани всички необходими доказателства и че е налице основание за това, и именно тя представлява държавното обвинение в съдебния процес.

113. Запитващата юрисдикция отбелязва също, че въпреки, че в рамките на наказателното производство е необходимо прокуратурата да поиска разрешение от съдията по разследването за мерките, които в най-голяма степен водят до намеса в основните права (например за повечето от мерките за наблюдение и за задържането под стража), прокуратурата също има правомощията да приема процесуални актове, водещи до интензивна намеса в няколко основни права⁶⁴.

114. Съмненията, изразени от запитващата юрисдикция по въпроса дали прокуратурата може да се квалифицира като „независима административна структура“ по смисъла на решение Tele2 Sverige и Watson и др., се дължат главно на факта, че в резултат на производството по разследване прокуратурата повдига обвинение на съответното лице, ако счита, че са били

⁶² Вж. по-специално решение от 27 май 2019 г., PF (Главен прокурор на Литва) (C-509/18, EU:C:2019:457, т. 39 и 40).

⁶³ Решение от 12 декември 1996 г., X (C-74/95 и C-129/95, EU:C:1996:491, т. 19).

⁶⁴ Например прокуратурата дава разрешение за скрито наблюдение на дадено лице, предмет или обект и в много случаи — за претърсване.

събрани всички необходими доказателства по наказателното дело и е налице основание за това. В този случай прокуратурата повдига и поддържа обвинението в съдебния процес и следователно е също страна в производството. Поради това запитващата юрисдикция изразява съмнения дали прокуратурата може да се счита за „независима административна структура“ по смисъла на решение *Tele2 Sverige и Watson* и др.

115. Така изразените от запитващата юрисдикция съмнения се отнасят по-специално до безпристрастността на прокуратурата при контрола за пропорционалност на достъпа до данните от разследващите органи, които тя следва да упражни, преди да разреши такъв достъп.

116. Преди да пристъпя към разглеждането на темата за безпристрастността, бих искал да отбележа, че член 1, параграф 1¹ от Закона за прокуратурата предвижда, че прокуратурата „е независима при изпълнението на възложените ѝ от закона функции“. Освен това съгласно член 2, параграф 2 от този закон „[п]рокурорът е независим при изпълнението на възложените му задачи и действия единствено съгласно закона и по собствено убеждение“⁶⁵.

117. В това отношение естонското правителство посочва, че макар прокуратурата да е орган, който е част от Министерството на правосъдието, естонската правна уредба не позволява на последното каквато и да било възможност да извършва преценка по конкретно производство или да предприема действия в рамките на всящо наказателно производство. Това правителство уточнява, че нарушаването на независимостта на прокуратурата съставлява наказуемо деяние.

118. Следователно, макар да няма основание за съмнение в независимостта на прокуратурата относно функциите, които са ѝ възложени съгласно естонската правна уредба, все пак ми се струва, че тази уредба може да породи основателни съмнения относно способността на прокуратурата да упражнява неутрален и обективен предварителен контрол върху пропорционалния характер на достъпа до данните, когато по дадено дело може да се наложи да изпълнява едновременно с този контрол и функциите да ръководи наказателното разследване, да взема решение за наказателно преследване и да повдига и поддържа обвинението в съдебния процес.

119. Вярно е, че редица елементи на естонската правна уредба, гарантират, че изпълнявайки възложените ѝ функции, прокуратурата действа при спазване на изискването за безпристрастност.

120. Така съгласно член 211, параграф 2 от Наказателно-процесуалния кодекс прокуратурата е длъжна да установява фактите, които уличават или оневиняват заподозряното лице или обвиняемия.

121. Освен това, както следва от член 1, параграф 1 от Закона за прокуратурата, тя е длъжна да осигури законосъобразността на производството по наказателно разследване, което е натоварена да ръководи. Освен това съгласно член 1, параграф 1¹ и член 2, параграф 2 от същия закон прокуратурата трябва да изпълнява възложените ѝ функции при спазване на законите. Това предполага, че когато ръководи производството по наказателно разследване, прокуратурата трябва да има за цел не само да осигури ефикасността на това производство, но и да гарантира, че то няма да бъде проведено при непропорционално засягане на правото на личен живот на засегнатите лица. Всъщност може да се приеме, че разрешението за достъп до запазените данни е неразделна част от по-общата задача на прокуратурата, състояща се в надзор над законосъобразността на използваните от разследващите органи средства, и по-специално над пропорционалността на действията по разследване с оглед на естеството и тежестта на деянията.

⁶⁵ Вж. също в този смисъл член 30, параграф 2 от Наказателно-процесуалния кодекс.

122. Ето защо би могло да се изтъкне доводът, че именно защото ръководи производството по разследване, прокурорът е в състояние да прецени също дали предвид особеностите на всяко дело достъпът до данните, запазени от операторите на електронни съобщения, е строго необходим поради липса на алтернативни доказателства за започването на разследване на предполагаемо престъпление.

123. Това обаче не променя факта, че от гледна точка на лицата, за които се отнася искането за достъп до данните, обстоятелството, че административната структура, която следва да провери дали този достъп е строго необходим в рамките на разследването, е едновременно тази, която може да проведе преследване срещу тях, а впоследствие и да повдигне и поддържа обвинението в евентуален последващ съдебен процес, според мен би могло да отслаби гаранциите за безпристрастност, предвидени от естонската правна уредба. От тази гледна точка може да е налице потенциален конфликт между тези функции на прокуратурата, от една страна, и изискването за неутралност и обективност на предварителния контрол за пропорционалност на достъпа до данните, от друга страна.

124. Всъщност в рамките на възложените ѝ функции прокуратурата е длъжна да събира доказателствата, да преценява тяхната относимост и да прави изводи относно вината на съответното лице. Задача на този държавен орган е да представи и обоснове преписката на обвинението в рамките на държавното обвинение, което е натоварен да представлява в съдебния процес, като следователно е страна в производството. Предвид тези функции прокуратурата се подчинява на изискванията за доказване, което в очите на лицата, заподозрени в извършване на престъпление, може да изглежда като несъвместимо със способността на същия орган да осъществява неутрално и обективно предварителен контрол за пропорционалния характер на достъпа до данните.

125. Както отбелязва Комисията, рискът би могъл се състои в това, че поради натрупването на функции, които са ѝ възложени, прокуратурата може да бъде възприемана от засегнатите лица като имаща интерес да предоставя в голяма степен достъп до техните данни, независимо дали те са уличаващи или оневиняващи. Освен това заподозрените в извършването на престъпление лица могат да имат основателни съмнения относно безпристрастността на прокуратурата, когато разрешава достъп до техните данни, при положение че в качеството си на обвинител тя може да предяви обвинение срещу тях в последващ процес. Считаю обаче, че изискването за безпристрастност на административната структура, на която е възложено извършването на предварителен контрол, съгласно решение *Tele2 Sverige* и *Watson* и др. предполага известно разграничаване и неутралитет по отношение на интересите, които могат да се противопоставят в рамките на производството по разследване, а именно, от една страна, ефикасността на разследването, и от друга страна, защитата на личните данни на засегнатите лица. Според Комисията положението би могло да е различно, ако вътрешната административна организация на прокуратурата беше такава, че прокурорът, който трябва да се произнесе по искането за достъп, не участва по никакъв начин в производството по разследване и в следващите етапи на производството, включително в повдигането и поддържането на обвинението.

126. Тъй като, както беше потвърдено в съдебното заседание, прокуратурата в Република Естония е организирана по йерархичен модел, не съм сигурен, че това предложение на Комисията би могло да отстрани неудобствата, които произтичат от натрупването на функциите, които естонската правна уредба възлага на прокуратурата. Във всеки случай това не променя важността на идеята, на която се основава това предложение, а именно че предварителната проверка на пропорционалния характер на достъпа до данните би трябвало да се осъществява от административна структура, която, от една страна, не участва пряко в провеждането на въпросното наказателно разследване, и от друга страна, заема неутрално положение по отношение на страните в наказателното производство. Подобна структура, която е отделена от интересите, свързани с разследването и с повдигането и поддържането на обвинението в разглежданото производство, не би могла да бъде упреknата, че отдава

предимство на интересите на разследването в ущърб на интересите, свързани със защитата на данните на засегнатите лица. При това положение посочената структура би била в състояние при пълна безпристрастност да приеме решение за ограничаване на достъпа до запазените данни, което е строго необходимо за постигането на преследваната цел, съгласно изискванията на член 15, параграф 1 от Директива 2002/58, както се тълкува от Съда в решения от 8 април 2014 г., *Digital Rights Ireland* и др.⁶⁶, и *Tele2 Sverige* и *Watson* и др. В същото време съзнавам, че установяването на външна преценка на интересите, свързани с разглежданото производство, не трябва да се извършва за сметка на намаляване на ефективността на разследването, преследването и наказването на престъпленията.

127. За да се спази процесуалната автономия на държавите членки, Съдът не би трябвало да се намесва допълнително в общата организация на правораздаването в държавите членки, нито във вътрешната организация на прокуратурите. Държавите членки са длъжни да въведат средства, с които да се гарантира, че предварителният контрол върху достъпа до запазените данни, осигурява постигане на справедлив баланс между интересите, свързани с ефикасността на наказателното разследване и правото на защита на личните данни на засегнатите от достъпа лица.

128. Ще завърша с уточнението, че според мен липсата на предварителен контрол, осъществяван от „независима“ административна структура по смисъла на решение *Tele2 Sverige* и *Watson* и др., не може да се компенсира с наличието на съдебен контрол, който може да се извърши, след като достъпът е бил разрешен⁶⁷. В противен случай изискването контролът да е предварителен, би загубило своя смисъл, който се състои в това да се предотврати разрешаването на достъп до запазените данни, който би бил непропорционален с оглед на целта за разследване, преследване и наказване на престъпленията.

129. С оглед на изложените по-горе съображения предлагам на Съда да отговори на третия преюдициален въпрос, 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 изискването достъпът на компетентните национални органи до запазените данни да подлежи на предварителен контрол от юрисдикция или от независима административна структура, не е изпълнено, когато национална правна уредба предвижда, че такъв контрол се извършва от прокуратурата, чиято задача е да ръководи производството по разследване, като едновременно с това може да представлява държавното обвинение в съдебното производство.

V. Заключение

130. С оглед на изложеното по-горе предлагам Съдът да отговори на поставените от *Riigikohus* (Върховен съд, Естония) въпроси, както следва:

„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 г., 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 сред критериите, които позволяват да се прецени тежестта на намесата в основните права, каквато представлява достъпът на

⁶⁶ C-293/12 и C-594/12, EU:C:2014:238.

⁶⁷ Според обстоятелствата, които бяха изложени пред Съда в хода на съдебното заседание, в естонското право този съдебен контрол може да бъде упражнен в края на производството по разследване, когато заподозряното лице, след като бъде уведомено за преписката, реши да оспори акт по това производство, а също и по време на съдебния процес.

компетентните национални органи до лични данни, които съгласно национална правна уредба доставчиците на електронни съобщителни услуги са длъжни да запазват, са категориите засегнати данни и продължителността на периода, за който е поискан този достъп. Запитващата юрисдикция следва да прецени в зависимост от тежестта на намесата дали посоченият достъп е строго необходим за постигане на целта да се гарантира предотвратяването, разследването, разкриването и преследването на престъпления.

- 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 изискването достъпът на компетентните национални органи до запазените данни да подлежи на предварителен контрол от юрисдикция или от независима административна структура, не е изпълнено, когато национална правна уредба предвижда, че такъв контрол се извършва от прокуратурата, чиято задача е да ръководи производството по разследване, като едновременно с това може да представлява държавното обвинение в съдебното производство“.