



## Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ  
Н. SAUGMANDSGAARD ØE  
представено на 3 май 2018 година<sup>1</sup>

Дело C-207/16

Ministerio Fiscal

(Преюдициално запитване, отправено от Audiencia Provincial de Tarragona (съд на провинция Тарагона, Испания)

„Преюдициално запитване — Електронни комуникации — Обработка на лични данни — Право на личен живот и на защита на тези данни — Директива 2002/58/ЕО — Член 1 и член 15, параграф 1 — Харта на основните права на Европейския съюз — Членове 7 и 8 и член 52, параграф 1 — Данни, събирани при предоставянето на електронни съобщителни услуги — Искане за достъп от полицейски орган за целите на наказателно разследване — Принцип на пропорционалност — Понятие „тежко престъпление“, което може да обоснове намеса в основните права — Критерии за тежест — Предвидено наказание — Минимален праг“

### I. Въведение

1. Настоящото преюдициално запитване по същество се отнася до тълкуването на понятието „тежки престъпления“<sup>2</sup> по смисъла на практиката на Съда, установена с решение Digital Rights Ireland и др.<sup>3</sup> (наричано по-нататък „решение Digital Rights“), и по-късно с решение Tele2 Sverige и Watson и др.<sup>4</sup> (наричано по-нататък „решение Tele2“), в които това понятие се използва като критерий за преценка на законосъобразността и пропорционалността на намесата в правата по членове 7 и 8 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“), а именно съответно правото на зачитане на личния и семейния живот, както и правото на защита на личните данни.

<sup>1</sup> Език на оригиналния текст: френски.

<sup>2</sup> В случая изразът трябва да се разбира в смисъла единствено на тежки престъпления съгласно наказателния закон.

<sup>3</sup> Решение от 8 април 2014 г. (C-293/12 и C-594/12, EU:C:2014:238), с което Съдът обявява за невалидна Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, 2006 г., стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51), поради това че „като е приел Директива 2006/24, законодателят на Съюза е надхвърлил границите, които налага зачитането на принципа на пропорционалност с оглед на членове 7 и 8 и на член 52, параграф 1 от Хартата“ (т. 69).

<sup>4</sup> Решение от 21 декември 2016 г. (C-203/15 и C-698/15, EU:C:2016:970), в което Съдът постановява, че правото на Съюза, *от една страна*, „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“, а *от друга страна*, „не допуска национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентни национални органи до запазените данни, като в рамките на борбата с престъпността не ограничава този достъп само до целите за борба с тежката престъпност, не го подчинява на предварителен контрол от юрисдикция или от независима административна структура и не изисква разглежданите данни да се запазват на територията на Съюза“ (т. 1 и 2 от диспозитива).

2. Настоящото преюдициално запитване е направено в контекста на производство по жалба против съдебно решение, с което на полицейски органи е отказана възможността да им бъдат предадени някои данни за гражданското състояние, притежавани от мобилни телефонни оператори, с цел идентифициране на лица за нуждите на наказателно разследване. Обжалваното решение е мотивирано по-специално със съображението, че деянията, предмет на това разследване, не съставляват тежко престъпление, в разрез с изискванията на приложимата испанска правна уредба.

3. По същество запитващата юрисдикция иска от Съда да установи начина за определяне на степента на тежест на престъпленията, над която, с оглед на посочената по-горе съдебна практика, може да се обоснове накърняване на основните права, предмет на закрила от членове 7 и 8 от Хартата, при достъпа на компетентните национални органи до лични данни, запазени от доставчици на електронни съобщителни услуги.

4. След като установя, че Съдът е компетентен да се произнесе по това преюдициално запитване и същото е допустимо, смятам да докажа, че в съответствие с посочената съдебна практика достъпът до лични данни при обстоятелства като разглежданите в случая води до намеса в споменатите основни права, неотговаряща на хипотезите, при които единствено борбата срещу тежките престъпления може да обоснове накърняването на тези права.

5. Тъй като предвид особения предмет на спора в главното производство според мен няма да е необходимо Съдът да отговори на преюдициалните въпроси съгласно първоначалната им формулировка, насоки относно критериите, които евентуално биха позволили да се дефинира понятието „тежки престъпления“ по смисъла на споменатата съдебна практика, и по-специално с оглед на критерия за предвиденото наказание, ще дам само при условията на евентуалност.

## II. Правна уредба

### A. Правото на Съюза

6. В преамбюла на 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)<sup>5</sup>, изменена с Директива 2009/136/ЕО<sup>6</sup> (наричана по-нататък „Директива 2002/58“), се посочва:

„(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 [нея].

[...]

(11) Както Директива 95/46/ЕО<sup>7</sup>, настоящата директива не се отнася до въпросите за защита на основните права и свободи свързани с дейности, които не се управляват от законодателството на Общността. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 15, параграф 1 от настоящата директива, необходими за

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

6 Директива на Европейския парламент и на Съвета от 25 ноември 2009 г. (ОВ L 337, 2009 г., стр. 11).

7 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 L 281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10).

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 [наричана по-нататък „ЕКПЧ“], съгласно тълкуването на решенията на Европейския съд за човешките права [наричан по-нататък „ЕСПЧ“]. 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 [ЕКПЧ] [8].

7. Съгласно член 1 („Обхват и цел“) от Директива 2002/58:

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

[...]

3. Настоящата директива не се прилага за дейности, които попадат извън обхвата на Договора за създаване на Европейската общност, като тези обхванати от дялове V и VI от Договора за Европейския съюз, и във всички случаи за дейности, отнасящи се до обществената сигурност, отбраната, сигурността на държавата (включително икономическото благосъстояние на държавата, когато дейностите се отнасят до проблемите за сигурността на държавата) и дейностите на държавата в областта на наказателното право“.

8. Член 2 („Дефиниции“) от същата директива предвижда:

„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) [9].

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 абониран 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;

8 И по-специално в съответствие с член 8 от ЕКПЧ, съгласно който:

„1. Всеки има право на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговата кореспонденция.

2. Намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите“.

9 ОВ L 108, 2002 г., стр. 33; Специално издание на български език, 2007 г., глава 13, том 35, стр. 195.

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;

[...]“.

9. Член 15 („Приложение на някои разпоредби от Директива [95/46]“) от Директива 2002/58 предвижда в параграф 1, 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, параграфи 1, 2, 3, и 4 и член 9 от настоящата директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива [95/46]. В тази връзка, държавите членки могат, *inter alia*, да одобрят законодателни мерки, предвиждащи съхраняването на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф. Всички мерки, упоменати в настоящия параграф, трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф 1 и 2 от Договора за Европейския съюз“.

## **Б. Испанското право**

### *1. Закон 25/2007*

10. Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Закон 25/2007 за запазването на данни относно електронните съобщения и обществените съобщителни мрежи) от 18 октомври 2007 г.<sup>10</sup> (наричан по-нататък „Закон 25/2007“) транспонира в испанското право Директива 2006/24<sup>11</sup>, обявена за невалидна от Съда с решение Digital Rights.

11. Съгласно член 1 от Закон 25/2007 в редакцията, приложима към спорните факти по главното производство:

„1. Този закон урежда задължението на операторите да запазват данните, създадени или обработени при предоставянето на електронни съобщителни услуги или на обществени съобщителни мрежи, както и задължението за предаване на тези данни на оправомощените лица, когато са поискани, при наличие на съответното разрешение от съда за целите на разкриването, разследването и преследването на тежки престъпления по смисъла на Наказателния кодекс или на специалните наказателни закони.

2. Този закон се прилага за данните за трафик и данните за местоположението, както на физическите, така и на юридическите лица, и за съпътстващите ги данни, необходими за идентифицирането на абоната или регистрирания потребител.

[...]“.

10 ВOE, бр. 251 от 19 октомври 2007 г., стр. 42517.

11 Това следва както от преамбюла на посочения закон, така и от основните разпоредби, чийто текст е сходен с този на съответните разпоредби от Директива 2006/24.

12. Член 3 от този закон изброява данните, които операторите са длъжни да запазват. Съгласно член 3, параграф 1, буква а), точка 1, подточка ii) от този член това по-специално са данни, необходими за проследяването и идентифицирането на източника на съобщението, например що се отнася до мобилните телефонни съобщения и името и адреса на абоната или на регистрирания потребител.

## 2. Наказателният кодекс

13. Съгласно член 13, параграф 1 от испанския наказателен кодекс в редакцията, приложима към фактите по спора в главното производство, „[т]ежки са престъпленията, за които законът предвижда тежко наказание“.

14. Член 33 от посочения кодекс има следния текст:

„1. В зависимост от естеството и продължителността им, наказанията са тежки, средно тежки и леки.

2. Тежки наказания са:

- а) доживотен затвор с право на замяна;
- б) лишаване от свобода за повече от пет години;

[...]“.

## 3. Наказателно-процесуален кодекс

15. Испанският наказателно-процесуален кодекс е изменен с Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Устройствен закон 13/2015 за изменение на Наказателно-процесуалния кодекс с цел увеличаване на процесуалните гаранции и уреждане на мерките за разследване с използване на новите технологии) от 5 октомври 2015 г.<sup>12</sup> (наричан по-нататък „Устройствен закон 13/2015“).

16. С този закон, влязъл в сила на 6 декември 2015 г., в Наказателно-процесуалния кодекс се урежда достъпът до данните за телефонни и телематични съобщения, запазени от доставчиците на електронни съобщителни услуги.

17. Съгласно член 579, параграф 1 от Наказателно-процесуалния кодекс, в редакцията след измененията с посочения закон, „[с]ъдът може да разреши прихващането на частната пощенска и телеграфна кореспонденция, включително по факс, чрез услугата Burofax, както и международните пощенски записи, които заподозреният изпраща или получава, а също и тяхното отваряне и проучване, ако са налице улики, даващи основание да се счита, че това ще даде възможност за разкриването или проверката на факт или обстоятелство, от значение по делото, ако се разследва някое от следните престъпления:

- 1) умишлено престъпление, което се наказва с лишаване от свобода с максимален срок най-малко три години;
- 2) престъпление, извършено в рамките на престъпна група или организация;

<sup>12</sup> BOE, бр. 239 от 6 октомври 2015 г., стр. 90192.

3) престъплението „тероризъм“.

18. Член 588ter j („Данни от автоматизираните архиви на доставчиците на услуги“) от същия кодекс предвижда:

„1. Електронните данни, които се съхраняват от доставчиците на услуги или от лицата, които осъществяват предаването на съобщения, в съответствие със законодателството относно съхраняването на данни за електронните съобщения или по тяхна инициатива поради търговски или други съображения, и които са свързани с процесите в областта на съобщенията, могат да бъдат приобщени към материалите по делото само с разрешение от съда.

2. Когато запознаването с тези данни е от съществено значение за разследването, от компетентния съд трябва да се поиска разрешение за получаване на информация от автоматизираните архиви на доставчиците на услуги, включително за кръстосано или интелегентно търсене на данни, като следва да се уточнят естеството на исканите данни и причините, обосноваващи тяхното предаване“.

### **III. Спорът в главното производство, преюдициалните въпроси и производството пред Съда**

19. Г-н Hernández Sierra е подал жалба в полицията за извършен на 16 февруари 2015 г. грабеж на неговия портфейл и мобилен телефон, по време на който е претърпял тежки наранявания.

20. На 27 февруари 2015 г. съдебната полиция отправя до Juzgado de Instrucción nº 3 de Tarragona (съдия-следовател № 3, Тарагона, Испания, наричан по-нататък „съдия-следователят“) искане да се разпорежи на различните телефонни оператори да предадат, от една страна, информация за телефонните номера, активирани между 16 и 27 февруари 2015 г. с кода IMEI<sup>13</sup> на откраднатия мобилен телефон, и от друга, личните данни на притежателите или ползвателите на всички телефонни номера, свързани с активирания с посочения код IMEI СИМ карти<sup>14</sup>.

21. С определение от 5 май 2015 г. съдия-следователят отхвърля искането, тъй като исканата мярка била неособено пригодна за разкриване на извършителите на престъплението, а и при всички положения Закон 25/2007 ограничавал предаването на запазени от телефонните оператори данни до тежките престъпления — т.е. съгласно испанския наказателен кодекс<sup>15</sup> онези, които се наказват с лишаване от свобода над пет години — а разглежданите деяния не били такива.

22. Ministerio Fiscal (прокуратурата на Испания), единствената страна в производството, обжалва това определение пред Audiencia Provincial de Tarragona (съд на провинция Тарагона, Испания), като посочва, че предаването на разглежданите данни е трябвало да бъде разрешено предвид естеството на разследваните обстоятелства и на решение на Tribunal Supremo (Върховен съд, Испания) по сходно дело<sup>16</sup>.

13 IMEI е съкращение на израза „International Mobile Equipment Identity“ (международен идентификатор на мобилно устройство). IMEI е уникален код за идентификация, състоящ се от около 15 цифри, обикновено изписан от вътрешната страна на отделението за батерията на мобилния телефонен апарат, както и върху кутията и фактурата, с които същият е закупен.

14 Испанското правителство посочва, че искането се отнася до четири телефонни компании, и уточнява, че ако IMEI е използван в телефонната мрежа на някоя от тези компании, а мрежата се управлява от виртуален мобилен оператор, посочените по-горе данни, събрани от последния, е трябвало също да бъдат предоставени.

15 Вж. разпоредбите, цитирани в точки 13 и 14 от настоящото заключение.

16 Вж. решение на Sala de lo Penal (наказателен състав) от 26 юли 2010 г. (№ 745/2010, ES:TS:2010:4200), достъпно на интернет адрес: <http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&database=match=TS&reference=5697924&links=&optimize=20100812&publicinterface=true>.

23. С определение от 9 февруари 2016 г. посоченият апелативен съд разпорежда като обезпечителна мярка, адресирана до телефонните оператори, удължаване на срока на запазване на данните, предмет на спорното искане.

24. В акта за преюдициално запитване посочената юрисдикция изтъква, че след приемане на обжалваното решение, с Устройствен закон 13/2015<sup>17</sup> испанският законодател въвежда два алтернативни критерия за определяне на степента на тежест на престъплението. Според нея първият е материалноправен, свързан с действия или бездействия, отговарящи на определени наказателноправни квалификации, с конкретна и тежка наказателна противоправност, които са особено опасни за индивидуалните и колективните правни интереси<sup>18</sup>. Вторият е формално-нормативен критерий, основан изцяло на наказанието, предвидено за съответното престъпление. Предвиденият с него праг от три години лишаване от свобода може да обхване огромното мнозинство от наказателни квалификации. Запитващата юрисдикция отбелязва също, че държавният интерес за предоставяне на защита на гражданите и за наказване на противоправните деяния не би могъл да легитимира несъразмерното засягане на основни права на човека.

25. При тези обстоятелства с акт от 6 април 2016 г., постъпил в Съда на 14 април 2016 г., Audiencia Provincial de Tarragona (съд на провинция Тарагона) решава да спре производството и да постави следните преюдициални въпроси на Съда:

- „1) Може ли достатъчната тежест на престъплението като критерий, обосноваващ засягането на признатите в членове 7 и 8 от [Хартата] основни права, да се определи единствено с оглед на наказанието, което може да се наложи за разследваното престъпление, или е необходимо освен това да се установи, че с престъпното деяние се увреждат в особена степен индивидуални и/или колективни правни интереси?
- 2) Евентуално, ако определянето на тежестта на престъплението с оглед единствено на наказанието, което може да се наложи, отговаря на конституционните принципи на Съюза, приложени от Съда на ЕС в решението му [Digital Rights] като критерии за строг контрол на Директивата[, обявена за невалидна с това решение], то какъв следва да е минималният праг за наказанието? Допустимо ли е по общ начин да се предвиди праг от три години лишаване от свобода?“.

26. С решение на председателя от 23 май 2016 г. производството пред Съда е спряно до обявяването от Съда на решение по съединени дела Tele2 Sverige и Watson и др., C-203/15 и C-698/15.

27. Запитана от Съда след обявяването на това решение на 21 декември 2016 г.<sup>19</sup>, запитващата юрисдикция посочва, че поддържа преюдициалното си запитване. Тя отбелязва, че поставените от нея преюдициални въпроси остават релевантни, доколкото наистина в споменатото съдебно решение се дават примери за тежки престъпления<sup>20</sup>, но не се определя достатъчно ясно материалноправното съдържание на понятието „тежест на престъплението“, така че да послужи като критерий, с оглед на който да се прецени обосновката на определена мярка за намеса. Според нея това понятие създава риска от твърде широко определяне на национално равнище на условията за запазване на данните и за достъп до тях, което да не зачита основните права,

17 Вж. точка 15 и сл. от настоящото заключение. Според запитващата юрисдикция това изменение е явно релевантно с оглед на преюдициалното запитване. В заседанието испанското правителство посочи, че новата правна уредба е приложима в настоящия случай.

18 И по-точно престъпленията „тероризъм“ и извършените в рамките на престъпна група или организация.

19 Вж. бележка под линия 4 от настоящото заключение.

20 Вж. точка 103 от решение Tele2, където са посочени „организираната престъпност и тероризм[ът]“. Отбелязвам, че същите два нагледяващи примера са посочени в точки 24 и 51 от решение Digital Rights, очевидно във връзка с текста на съображения 7–10 от Директива 2006/24, обявена за невалидна с това решение.

упоменати в решение Tele2. В този смисъл при приемане на Устройствен закон 13/2015, въпреки критериите, посочени в решение Digital Rights<sup>21</sup>, испанският законодател много осезаемо намалил прага на тежест на престъпленията, в сравнение с действащите преди това правила съгласно Закон 25/2007, за които се разрешават запазването и предаването на лични данни.

28. След този отговор производството пред Съда е възобновено на 16 февруари 2017 г. Писмени становища впоследствие представят испанското, чешкото, естонското, ирландското, френското, латвийското, унгарското, австрийското правителство, правителството на Обединеното кралство и Европейската комисия.

29. Във връзка със заседанието Съдът поставя на испанското правителство въпроси, на които иска писмен отговор, на които то отговаря на 9 януари 2018 г., както и въпроси до всички заинтересовани субекти по член 23 от Статута на Съда на Европейския съюз, от които иска устен отговор.

30. В заседанието, проведено на 29 януари 2018 г., испанската прокуратура, испанското, чешкото, датското, естонското, ирландското, френското, латвийското, полското правителство, правителството на Обединеното кралство и Комисията представят устни становища.

#### IV. Анализ

##### A. Встъпителни бележки

31. Преди да пристъпя към задълбочено разглеждане на въпросите, които повдига настоящото преюдициално запитване, смятам за необходимо да направя някои бележки във връзка със специфичния му предмет.

32. *Първо*, с оглед на данните, съдържащи се в акта за преюдициално запитване, и на допълнителната информация, предоставена от испанското правителство, за мен *спорът в главното производство* има значителни особености, които го разграничават по-специално от контекста по делата, приключили с решения Digital Rights и Tele2<sup>22</sup>.

33. Действително, установява се, че разглежданото по настоящото дело искане на полицейските органи е насочено към предаването *единствено* на данни, позволяващи да се разкрие самоличността на притежателите или ползвателите на телефонните номера, свързани със СИМ картите, поставени в откраднатия мобилен телефон<sup>23</sup>. Освен това е безспорно, че искането е за ясно определен и ограничен във времето период, а именно около 12 дни<sup>24</sup>.

21 Запитващата юрисдикция споменава по-специално точка 60 от решение Digital Rights, в която Съдът отбелязва, че „Директива 2006/24 не предвижда никакъв обективен критерий, позволяващ да се ограничи достъпът на компетентните национални органи до данните и тяхното последващо използване за целите на предотвратяването, разкриването или преследването на престъпления, които — с оглед на широтата и сериозността на намеренията в основните права по членове 7 и 8 от Хартата — да могат да се считат за достатъчно тежки, че да обосновават подобна намеса. Обратно, член 1, параграф 1 от Директива 2006/24 съдържа единствено общо препращане към тежките престъпления, както са определени в националното право на всяка държава членка“.

22 По този въпрос вж. по-специално бележки под линия 3 и 4 от настоящото заключение.

23 Според мен споменатите „притежатели и ползватели“, посочени в искането, няма как да не са абонати, регистрирани или поне подлежащи на идентифициране лица (вж. и бележка под линия 25 от настоящото заключение), а не просто хора, които са купили СИМ карта, без да оставят следи.

24 Вж. точка 20 от настоящото заключение.



34. При тези обстоятелства броят на лицата, които е възможно да бъдат засегнати от спорната мярка, не е неограничен, а тъкмо обратното. Освен това тези лица са не просто най-обикновени притежатели на СИМ карта, а хора с твърде специфичен профил, тъй като са използвали откраднатия телефон, след като е бил отнет, той дори е все още у тях и следователно могат да се окажат заподозрени, че или те самите са извършителите на престъплението, или се намират във връзка с последните.

35. В допълнение, посочените данни не са какъв да е вид „лични данни“<sup>25</sup>, притежавани от доставчиците на електронни съобщителни услуги, а само свързани с гражданскоправната самоличност на посочените физически лица, т.е. тяхното лично и фамилно име и евентуално адрес<sup>26</sup>, като в този смисъл би могло също да се каже, че става дума за информация „за контакт“. Останалата информация за тези хора, която би могла да се намира в архивите на доставчиците<sup>27</sup>, според мен е изключена от предмета на главното производство.

36. Освен това целта, преследвана според мен в случая, е да се съберат сведения, които не са свързани нито със самото местонахождение, нито със самите съобщения<sup>28</sup>, а с физически лица, издирвани заради това, че може да са използвали електронна съобщителна услуга през откраднат телефон, дори и да не са провеждали конкретен телефонен разговор. Всъщност от разясненията, предоставени от испанската прокуратура на Съда, е видно, че исканите лични данни, изведени от връзката между определена СИМ карта и IMEI номера на откраднатия апарат, технически могат да се получат след самото му свързване с мобилна телефонна клетка, дори притежателят на картата изобщо да не е провеждал разговор с помощта на съответния телефон, т.е. независимо от всякаква ефективна комуникация<sup>29</sup>. Запитващата юрисдикция следва да провери това фактическо по характера си твърдение, което все пак ми се струва достатъчно правдоподобно, за да се приеме за истина.

37. С оглед на изложените съображения още тук ще подчертая, че спорът в главното производство е относно лични данни, чието предаване е поискано не общо и недиференцирано, а целенасочено, що се отнася до лицата, и ограничено, що се отнася до обхванатия период. Вижда се също, че поисканите данни на пръв поглед не са особено чувствителни, макар да има възможност достъпът до този вид данни да засегне основните права, закрепени в членове 7 и 8 от Хартата<sup>30</sup>.

25 Съгласно определението по член 2, буква а) от Директива 95/46, към което препраща член 2 от Директива 2002/58, понятието „лични данни“ обхваща „всяка информация, свързана с идентифицирано или подлежащо на идентификация лице“, като се уточнява, че „за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност“. Съдът вече е отбелязал, че „зачитането на правото на личен живот с оглед на обработката на лични данни се отнася до всяка информация“, отговаряща на това определение (вж. по-специално решение от 17 октомври 2013 г., Schwarz, C-291/12, EU:C:2013:670, т. 26), и че нейният обхват е много широк (вж. по-специално решение от 20 декември 2017 г., Nowak, C-434/16, EU:C:2017:994, т. 33).

26 Според испанското правителство адресът на заинтересованите лица не е бил поискан изрично.

27 Информация като например семейното положение на лицето, номера на националната му лична карта, банковата му сметка или евентуално абонамента му за телефон.

28 Сведения, които би могло да се отнасят до входящи или изходящи обаждания, или пък до датата, продължителността или честотата на комуникациите, а дори и до тяхното съдържание. Испанското правителство уточнява, че в случая полицейските органи са посочили изрично, че искането им няма за цел получаването на данни, защитени от тайната на съобщенията.

29 С други думи, тези данни би могло да се получат при самото активиране на въпросния мобилен апарат, независимо дали същият впоследствие е бил използван от собственика или притежателя в рамките на определен процес на междуличностна комуникация.

30 Вж. точка 74 и сл. от настоящото заключение.

38. *Второ*, отбелязвам, че от мотивите на акта за преюдициално запитване е видно, че поставените по настоящото дело преюдициални въпроси се характеризират с това, че се отнасят не до условията за *запазване* на лични данни в сектора на електронните съобщения, а по-скоро до условията и реда за *достъп* на националните органи до такива данни, запазени от доставчиците на услуги, действащи в този сектор<sup>31</sup>.

39. Запитващата юрисдикция посочва по-специално че съгласно член 588ter j от Наказателно-процесуалния кодекс се изисква съдебно разрешение, за да бъдат архивирани електронни данни, предадени от доставчиците на услуги на компетентните органи с цел приобщаването им към материалите по делото. Параграф 1 от този член уточнява, че запазването на такива данни може да е било извършено от доставчиците или съгласно приложимия закон, или по тяхна инициатива по търговски или други съображения.

40. В случая е видно, че личните данни, до които полицейските органи искат да получат достъп за целите на разследването, са могли да бъдат архивирани от мобилните телефонни оператори в изпълнение на задължение, произтичащо от испанския закон<sup>32</sup>. Запитващата юрисдикция не дава разяснения по този въпрос, като трябва да се напомни, че преюдициалното ѝ запитване се съсредоточава около евентуалния достъп до данни, които вече са били запазени, както и да се уточни, че в спора по главното производство съответствието на съхраняването на данните с изискванията на правото на Съюза не се поставя под съмнение<sup>33</sup>. Ето защо според мен трябва да се допусне, че разглежданите в главното производство данни са били запазени в съответствие с националното законодателство, при спазване на условията, установени в член 15, параграф 1 от Директива 2002/58 — нещо, което единствено запитващата юрисдикция трябва да провери<sup>34</sup>.

41. В по-нататъшното изложение ще разгледам правното значение на констатациите, изложени във встъпителната част по-горе<sup>35</sup>.

## ***Б. По процесуалните възражения, повдигнати от испанското правителство***

42. Испанското правителство повдига две категории процесуални възражения, едната във връзка с компетентността на Съда, а другата — с допустимостта на преюдициалното запитване, които Съдът ще трябва да обсъди, преди евентуално да се произнесе по същество.

31 Уточнявам, че като цяло достъпът до лични данни според мен не крие по-малко рискове по отношение на основните права, закрепени в членове 7 и 8 от Хартата, отколкото тяхното запазване. Може дори да се счита, че опасността е по-голяма, тъй като достъпът до запазени данни конкретизира евентуалната възможност за вредоносното им използване.

32 Испанското правителство посочва, че личното и фамиалното име и евентуално адресът на притежателя на СИМ карта могат законосъобразно да бъдат запазени в Испания. Всъщност смятам, че видно от член 1 и член 3, параграф 1, буква а), точка 1, подточка ii) от Закон 25/2007 (вж. т. 10 и сл. от настоящото заключение), мобилните телефонни оператори са длъжни да запазват данните, генерирани или обработвани в рамките на предоставяните от тях услуги, и по-специално името и адреса на абоната или на регистрирания потребител, необходими за проследяване и идентифициране на източника на съобщението. Напомням, че равностойни изисквания се съдържат в член 3 и член 5, параграф 1, буква а), точка 1, подточка ii) от Директива 2006/24, транспонирана с посочения закон.

33 Обстоятелство, отбелязано от Съда и в решение от 29 януари 2008 г., Promusicae (C-275/06, EU:C:2008:54, т. 45 in fine).

34 В този смисъл решение от 19 април 2012 г., Bonnier Audio и др. (C-461/10, EU:C:2012:219, т. 37).

35 По-специално, що се отнася до компетентността на Съда и до отговора на първия преюдициален въпрос, вж. съответно точка 43 и сл, както и точка 70 и сл. от настоящото заключение.

*1. По компетентността на Съда с оглед на приложното поле на правото на Съюза*

43. Най-напред напомням, че съгласно постоянната съдебна практика основните права, гарантирани в правния ред на Съюза, и по-специално закрепените в членове 7 и 8 от Хартата, трябва да се прилагат само ако съответният случай се урежда от правото на Съюза<sup>36</sup>. Освен това член 51, параграф 1 от Хартата предвижда, че разпоредбите ѝ се отнасят за държавите членки единствено „когато те прилагат правото на Съюза“, съгласно практиката на Съда относно това понятие<sup>37</sup>. Следователно, когато дадено правно положение не попада в приложното поле на правото на Съюза, Съдът няма компетентност да се произнася по него и евентуално посочените разпоредби на Хартата сами по себе си не биха могли да обосноват такава компетентност<sup>38</sup>.

44. В случая въпросите на запитващата юрисдикция се отнасят единствено до членове 7 и 8 от Хартата, както и до „конституционните принципи на Съюза, приложени от Съда на ЕС в решението му [Digital Rights]“. Същевременно според тази юрисдикция директивите, приложими в областта на личните данни, например Директива 95/46 и Директива 2002/58, установяват изискваната съгласно член 51, параграф 1 от Хартата привръзка между главното производство и правото на Съюза.

45. В това отношение отбелязвам, *на първо място*, че испанското правителство поддържа основно че Съдът няма необходимата компетентност, за да се произнесе по настоящото преюдициално запитване, тъй като последното не е свързано с прилагането на правото на Съюза. То по-специално твърди, че спорът по главното производство бил *изключен от приложното поле на правото на Съюза*, тъй като се отнася до зависещ от съдебно решение достъп на полицията до данни в рамките на разследване, а това съставлявало дейност на държавата в областта на наказателното право<sup>39</sup> и следователно попадало сред изключенията по член 1, параграф 3 от Директива 2002/58, както и по член 3, параграф 2, първо тире от Директива 95/46<sup>40</sup>. В заседанието правителството на Обединеното кралство посочи, че споделя това виждане на испанското правителство.

46. Според мен обаче Директива 2002/58 е приложима към национални мерки като разглежданите в главното производство. Всъщност в решение Tele2 Съдът вече е постановил, че националните законодателства относно запазването на данни за целите на борбата с престъпността попадат в приложното поле на тази директива, тъй като не само определят задълженията, възложени на това основание на доставчиците на електронни съобщителни услуги, но и уреждат достъпа на националните органи до запазените в тази връзка данни<sup>41</sup>. Подобно на Комисията считам, че изложените в това решение съображения могат да бъдат пренесени към приложимите в случая национални правила, а именно съдържащите се в Закон 25/2007 във връзка с испанския наказателно-процесуален кодекс, изменен с Устройствен закон 13/2015<sup>42</sup>, и следователно могат да бъдат пренесени към предмета на спора в главното производство.

36 Вж. по-специално решение от 16 май 2017 г., Berlioz Investment Fund (C-682/15, EU:C:2017:373, т. 49 и цитираната съдебна практика).

37 Вж. по-специално решение от 6 октомври 2016 г., Paoletti и др. (C-218/15, EU:C:2016:748, т. 14 и сл.).

38 Вж. по-специално решение от 1 декември 2016 г., Daouidi (C-395/15, EU:C:2016:917, т. 63).

39 Според испанското правителство се упражнявало правото на държавните органи да налагат наказание (ius puniendi). По този въпрос вж. заключението на генералния адвокат Campos Sánchez-Bordona по дело Breyer (C-582/14, EU:C:2016:339, т. 86—92).

40 Принципиите, установени с тези разпоредби, са упоменати и в съображение 11 от Директива 2002/58, което препраща към член 15, параграф 1 от нея (вж. т. 6 и 7 от настоящото заключение).

41 Вж. точки 72—81 от решение Tele2. В този аспект вж. и заключението ми по съединени дела Tele2 Sverige и др. (C-203/15 и C-698/15, EU:C:2016:572, т. 88—97 и 124).

42 Вж. по-специално член 1, параграф 1 от Закон 25/2007 и член 579, параграф 1 от Наказателно-процесуалния кодекс, цитирани в точки 11 и 17 от настоящото заключение, както и точка 40 от настоящото заключение във връзка със законовото задължение на посочените доставчици.

47. Добавям, че следва да не се смесват, от една страна, личните данни, обработвани *пряко* в рамките на властническите<sup>43</sup> по естеството си дейности на държавата в определена област от наказателното право<sup>44</sup>, и от друга страна, личните данни, обработвани в рамките на търговски по естеството си дейности на доставчик на електронни съобщителни услуги, които се използват *впоследствие* от компетентните държавни органи<sup>45</sup>. В допълнение отбелязвам, че Съдът наскоро бе сезиран с преюдициално запитване за тълкуването по-специално на член 1, параграф 3 от Директива 2002/58 в контекста на използването от службите за сигурност и разузнавателните служби на масиви от данни, които трябва да им бъдат предадени от такива доставчици<sup>46</sup> — проблем, който според мен не е необходимо да се решава в настоящото дело<sup>47</sup>.

48. *На второ място* отбелязвам, че във връзка с *приложното поле на Директива 2002/58* възникват други въпроси, от които зависи компетентността на Съда по настоящото дело *предвид вида на данните, разглеждани в главното производство*.

49. Както вече отбелязах<sup>48</sup>, от материалите по делото е видно, че спорното искане за достъп е за предаването на информацията относно самоличността на притежателите или ползвателите на телефонните номера, съответстващи на СИМ картите, активирани с помощта на откраднатия мобилен телефон, за да се открият лицата, в чиято фактическа власт се е намирал този апарат, а не сведенията за евентуално осъществяваните от него обмядания.

50. С други думи, макар с оглед на испанската правна уредба<sup>49</sup> да би било възможно да се засегнати по-широк кръг от данни, спорът по главното производство в настоящия случай се отнася за данни, свързани само със самоличността на „потребители“ по смисъла на член 2, втора алинея, буква а) от Директива 2002/58, а не с каквото и да било „местоположение“<sup>50</sup> по смисъла на същия член 2, втора алинея, буква в), нито със самите „комуникации“ по смисъла на член 2, втора алинея, буква г)<sup>51</sup>.

51. Според испанската прокуратура, испанското, датското, ирландското и латвийското правителство, правителството на Обединеното кралство и Комисията, информацията като разглежданата в случая, при положение че се отчита изолирано, т.е. независимо от евентуално осъществяваните комуникации, по принцип също не би трябвало да попада в понятието „данни за трафик“ по смисъла на посочения член 2, втора алинея, буква б), който ги определя като „всякакви данни, обработени с цел пренасяне на комуникация през електронни комуникационни мрежи или за изготвяне на сметка за това“<sup>52</sup>.

43 Следва да се уточни, че т.нар. „властнически“ дейности на държавата се свързват със запазените за държавата и нейните подразделения функции, които тя не може да делегира на частноправни субекти, а именно дейностите, свързани с правораздаването, полицията и въоръжените сили.

44 Например данните, обработвани от полицейските или съдебни органи с цел издирване на извършители на престъпления (например данните, събрани и анализирани при прихващане на телефонни разговори, извършено от полицейски служители по разпореждане на съдия-следовател).

45 Например данните относно координатите на ползвателите на телефонна услуга, когато тези данни се използват при наказателно разследване, както в главното производство.

46 Вж. акта за преюдициално запитване по висящото дело Privacy International (C-623/17), в който по-специално се посочват решенията от 30 май 2006 г., Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346, т. 56–59), както и от 10 февруари 2009 г., Ирландия/Парламент и Съвет (C-301/06, EU:C:2009:68, т. 88 и 91), откъдето следвало, че обработването на данните за пътниците във въздушния транспорт, предмет на първото решение, се изисква с оглед не на извършването на доставка на услуги, а на опазването на обществената сигурност, и следователно е изключено от приложното поле на Директива 95/46.

47 Като се има предвид, от една страна, че спорът по главното производство има за предмет предаване не на масиви, а на целеви данни, и от друга, че съображенията на Съда по дело Tele2 според мен могат да бъдат пренесени към настоящия случай, както отбелязах това в точка 46 от настоящото заключение.

48 Вж. точка 33 и сл. от настоящото заключение.

49 Вж. по-специално член 1, параграф 2 от Закон 25/2007 и член 579, параграф 1 от Наказателно-процесуалния кодекс.

50 Всъщност искането на полицейските органи е за установяване не на географското положение на откраднатия апарат или на лицата, у които се е намирал, а единствено на самоличността им.

51 Разпоредби от споменатия член 2, цитирани в точка 8 от настоящото заключение.

52 Данните за трафик са уредени в член 6 от Директива 2002/58.

52. Действително, изглежда, че поисканите от полицейските органи данни за идентификация не са свързани с „трафика“ на комуникации в тесен смисъл, доколкото е видно, че тези данни могат да бъдат получени въпреки евентуалното пълно отсъствие на обаждания от откраднатия апарат, и следователно дори въпреки липсата на пренос от мобилен телефонен оператор на каквато и да било междуличностна комуникация през разглеждания в искането период<sup>53</sup>.

53. Въпреки това считам, че спор като този по главното производство попада в приложното поле на Директива 2002/58, след като обработването на информацията, свързана със СИМ картите и техните притежатели, обект на внимание в случая, е необходимо от търговска гледна точка за предоставянето на електронни съобщителни услуги<sup>54</sup>, поне за да се изготви сметката за предоставяната услуга<sup>55</sup>, независимо какви обаждания са били правени или не в рамките на услугата.

54. С оглед на член 1, параграф 1 и член 3 от Директива 2002/58<sup>56</sup> споделям становището, изложено по-специално от Комисията, че Директивата има за цел да уреди изцяло обработването на лични данни, осъществявано при предоставянето на електронни съобщителни услуги, поради което нейното приложно поле включва данните за самоличността на потребителите на такива услуги, каквито са разглежданите в случая, а не само тези за конкретно съобщение. Ето защо с оглед и на целите за защита, залегнали в тази директива, изразяващи се най-вече в опазване на основните права, гарантирани от Хартата<sup>57</sup>, според мен понятието „комуникация“ по смисъла на този акт трябва да се схваща широко и предвиденият в него принцип на поверителност на съобщенията<sup>58</sup> в случая действително намира приложение.

55. Според мен това тълкуване се потвърждава от предходно решение на Съда, в което той вече е приел, че приложното поле на Директива 2002/58 обхваща спор относно предаването на имената и адресите на потребителите на електронна съобщителна услуга<sup>59</sup>. Добавям, че член 12 от същата директива, който се отнася до указателите на абонатите, според мен със сигурност засяга данни от такова естество<sup>60</sup>, както и че съображение 15 от нея също свидетелства за гъвкаво схващане на понятието „комуникация“, включвайки в него по-специално „адресиране на информация, предоставена от изпращача на комуникация“<sup>61</sup>.

53 Вж. точка 36 от настоящото заключение.

54 Електронната съобщителна услуга е дефинирана в член 2, буква в) от Директива 2002/21 (с която се приема общата регулаторна рамка в тази област) като „услуга, осигурявана обикновено срещу заплащане, която се състои изцяло или главно в пренасянето на сигнали по електронни съобщителни мрежи [...]“.

55 Обстоятелството, че обработването на данни може да е необходимо за изготвянето на сметка за услугата, по-специално що се отнася до абонатите, е упоменато в редица разпоредби от Директива 2002/58 (и по-специално в съображения 26, 27 и 29, в член 2, втора алинея, буква ж) и в член 6, параграфи 2 и 5). Във връзка с това вж. и точка 86 от решение Tele2 и цитираната там съдебна практика.

56 Разпоредби, отнасящи се съответно най-общо до „обработката на лични данни в електронно-комуникационния сектор“ и „обработката на лични данни във връзка с предоставянето на публично достъпни електронни комуникационни услуги“.

57 Вж. съображения 2, 7 и 11, член 1, параграф 1 и член 15, параграф 3 от Директива 2002/58.

58 Вж. съображение 21 от Директива 2002/58, както и член 1, параграф 1 и член 5 от нея, като последният урежда специално конфиденциалността на комуникациите.

59 Вж. решение от 29 януари 2008 г., Promusicae (C-275/06, EU:C:2008:54, т. 29—31 и 45).

60 Относно тълкуването на член 12 вж. по-специално решение от 15 март 2017 г., Tele2 (Netherlands) и др. (C-536/15, EU:C:2017:214, т. 33 и сл. и цитираната съдебна практика).

61 Съгласно посоченото съображение 15 „[к]омуникацията може да включва всякаква информация относно наименование, номериране или адресиране на информация, предоставена от изпращача на комуникация или потребителя на връзка, за да извърши комуникацията [...]“.

56. Освен това подобен подход е в съответствие с практиката на ЕСПЧ в тази област<sup>62</sup>, като следва да се напомни, че в съображенията на Директива 2002/58 се подчертава, че тя има за цел да гарантира поверителния характер на комуникациите и правото на потребителите на личен живот в съответствие с ЕКПЧ и тълкуването ѝ от посочения съд<sup>63</sup>, макар и този акт формално да не е част от правния ред на Съюза<sup>64</sup>

57. Следователно считам, че спор като този по главното производство попада в материалния обхват на Директива 2002/58 и че поради това възражението за липса на компетентност, повдигнато от испанското правителство, трябва да се отхвърли.

58. За изчерпателност все пак уточнявам, че ако Директива 2002/58 не бъде призната за приложима в подобна хипотеза, Директива 95/46, посочена както от запитващата юрисдикция, така и от испанското правителство, не би могла да послужи като основание за компетентността на Съда да се произнесе по настоящото дело.

59. Както посочва Комисията, Директива 95/46 действително представлява акт с общо приложение в областта на обработването на лични данни<sup>65</sup>, но считам, че поставените от запитващата юрисдикция въпроси биха се оказали ирелевантни, ако се разгледат само от тази позиция, като се има предвид, че са насочени към определянето на прага, отвъд който престъпленията могат да се окачествят като „тежки“ по смисъла на съдебната практика, установена с решения Digital Rights и Tele2, които не разглеждат тълкуването на посочената директива<sup>66</sup>.

## 2. По допустимостта на преюдициалното запитване

60. При условията на евентуалност, ако Съдът приеме, че е компетентен да отговори на поставените въпроси, испанското правителство твърди, че преюдициалното запитване би трябвало да се обяви за недопустимо поради две причини.

61. *На първо място* то сочи, че запитващата юрисдикция *не идентифицирала ясно нормативната уредба на Съюза*, по която Съдът трябва да се произнесе.

62 Понятието за данни относно личния живот на лицето по смисъла на член 8 от ЕКПЧ (цитиран в бележка под линия 8 от настоящото заключение) се тълкува разширително от ЕСПЧ (вж. по-специално ЕСПЧ, 13 февруари 2018 г., Ivashchenko с/у Русия, SE:ECHR:2018:0213JUD006106410, §§ 63 и сл.), както това вече е било отбелязано (вж. решение от 9 ноември 2010 г., Volker und Markus Schecke и Eifert, C-92/09 и C-93/09, EU:C:2010:662, т. 59 и цитираната практика на ЕСПЧ).

63 Вж. съображения 3, 11 и 24 от Директива 2002/58.

64 Вж. по-специално решение Tele2 (т. 120, в която се прави аналогия с практиката на ЕСПЧ, както и т. 126 и сл., в които се напомня положението на Съюза по отношение на ЕКПЧ).

65 Докато Директива 2002/58 урежда конкретно сектора на електронните комуникации (вж. по-специално съображения 4 и 10 и член 1, параграфи 1 и 2 от нея).

66 Напомням, че понятието „тежки престъпления“ е въведено като критерий, ограничаващ действията на държавите членки, с Директива 2006/24 за запазването на данните, обявена за невалидна с решение Digital Rights, а след това е използвано от Съда в решение Tele2 за тълкуване на разпоредбите на Директива 2002/58 в контекста на национална правна уредба за запазване на данни и достъп до тях (вж. и бележки под линия 3 и 4 от настоящото заключение). От това според мен следва, че ако Директива 2002/58 се обяви за неприложима в случая, не би имало основание да се прави исканото от запитващата юрисдикция тълкуване на това понятие.

62. По този въпрос то припомня постоянната съдебна практика, съгласно която в рамките на въведеното с член 267 ДФЕС сътрудничество Съдът може да откаже да се произнесе по преюдициални въпроси, които се ползват с презумпция за релевантност, само когато е очевидно, че исканото тълкуване или преценка на валидността на норма от правото на Съюза няма никаква връзка с действителността или предмета на спора по главното производство, когато проблемът е хипотетичен или когато Съдът не разполага с необходимите данни от фактическа и правна страна, за да бъде полезен с отговора на поставените му въпроси<sup>67</sup>.

63. Считаю обаче, че в случая възражението на испанското правителство е неоснователно. Всъщност, видно от предоставените от запитващата юрисдикция сведения, според мен тя в достатъчна степен е идентифицирала разпоредбите от правото на Съюза, които счита за релевантни. Напомням, от една страна, че поставените въпроси се отнасят по-специално до членове 7 и 8 от Хартата, от друга страна, че за посочената юрисдикция Директиви 95/46 и 2002/58 съставляват необходимата привръзка между приложимата в главното производство национална правна уредба и правото на Съюза<sup>68</sup>, и накрая, че както е посочено в съображение 2 от Директива 2002/58, тя се стреми да осигури по-специално пълно зачитане на правата, предвидени в членове 7 и 8 от Хартата<sup>69</sup>.

64. Добавям, че е без значение обстоятелството, че един от актовете от испанската правна уредба, посочени в преюдициалното запитване, а именно Закон 25/2007, е имал за цел да транспонира Директива 2006/24, отменен след обявяването ѝ за невалидна с решение Digital Rights<sup>70</sup>. Както правилно отбелязва запитващата юрисдикция, би било неточно да се приеме, че поставените в случая на Съда преюдициални въпроси са ирелевантни поради обявяването на посочения акт за невалиден. В тази насока е достатъчно да се констатира, че материята, до която се отнасят тези въпроси, а именно защитата на личните данни, попада в компетентността на Съюза, а спорът в главното производство е в приложното поле на акт на Съюза — Директива 2002/58<sup>71</sup>, която обявената за невалидна Директива 2006/24 е трябвало да измени.

65. Впрочем може да се отбележи, че повечето от страните, представили становища пред Съда, изхождат от принципа, че настоящото преюдициално запитване трябва да се изследва от гледна точка на член 15, параграф 1 от Директива 2002/58 във връзка с членове 7 и 8 от Хартата, както и с оглед на изводите, произтичащи от решения Digital Rights и Tele2. Това е и моето мнение, но уточнявам, че в Директива 2002/58 изразът „криминални нарушения“, а не „тежки престъпления“ се съдържа само в посочения член 15, параграф 1<sup>72</sup>.

66. *На второ място*, испанското правителство поддържа, че член 7 от Хартата, около който се съсредоточавало настоящото преюдициално запитване, *не бил релевантен*, поради това че исканата по делото в главното производство мярка за разследване не била насочена към прихващането на комуникации и следователно не можела да засегне тяхната поверителност, което правело хипотетични поставените въпроси.

67 Вж. по-специално решения от 16 юни 2015 г., Gauweiler и др. (C-62/14, EU:C:2015:400, т. 24 и 25), както и от 22 февруари 2018 г., Pórras Guisado (C-103/16, EU:C:2018:99, т. 34).

68 Вж. и точка 44 от настоящото заключение.

69 Вж. и решение Tele2 (т. 82).

70 Вж. и точка 10 от настоящото заключение. Отбелязвам, че положението е сходно по едно от делата, приключили с решение Tele2 (вж. т. 15 и 63).

71 Във връзка с последното вж. точка 45 и сл. от настоящото заключение.

72 Вж. и точка 71 от настоящото заключение.

67. От своя страна считам, че член 7 от Хартата е релевантен по настоящото дело и поради това преюдициалното запитване не е хипотетично по характер. Вярно е, че в случая няма риск от нарушение на правото на тайна на съобщенията с оглед на предмета на разглежданата в главното производство мярка<sup>73</sup>, но това не променя факта, че такъв вид мярка може да засегне правото на зачитане на личния живот, гарантирано с тази разпоредба, макар според мен засягането да е слабо по интензитет<sup>74</sup>.

68. Както Съдът е постановявал неведнъж, всъщност съобщаването на лични данни на трето лице, например публичен орган, представлява намеса в основното право, закрепено в член 7 от Хартата, независимо от последващото използване на съобщената информация. Същото се отнася за запазването на лични данни, по-специално от доставчици на електронни съобщителни услуги, както и за достъпа до тези данни с оглед на използването им от публични органи<sup>75</sup>.

69. Ето защо съм на мнение, че повдигнатото от испанското правителство възражение за недопустимост трябва да бъде отхвърлено и поради това следва преюдициалното запитване да бъде разгледано по същество.

***В. По необходимите елементи, определящи достатъчната тежест на престъплението, която обосновава намеса в разглежданите основни права (първи въпрос)***

70. С първия си въпрос запитващата юрисдикция по същество иска от Съда да определи, в съответствие със съдебната практика, установена с решение Digital Rights, последвано от решение Tele2, кои елементи следва да се вземат предвид, за да се установи, че престъпленията са достатъчно тежки, за да обосноват накърняването на основните права, гарантирани с членове 7 и 8 от Хартата, при запазването на лични данни и достъпа до тях.

71. В тази насока напомням, че понятието „тежки престъпления“ се използва от Съда в решение Digital Rights<sup>76</sup>, понякога в съчетание с понятието „тежка престъпност“<sup>77</sup>, като критерий за проверка на целта и пропорционалността на намесата в посочените основни права, до която водят разпоредбите от правото на Съюза относно личните данни, а именно тези на Директива 2006/24. Уточнявам, че това понятие, което не се съдържа в Директива 2002/58<sup>78</sup>, е използвано в Директива 2006/24<sup>79</sup>, обявена за невалидна с посоченото решение. Впоследствие Съдът използва двете понятия в решение Tele2<sup>80</sup> отново като критерий за преценка, но този път за съответствие с правото на Съюза<sup>81</sup> на приети от държавите членки разпоредби.

73 Вж. точки 36 и 52 от настоящото заключение.

74 Относно липсата на сериозност на извършената в случая намеса вж. точка 74 и сл. от настоящото заключение.

75 Вж. по-специално решение Digital Rights (т. 26 и сл.), както и становище 1/15 (Споразумение PNR ЕС—Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 124 и цитираната съдебна практика).

76 Вж. точки 24, 41, 49 и 57—61 от решение Digital Rights.

77 Вж. точки 41, 42, 51 и 59 от решение Digital Rights.

78 Следва да се напомни, че в член 15, параграф 1, първо изречение от Директива 2002/58 се съдържа само изразът „криминални нарушения“.

79 По същество в съображение 9 от Директива 2006/24, както и буквално в съображение 21 и член 1, параграф 1 от нея.

80 Вж. относно понятието „тежки престъпления“ точки 105, 106 и 119, а относно понятието „тежка престъпност“ — точки 102, 103, 108, 110, 111, 114, 115, 118, 125 и 134 от решение Tele2.

81 А именно член 15, параграф 1 от Директива 2002/58, съгласно който държавите членки могат да приемат мерки, които дерогират принципа на поверителност на съобщенията и на свързаните с тях данни за трафик, когато това е необходимо, подходящо и пропорционално в рамките на демократично общество с оглед на посочените в същата разпоредба цели.



72. По-конкретно първият преюдициален въпрос приканва Съда да установи дали, за да се прецени наличието на „тежко престъпление“, годно да обоснове осъществена по отношение на лични данни намеса в основните права, закрепени в членове 7 и 8 от Хартата, трябва да се вземе предвид само предвиденото наказание за съответното престъпление, или и особено вредоносният характер на престъпното деяние по отношение на засегнатите в случая индивидуални или колективни интереси.

73. Подобно на Комисията обаче считам, че преди произнасянето по този въпрос следва да се провери дали намесата, разглеждана в рамките на спор като този в главното производство, е достатъчно сериозна, така че съгласно правото на Съюза, за да бъде допусната, да се изисква тя да бъде обоснована с борбата срещу тежко престъпление. Всъщност считам, че ако това не е така, Съдът би трябвало да тълкува релевантните разпоредби от правото на Съюза, но не като се придържа към поисканото от запитващата юрисдикция, а след като преформулира в необходимата степен първия поставен въпрос<sup>82</sup> с оглед на обстоятелствата по спора в главното производство<sup>83</sup>.

#### *1. По отчитането на липсата на сериозност на спорната намеса*

74. *Най-напред* следва да се установи, че действия като разглежданите в главното производство могат действително да накърнят основните права, гарантирани с членове 7 и 8 от Хартата, и следователно да *представляват намеса* в тези права по смисъла на практиката, установена с решения Digital Rights и Tele2.

75. Наистина, както посочват испанското и датското правителство в устните си становища<sup>84</sup> и както вече отбелязах<sup>85</sup>, данните, до които органите, натоварени с провеждането на разглежданото наказателно разследване, искат да получат достъп, изглежда не са толкова чувствителни, колкото някои други категории лични данни<sup>86</sup>, като се има предвид, че разглежданото искане явно се отнася само до личното, фамилното име и евентуално адреса на разследваните лица като ползватели на телефонни номера, активирани с откраднатия мобилен телефон, който е предмет на това разследване.

76. Според мен обаче, за да се определи дали личните данни трябва да се ползват от защитата, предвидена от правото на Съюза, и по-специално от Директива 2002/58<sup>87</sup>, няма значение дали информацията, за която се отнася искането за запазване или предаване, е особено чувствителна или не. Всъщност, както се отбелязва в първите законодателни работи в тази област, „в зависимост от целта, за която се използват, всички отнасящи се до определено лице данни, дори на пръв поглед да изглеждат безобидни, могат да се окажат чувствителни (например един

82 Следва да се отбележи, че вторият преюдициален въпрос е поставен само при условията на евентуалност.

83 От постоянната съдебна практика е видно, че за да се даде полезен отговор на запитващата юрисдикция, който да ѝ позволи да реши спора, с който е сезирана, при необходимост Съдът трябва да преформулира въпросите, които са му зададени (вж. по-специално решение от 22 февруари 2018 г., SAKSA, C-185/17, EU:C:2018:108, т. 28).

84 Испанското правителство подчертава, че спорните данни в главното производство не позволяват да се установи например профилът на съответното лице.

85 Вж. точки 35—37 от настоящото заключение.

86 Напомням че член 8 от Директива 95/46 предвижда специални правила за обработването на „лични данни, разкриващи расов или [етнически] произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи, ка[р]то и обработването на данни, свързани със здравословното състояние и половия живот“. За понятието за чувствителни данни и обработването им вж. *Наръчник по европейско право в областта на защитата на данните*, изготвен под егидата на Агенцията на Европейския съюз за основните права и Съвета на Европа от 2014 г., чиято актуализирана редакция е достъпна в интернет на следния адрес: <https://www.coe.int/fr/web/data-protection/home>, стр. 46 и сл., както и стр. 94 и сл.

87 Чувствителността на определени данни се споменава само в съображение 25 от Директива 2002/58, без да може на това основание да се направи извод, че това е общо изискване.

обикновен пощенски адрес)<sup>88</sup> [неофициален превод]. Освен това Съдът вече е постановил, че за да е *налице намеса* в основното право, закрепено в член 7 от Хартата, „е без значение дали съответните данни за личния живот имат чувствителен характер и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса“<sup>89</sup>.

77. Освен това напомням, че съобщаването на лични данни на трето лице, дори и на публичен орган като съдебната полиция, представлява намеса в основното право, закрепено в член 7 от Хартата<sup>90</sup>, включително ако информацията се предава за целите на наказателно разследване — положение, което впрочем е изрично предвидено в член 15, параграф 1 от Директива 2002/58<sup>91</sup>. Добавям, че такъв вид действие може да накърни и основното право на защита на личните данни, гарантирано в член 8 от Хартата, тъй като води до обработка на лични данни<sup>92</sup>.

78. Ето защо считам, че следва да се приеме, че мярка като разглежданата в главното производство представлява намеса в основните права, закрепени в членове 7 и 8 от Хартата.

79. При обстоятелствата по случая *обаче* според мен липсва основен елемент, който Съдът изисква, за да е *налице „тежко престъпление“* — понятие, чиято дефиниция е поискана от националната юрисдикция — на етапа на обосновка на намесата, за да може да бъде дерогиран принципът на поверителност на електронните съобщения. Според мен *липсващият* елемент в случая, за да се отговори на първия преюдициален въпрос в съответствие с използваната от тази юрисдикция формулировка, е *сериозността на спорната намеса* — фактор, при чието наличие би била необходима допълнителна обосновка.

80. В това отношение отбелязвам, че в решение Digital Rights Съдът подчертава, че намесата в резултат от разглежданата правна уредба е силно изразена и особено сериозна, като по-специално посочва, че „Директива 2006/24 се прилага общо за всички лица, за всички електронни съобщителни средства, както и за всички данни за трафик, без да въвежда никакво разграничаване, ограничаване или изключение с оглед на целта за борба с тежките престъпления“<sup>93</sup>.

81. По сходен начин в решение Tele2 Съдът постановява, че „[ч]лен 15, параграф 1 от Директива 2002/58 [...] 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“<sup>94</sup>. В това решение е установена и корелативна връзка между, от една

88 Вж. Съобщение на Комисията от 13 септември 1990 година относно защитата на лицата при обработването на лични данни в Общността и относно сигурността на информационните системи (COM(90) 314 окончателен, стр. 20).

89 Вж. Становище 1/15 (Споразумение PNR ЕС-Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 124 и цитираната съдебна практика). ЕСПЧ се произнася в същия смисъл (вж. ЕСПЧ, 16 февруари 2000 г., *Amanp c/y Швейцария*, CE:ECHR:2000:0216JUD002779895, §§ 68—70).

90 Вж. точка 68 от настоящото заключение. Вж. и ЕСПЧ, 8 февруари 2018 г., *Ben Faiza c/y Франция* (CE:ECHR:2018:0208JUD003144612, §§ 66—68) във връзка със съдебно разпореждане за предаването на информация относно начина на използване на телефон.

91 По следния начин: „за да гарантира [...] превенцията, разследването, разкриването и преследването на криминални нарушения“.

92 Вж. в този смисъл становище 1/15 (Споразумение PNR ЕС-Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 126 и цитираната съдебна практика).

93 Точка 57 от решение Digital Rights. Относно особената тежест на разглежданата намеса вж. и точки 37, 39, 47, 48, 60 и 65 от това решение.

94 Точка 1 от диспозитива на решение Tele2.

страна, така констатираната особена „сериозност на намесата“, и от друга, необходимостта да се обоснове засягане с такъв обхват на основните права, гарантирани от членове 7 и 8 от Хартата, на основание на съображение от толкова първостепенен обществен интерес, какъвто е „борбата с тежките престъпления“<sup>95</sup>.

82. Поставянето на констатираната сериозност на намесата във връзка с тежестта на съображението, позволяващо нейното обосноваване, е направено в съответствие с принципа на пропорционалност<sup>96</sup>. Освен това според мен в практиката си по член 8 от ЕКПЧ<sup>97</sup> ЕСПЧ установява равностойна корелативна връзка с произтичащата според мен от решения Digital Rights и Tele2.

83. Както обаче посочих по-горе<sup>98</sup> и както подчертават по-специално френското правителство, правителството на Обединеното кралство и Комисията, естеството на разглежданата в спора по главното производство по настоящото дело намеса в редица отношения се отличава от намесите, които Съдът е разгледал в тези две предишни решения. Следователно изследването на съответствието с правото на Съюза на мярка като тази в случая трябва да се осъществи по друг начин.

84. В случая не е налице мярка, свързана с общо и недиференцирано задължение за запазване на данни за трафика или местонахождението на какъвто и да било абонат или регистриран потребител относно всички електронни съобщителни средства. Мярката е целенасочена и предназначена да предостави възможност за достъп на компетентните органи за нуждите на наказателно разследване до данни, притежавани за търговски нужди от доставчици на услуги, и обхваща единствено самоличността (лично, фамилно име и евентуално адрес) на ограничена категория абонати или ползватели на конкретно средство за комуникация, т.е. лицата, чийто телефонен номер е бил активиран от мобилния телефон, кражбата на който се разследва, при това през ограничен период, а именно около 12 дни<sup>99</sup>.

85. Добавям, че евентуалните вредоносни последици за лицата, за които се отнася разглежданото искане за достъп, едновременно са умерени и ясно очертани. Всъщност, тъй като са предназначени да се използват специално за нуждите на мярка по разследване, поисканите данни не е предвидено да бъдат оповестявани на широката общественост<sup>100</sup>. Освен това

95 Съгласно точка 102 от решение Tele2, „[и]редвид тежестта на намесата в разглежданите основни права, каквато представлява национална правна уредба, предвиждаща за целите на борбата с престъпността запазване на данни за трафик и на данни за местонахождение, само борбата с тежките престъпления може да обоснове такава мярка (вж. по аналогия, що се отнася до Директива 2006/24, решение Digital Rights, т. 60 (където се съдържа формулировката „с оглед на широтата и тежестта на намесата“)“ (курсивът е мой). В точка 115 от решение Tele2 се съдържат същите мотиви във връзка с достъпа до такива данни. Относно особената тежест на разглежданата намеса вж. също точки 97 и 100 от това решение.

96 В този смисъл точка 115 от решение Tele2 подчертава, че „преследваната с [национална правна уредба, с която се дерогира принципът на поверителност на електронните съобщения,] цел трябва да е свързана с тежестта на намесата в основните права, до която води достъпът до запазените данни, поради което същият би бил обоснован — що се отнася до превенцията, разследването, разкриването и преследването на престъпления — само в случаите на борба с тежката престъпност“ (курсивът е мой).

97 Всъщност посочената юрисдикция многократно подчертава необходимостта да се постигне баланс между, от една страна, интереса на държавата да защити своята национална сигурност посредством мерки, засягащи личните данни, и от друга, тежестта на нагърняването на правото на лицето на зачитане на личния живот, два фактора, от които зависи правото на преценка на държавата, по-специално когато последната възнамерява да предотврати или преследва тежки престъпления (вж. ЕСПЧ, 26 март 1987 г., Leander c/y Швеция, CE:ECRH:1987:0326JUD000924881, § 59; ЕСПЧ, 26 юни 2006 г., Weber и Saravia c/y Германия, CE:ECRH:2006:0629DEC005493400, §§ 106, 125 и 126, както и ЕСПЧ, 4 декември 2015 г., Roman Zakharov c/y Русия, CE:ECRH:2015:1204JUD004714306, §§ 232 и 244).

98 Вж. точка 32 и сл. от настоящото заключение.

99 Отбелязвам, че в становище 1/15 (Споразумение PNR ЕС-Канада) от 26 юли 2017 г. (EU:C:2017:592, т. 194 и 207—209) Съдът преценява и необходимостта на намесите съгласно предвиденото споразумение, като разглежда съдържащите се в него правила за използване и запазване на данните, по-специално от гледна точка на особения контекст на тези мерки, на тяхната специфика и времетраене.

100 Такъв би бил случаят например ако самоличността на определени лица бъде разгласена в статия в пресата или в интернет сайт.

възможността за достъп, с която разполагат полицейските органи, се съпътства от процесуални гаранции съгласно испанската правна уредба, тъй като е свързана с последващ съдебен контрол, който впрочем води до отхвърляне на полицейското искане в спора, предмет на главното производство.

86. Намесата в посочените основни права, произтичаща от предаването на споменатите данни за гражданското състояние, според мен не се отличава с особена сериозност<sup>101</sup>, тъй като данни от подобно естество и с толкова ограничен обхват сами по себе си не дават възможност за получаването на различни и/или точни сведения за засегнатите лица<sup>102</sup> и следователно не засягат пряко и интензивно интимната сфера на техния личен живот при конкретните обстоятелства<sup>103</sup>.

87. Следователно, подобно на Комисията, считам, че за да се предоставят релевантни насоки на запитващата юрисдикция, които да ѝ позволят да разреши спора, с който е сезирана, следва първият преюдициален въпрос да се *преформулира*, в резултат от което отговорът, който Съдът ще даде, да бъде относно тълкуването на член 15, параграф 1 от Директива 2002/58 с оглед на обстоятелства като разглежданите в случая, а именно при намеса в посочените основни права, лишена от особена сериозност и обоснована с борбата с определен вид престъпления, чиято тежест е поставена под съмнение.

88. В това отношение напомням, че след като целите, които могат да обосноват национална правна уредба, с която се дерогира принципът на поверителност на електронните съобщения, са изброени изчерпателно в член 15, параграф 1 от Директива 2002/58, достъпът до запазените данни трябва действително и строго да преследва някоя от тях<sup>104</sup>. Сред последните е целта от общ интерес да се „гарантира [...] превенцията, разследването, разкриването и преследването на *криминални нарушения*“<sup>105</sup>, без по друг начин да се уточнява естеството им.

89. От използваната терминология е видно, че не е задължително престъпленията, които легитимират разглежданата ограничителна мярка съгласно член 15, параграф 1, да могат да се окачествят като „тежки“ по смисъла на съдебната практика, установена с решения Digital Rights и Tele2. Според мен само когато претърпяната намеса е особено сериозна, както по делата, приключили с посочените решения, престъпленията, които могат да обосноват такава намеса, трябва също да бъдат особено тежки. Обратно, в случай на намеса, която не е сериозна, следва да се върнем към основния принцип, произтичащ от текста на тази разпоредба, а именно че всякакъв вид „криминални нарушения“ могат да обосноват такава намеса.

90. Според мен следва да се внимава, за да не се възприеме твърде широко разбиране относно изискванията, поставени от Съда с тези две решения, за да не се препятства, или поне не прекомерно, възможността на държавите членки да дерогират установения от Директива 2002/58 режим, която им е предоставена с член 15, параграф 1 от същата, в случаите, в които разглежданите намеси в личния живот едновременно преследват законна цел и са с ограничен обхват, каквито е възможно да настъпят в случая в резултат от искането на разследващата

101 В този смисъл вж. Конвенция за престъпления в кибернетичното пространство, сключена под егидата на Съвета на Европа в Будапеща на 23 ноември 2001 г. и подписана от всички държави — членки на Съюза (достъпна в интернет на адрес: [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?coeconventions\\_WAR\\_coeconventionsportlet\\_languageId=fr\\_FR](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?coeconventions_WAR_coeconventionsportlet_languageId=fr_FR)), в която член 18 изисква приемането на законодателни мерки, овластяващи компетентните органи да разпореждат на доставчик на услуги да предоставя притежавани от него данни за абоната, например „самоличността на потребителя, неговия [...] адрес [и] [телефонен] номер“.

102 Както правилно отбелязва датското правителство, когато полицията получава, както в случая, сведения за името и адреса на собственика на СИМ карта, използвана в рамките на престъпление, това не е коренно различно например от получаването на информация за собственика на автомобил, използван за извършване на престъпление.

103 За разлика от особено подробната информация, по-специално относно проследяването на съобщенията и профила на засегнатите лица, разглеждани по делата, приключили с решение Digital Rights (вж. т. 26—29 и 37) и с решение Tele2 (вж. т. 97—100).

104 Вж. по-специално точки 90 и 115 от решение Tele2.

105 Курсивът е мой.

полицейска служба. По-конкретно считам, че правото на Съюза допуска възможността за компетентните органи да имат достъп до държаните от доставчици на електронни съобщителни услуги данни за идентификация, позволяващи да се издирят предполагаемите извършители на престъпление, което не е тежко.

91. С оглед на това препоръчвам на Съда да отговори на *преформулирания преюдициален въпрос*, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7 и 8 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че мярка, която за целите на борбата с престъпленията дава на компетентните национални органи достъп до идентификационните данни на ползвателите на телефонни номера, активирани с определен мобилен телефон през ограничен период, при обстоятелства като разглежданите в главното производство води до намеса в гарантираните от споменатата директива и Хартата основни права, която не е толкова сериозна, че да налага такъв достъп да се предоставя само в случаите, в които съответното престъпление е тежко.

92. С оглед на предложението отговор следващите съображения в тяхната цялост са представени само при условията на *евентуалност*, за изчерпателност.

*2. По евентуалното определяне на релевантните критерии за наличие на достатъчна тежест на престъплението*

93. В случай че обратно на това, което препоръчвам, Съдът реши, че въпреки твърде особенията обстоятелства по спора в главното производство, следва по настоящото дело да се определи какво се разбира под „тежко престъпление“ по смисъла на съдебната практика, установена с решения Digital Rights и Tele2<sup>106</sup>, би следвало да се провери и, *на първо място*, дали тази квалификация действително представлява *самостоятелно понятие* на правото на Съюза, което поради това би следвало да се дефинира от Съда. Подобно на отговора, предложен от френското правителство, според мен това не е така поради следните съображения.

94. Най-напред отбелязвам, че Директива 2006/24, от която произтича употребата на понятието „тежко престъпление“<sup>107</sup>, не съдържа дефиниция за него, а в това отношение препраща към правната уредба на държавите членки<sup>108</sup>. Добавям, че релевантните съображения, които се съдържат в решения Digital Rights и Tele2, по мое мнение не трябва да се разбират в смисъл, че целят да хармонизират действащите в държавите членки правни норми относно съдържанието на това понятие.

95. В тази насока напомням, че наказателното законодателство и нормите на наказателния процес попадат в компетентността на държавите членки, макар че правният ред на последните все пак може да бъде засегнат от разпоредбите на правото на Съюза, приети в тази област<sup>109</sup>. Съгласно член 83, параграф 2 ДФЕС само когато сближаването на наказателното право на държавите членки е належащо за ефективното прилагане на политика на Съюза в област, в

106 А именно ако Съдът приеме или че разглежданата в главното производство намеса е достатъчно тежка, за да се отговори на първия въпрос по начина, по който е поставен от запитващата юрисдикция, или че в това отношение е без значение, че тази намеса не е сериозна.

107 Вж. точка 71 от настоящото заключение.

108 Член 1, параграф 1 от Директива 2006/24 е предвиждал, че тя „има за цел да хармонизира разпоредбите на държавите членки, свързани със задълженията на доставчиците на [...] електронни съобщителни услуги [...], за да се гарантира, че данните са достъпни за разследването, разкриването и преследването на [тежки] престъпления, както те са определени в националното право на всяка държава членка“ (курсивът е мой). Вж. и съображение 21 от тази директива.

109 Вж. по-специално решения от 15 септември 2011 г., Dickinger и Ömer (C-347/09, EU:C:2011:582, т. 31), и от 6 декември 2011 г., Achughbadian (C-329/11, EU:C:2011:807, т. 33).

която са приети мерки за хармонизиране, Съюзът може да приеме директиви, чиято цел е да се установят минимални правила относно определянето на престъпленията и на санкции в съответната област. Съгласно действащото в момента право на Съюза обаче няма обща разпоредба, предоставяща хармонизирано определение на понятието „тежко престъпление“<sup>110</sup>.

96. Според мен право да определят какво представлява „тежко престъпление“ имат по принцип компетентните органи на държавите членки. Независимо от това, благодарение на преюдициалните запитвания, с които юрисдикциите на държавите членки могат да сезират Съда, същият е натоварен да следи за спазването на всички изисквания, произтичащи от правото на Съюза, и по-специално да осигури последователно прилагане на закрилата, предоставена от разпоредбите на Хартата.

97. Отбелязвам, че въпросната правна квалификация може не само да варира между отделните държави членки в зависимост от следваните традиции и определените от всяка от тях приоритети, но и да търпи колебания с течение на времето в зависимост от насоките в наказателната политика към повече или по-малко строгост, за да се отчетат развитието на престъпността<sup>111</sup> и, в по-общ план, промените в обществото и съществуващите в национален план потребности, по-специално в областта на наказателното преследване.

98. Освен това подчертавам, че след като между минималните и максималните санкции, които традиционно се прилагат в различните държави членки, съществуват големи разлики<sup>112</sup>, тежестта на престъплението не е свързана само с тежестта на наказанието, което се полага за него. Въпросът дали едно престъпление е тежко е твърде относителен, в смисъл че зависи от скалата на санкциите, които поначало се прилагат в съответната държава членка. Ето защо обстоятелството, че дадена държава членка предвижда лишаване от свобода с неголяма продължителност, все пак не предопределя присъщата тежест на съответния вид престъпление<sup>113</sup>.

99. Според мен следва да се зачитат спецификите на наказателноправната система на всяка от държавите членки, доколкото правото на Съюза не определя задължения, които да обвързват стриктно последните, по аналогия с постановеното от Съда във връзка с опазването на обществената сигурност<sup>114</sup>, понятие, което според мен е сходно с понятието за борба с тежката престъпност, по-специално с оглед на текста на член 15, параграф 1, първо изречение от Директива 2002/58.

<sup>110</sup> По този въпрос вж. също точка 112 от настоящото заключение.

<sup>111</sup> Относно динамичния характер на тежката престъпност вж. също моето заключение по съединени дела *Tele2 Sverige* и др. (C-203/15 и C-698/15, EU:C:2016:572, т. 214).

<sup>112</sup> Показателен в това отношение, в областта на борбата с организираната престъпност, е доклад на Комисията от 7 юли 2016 г., който посочва, че наказанията, които са предвидени в държавите членки за тежко престъпление, каквото е участието в престъпна организация, варират значително (от 3 месеца до 17 години лишаване от свобода) (вж. Доклад до Европейския парламент и Съвета въз основа на член 10 от Рамково решение 2008/841/ПВР на Съвета от 24 октомври 2008 година относно борбата срещу организираната престъпност, COM(2016) 448 окончателен, стр. 7, т. 2.1.4.1).

<sup>113</sup> Както посочва датското правителство, в Дания се прилагат по-леки санкции в сравнение с други държави членки, без това да означава, че престъплението се счита за лишено от особена тежест. Например санкцията, предвидена за притежаване на порнографски материал с участие на лице, ненавършило 18 години, е една година лишаване от свобода, докато в други държави членки тя би могла да стигне до 10 години лишаване от свобода за същото деяние, но това не поставя под съмнение констатацията, че това престъпление по естеството си е особено тежко.

<sup>114</sup> Вж. по-специално решение от 22 май 2012 г., I (C-348/09, EU:C:2012:300, т. 21—23), съгласно което „правото на Съюза не налага на държавите членки единна ценностна система, що се отнася до преценката на поведение, което може да бъде счтено за противоречащо на обществената сигурност“ и „държавите членки [...] са свободни да определят изискванията, свързани с обществения ред и обществената сигурност, според националните си нужди, които могат да се различават в отделните държави членки и в различните периоди от време, по-специално като обосноваване на дерогацията от основния принцип за свободното движение на лицата“, но „все пак тези изисквания следва да се разбират в строг смисъл, така че техният обхват не може да бъде определен едностранично от всяка от държавите членки, без контрол от страна на институциите на Европейския съюз“.

100. С оглед на това, при условията на евентуалност, съм на мнение, че понятието „тежко престъпление“ по смисъла на практиката на Съда, установена с решения Digital Rights и Tele2, не представлява самостоятелно понятие на правото на Съюза, чието съдържание би трябвало да се определи от Съда, макар че дерогацията, предвидена в член 15, параграф 1 от Директива 2002/58, трябва да се прилага от държавите членки в съответствие със задълженията, произтичащи от правото на Съюза, и по-специално от основните права, гарантирани от Хартата, при това под контрола на Съда.

101. Във връзка с последното отбелязвам, че от практиката на Съда следва по-специално че член 15, параграф 1, тъй като допуска държавите членки да ограничат обхвата на някои права и задължения, предвидени от тази директива, трябва да се тълкува стеснително и поради това не би могъл да доведе до превръщането на дерогирането на тези принципни права и задължения в правило<sup>115</sup>. Ето защо държавите членки не биха могли да разглеждат твърде широко обхвата на споменатото понятие „тежко престъпление“.

102. *На второ място* и при условията на евентуалност спрямо предходното, ако Съдът приеме, че въпросното понятие е самостоятелно, той би трябвало да отговори на въпроса, както е формулиран от запитващата юрисдикция, и следователно да се произнесе относно критериите, позволяващи да се прецени от гледна точка на правото на Съюза дали определено престъпление се отличава с достатъчна тежест, за да обоснове накърняването на основните права, закрепени в членове 7 и 8 от Хартата.

103. По-конкретно, Съдът би трябвало да определи дали, за да се установи наличието на „тежко престъпление“ по смисъла на цитираната съдебна практика, е достатъчно да се почерпи основание от предвиденото наказание за твърдяното престъпление, или е необходимо и противоправното деяние да е било особено вредоносно за засегнатите в случая индивидуални или колективни интереси. В това отношение според мен, както и според датското, испанското, френското, унгарското, австрийското и полското правителство и правителството на Обединеното кралство би трябвало да се избере не първата, а по същество втората възможност в тази алтернатива, като се отдаде предпочитание на определение, основаващо се на *множество критерии за преценка*<sup>116</sup>.

104. Колкото до тежестта на престъплението, която може да обоснове достъпа до данните, с оглед на принципа на пропорционалност според мен би било невъзможно да се определи тежестта на инкриминираните деяния, отчитайки само евентуалното наказание. Всъщност предвид значителните различия, които все още съществуват между наказателноправните системи на държавите членки, по мое мнение няма как да се приеме, че предвиденото наказание може само по себе си да отрази, независимо дали от качествената гледна точка на вида на наказанието и/или от количествената гледна точка на неговия размер, конкретната тежест на определено престъпление.

105. Независимо че наказанието има важно значение, в тази връзка трябва в същата степен да се вземат предвид и други обективни фактори. От една страна, това по-специално са контекстът, в който се вписва твърдяното престъпление — дали противоправното поведение е умишлено, дали се съпътства от отегчаващи вината обстоятелства и/или е било извършено при условията на рецидив, а от друга страна, значимостта на обществените интереси, които извършителят на престъплението е засегнал, както и естеството и/или мащабите на вредите, които пострадалият

<sup>115</sup> Вж. в този смисъл точка 89 и сл. от решение Tele2 относно принципното задължение да се осигури поверителността на съобщенията и на свързаните с тях данни за трафика.

<sup>116</sup> Уточнявам, че чешкото и естонското правителство по същество предлагат да се отговори, че е възможно като критерий, обосноваващ накърняването на основните права, признати в членове 7 и 8 от Хартата, да се определи достатъчната тежест на престъпленията въз основа само на предвиденото наказание, но според посочените правителства все пак всяка държава членка би трябвало да запази свободата си да предвиди и други обективни критерии, отразяващи спецификата на правната си уредба, ако счита това за необходимо.

е претърпял от последното<sup>117</sup>, и накрая, скалата на приложимите поначало наказания в съответната държава членка<sup>118</sup>. Въз основа на този набор от алтернативни и неизчерпателни критерии за преценка според мен следва евентуално престъплението да се квалифицира като „тежко“ по смисъла на разглежданата практика на Съда.

106. Добавям, че така предложеното тълкуване е съобразено с подхода, който за мен е възприел ЕСПЧ в практиката си относно „предотвратяването на престъпленията“ като цел, позволяваща обосноваването на намеса в правото на личен живот, закрепено в член 8 от ЕКПЧ, с уговорката, че трябва да бъдат изпълнени и други условия<sup>119</sup>. От тази практика според мен следва, че борбата с някои видове престъпления може да бъде валидно основание в този контекст, на което държавите — страни по ЕКПЧ<sup>120</sup>, могат да се позовават, с оглед не толкова само на предвиденото наказание, а по-скоро на различни фактори за оценка, сред които важно място заемат естеството на разглежданите престъпления, както и обществените и частни интереси, които те открояват<sup>121</sup>.

107. Ето защо моето мнение е, че ако понятието „тежко престъпление“ по смисъла на съдебната практика, установена с решения Digital Rights и Tele2, бъде прието от Съда за самостоятелно понятие на правото на Съюза, то би трябвало да се тълкува в смисъл, че тежестта на дадено престъпление, която може да оправдае достъпа на компетентните национални органи до лични данни съгласно член 15, параграф 1 от Директива 2002/58, трябва да се измерва, като се вземат предвид не само наказанията, които е възможно да бъдат наложени, но и съвкупност от други обективни критерии за преценка като упоменатите по-горе.

***Г. По евентуалното определяне на минималния размер на наказанието, необходим за да се определи достатъчната тежест на престъплението, която обосновава намеса в разглежданите основни права (втори въпрос)***

108. С втория си въпрос запитващата юрисдикция по същество приканва Съда, от една страна, да установи минималния размер, който предвиденото наказание трябва да достига, за да може престъплението да се квалифицира като „тежко“ по смисъла на съдебната практика, установена с решения Digital Rights и Tele2, както и, от друга страна, да реши дали праг от три години лишаване от свобода, какъвто предвижда испанският наказателно-процесуален кодекс след реформата от 2015 г.<sup>122</sup>, е в съответствие с изискванията на правото на Съюза.

117 Споделям гледната точка на френското правителство, че съвсем естествено посегателствата срещу основните интереси на нацията, институциите или националната териториална цялост по естеството си попадат в обхвата на „тежката престъпност“, но в него би трябвало да попаднат и други престъпления, например посегателствата срещу живота, физическата или психическа неприкосновеност и достойнството на лицата, както и посегателствата срещу собствеността, водещи до тежки имуществени вреди за пострадалия, а така също и посегателствата, които съставляват поредица и многократни нарушения на установения обществен ред. По отношение на последното, унгарското правителство посочва и възможността за отчитане на изключителното увеличаване на някои престъпления като относителен дял от престъпността в страната.

118 По този въпрос вж. и точка 98 от настоящото заключение.

119 Съгласно член 8, параграф 2 от ЕКПЧ подобна намеса може да бъде обоснована само ако е предвидена в закона, преследва една или няколко законни цели, изброени в този параграф, и е необходима в едно демократично общество за постигането на тази или тези цели.

120 ЕСПЧ е постановил, че съответните престъпления трябва лесно да могат да бъдат идентифицирани от гражданите, без това изискване за предвидимост да налага държавите изчерпателно да изброяват престъпленията, които могат да доведат до подобна мярка (вж. по-специално ЕСПЧ, 4 декември 2015 г., Roman Zakharov c/y Русия, CE:ECHR:2015:1204JUD004714306, § 244).

121 Вж. по-специално ЕСПЧ, 26 юни 2006 г., Weber и Saravia c/y Германия (CE:ECHR:2006:0629DEC005493400, §§ 106 и 115); ЕСПЧ, 4 декември 2008 г., Maqreg c/y Обединено кралство (CE:ECHR:2008:1204JUD003056204, §§ 104 и 119), и ЕСПЧ, 30 май 2017 г., Trabaja Rueda c/y Испания (CE:ECHR:2017:0530JUD003260012, §§ 39 и 40).

122 Вж. точка 15 и сл. от настоящото заключение.



109. Тези въпроси са поставени само при условията на евентуалност, ако в отговор на първия преюдициален въпрос Съдът постанови, че дали определено престъпление е тежко, в смисъл на фактор, който може да обоснове намеса в основните права съгласно посочената съдебна практика, е въпрос, на който може да се отговори, като се държи сметка единствено за количествените аспекти на наказанието лишаване от свобода, което може да бъде наложено.

110. Предвид отговора, който предлагам да се даде на първия преюдициален въпрос, според мен не е необходимо Съдът да се произнася по втория въпрос. Независимо от това, по съображения за изчерпателност, възнамерявам да изложа съображения във връзка с него.

111. Във връзка с *първата част на втория въпрос* считам, по-специално подобно на чешкото и естонското правителство, че *размерът на предвиденото наказание*, който можел сам по себе си да квалифицира престъплението като „тежко“, не би могъл да се определи еднакво на цялата територия на Съюза предвид изложените по-горе съображения в отговор на първия въпрос, поставен от запитващата юрисдикция<sup>123</sup>.

112. Впрочем различията в определението за това, което следва да се разбира под „тежко престъпление“, и по-специално относно прага на наказанието, над който е приложима тази квалификация, присъстват и в актовете на правото на Съюза. Всъщност може да се констатира, че в актове на Съюза, приети на основание член 83, параграф 1 ДФЕС, се предвиждат различни по размер наказания лишаване от свобода за престъпления, които при все това се считат за попадащи в понятието „особено тежка престъпност“<sup>124</sup>, както например следва от член 3 от Директива 2011/92/ЕС<sup>125</sup> и член 15 от Директива (ЕС) 2017/541<sup>126</sup> — актове, отнасящи се съответно до борбата със сексуалното насилие над деца и до борбата с тероризма. В този смисъл самият законодател на Съюза не е избрал еднаква дефиниция на понятието „тежко престъпление“ с оглед на определен количествен аспект на предвиденото наказание.

113. Напомням, че свободата, предоставена на държавите членки, да решават относно минималния размер на наказанията, които се изисква, за да попадне престъплението сред т.нар. „тежки“ престъпления, е ограничена от нормите, съдържащи се в разпоредбите на правото на Съюза в тази област, както и от принципа, че на изключенията не може да се придаде толкова широк обхват, че фактически да се превърнат в общо правило<sup>127</sup>.

114. В случая, макар всяка държава членка да има възможност да преценява какъв праг на наказанието е удачен, за да е налице тежко престъпление, тя все пак е задължена да не установява този праг толкова ниско с оглед на обичайния размер на приложимите в нея наказания<sup>128</sup>, че изключенията от забраната за съхраняване и използване на лични данни, предвидени в посочения член 15, параграф 1, да се превърнат в принципи, както правилно отбелязва ирландското правителство.

<sup>123</sup> Вж. точка 93 и сл. от настоящото заключение.

<sup>124</sup> Следва да се напомни, че член 83, параграф 1 ДФЕС допуска приемането на „минимални правила относно определянето на престъпленията и на санкциите в областта на особено тежката престъпност с трансгранично измерение“, изброени в тази разпоредба.

<sup>125</sup> Директива на Европейския парламент и на Съвета от 13 декември 2011 година относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 2011 г., стр. 1), член 3 от която предвижда наказания от най-малко една година до най-малко десет години лишаване от свобода за различните видове „престъпления, свързани със сексуално насилие“, предвидени в него.

<sup>126</sup> Директива на Европейския парламент и на Съвета от 15 март 2017 година относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета (ОВ L 88, 2017 г., стр. 6), член 15, параграф 3 от която предвижда наказания лишаване от свобода, не по-малки от 8 или от 15 години в зависимост от различните видове „престъпления, свързани с терористични групи“, предвидени в член 4 от същата директива.

<sup>127</sup> Вж. и точка 101 от настоящото заключение.

<sup>128</sup> По този въпрос вж. точка 98 от настоящото заключение.

115. Също така е безспорно, че при намесите в правата, гарантирани от членове 7 и 8 от Хартата, които биха могли да бъдат разрешени от държавите членки съгласно член 15, параграф 1 от Директива 2002/58, във всички случаи трябва да продължат да се спазват общите изисквания, произтичащи от закрепения в член 52, параграф 1 от Хартата принцип на пропорционалност<sup>129</sup>.

116. Що се отнася до *последната част от втория въпрос*, според естонското правителство и Комисията, от една страна, праг, основаващ се единствено на наказание от най-малко *три години лишаване от свобода*, разгледан сам по себе си, изглежда достатъчен за окачествяване на престъпление като „тежко“ по смисъла на практиката на Съда относно достъпа до лични данни, установена с решение Digital Rights, и от друга страна, този праг не е явно несъвместим с правото на Съюза поначало<sup>130</sup>, и по-конкретно с член 15, параграф 1 от Директива 2002/58.

117. Според мен обаче би било желателно Съдът да се въздържа от заемането на позиция в полза на точно определен срок на предвиденото наказание, тъй като това, което за някои държави членки е подходящо, няма непременно да бъде подходящо за други, както и това, което важи към днешна дата за определен вид престъпления, няма непременно да важи по неотменяем начин в бъдеще, както вече посочих<sup>131</sup>. След като определянето на въпросния праг изисква сложна и евентуално подлежаща на развитие оценка, според мен следва да се прояви предпазливост в това отношение и тези действия да се оставят на преценката на законодателя на Съюза в сферата на предоставената му компетентност или на преценката на законодателя на всяка държава членка в границите на изискванията, произтичащи от правото на Съюза.

118. Във връзка с последното отбелязвам, че запитващата юрисдикция посочва риска от размяна на местата между общото правило и дерогациите, предвидени в Директива 2002/58 — риск, който беше споменат по-горе<sup>132</sup>, като тя посочва, че „предвидено[то през 2015 г. от испанския законодател<sup>133</sup>] наказание от най-малко три години лишаване от свобода обхваща мнозинството от престъпните състави“. С други думи, според тази юрисдикция въведеният с измененията в Наказателно-процесуалния кодекс настоящ списък с престъпления, които могат да обосноват в Испания ограничения на правата, защитени съгласно членове 7 и 8 от Хартата, на практика би довел до включването в този списък на повечето предвидени в Наказателния кодекс престъпления.

119. Дори да се допусне, че Съдът приеме като сериозна разглежданата в главното производство намеса, и да се предположи, че посоченият от запитващата юрисдикция резултат настъпи, според мен последният няма да е в съответствие с изискването за пропорционалност, на което трябва да отговарят тези ограничения<sup>134</sup>. Това според мен е така въпреки наличието на съдебен контрол, посочено от испанското правителство, тъй като упражняването на такъв контрол позволява единствено да се попречи на прилагането на мерки, преценени във всеки отделен случай като произволни или твърде интензивни, а не по общ начин да се възпре прилагането на този вид мерки и тяхното разгръщане.

129 Вж. по-специално съображение 11 и член 15, параграф 1 от Директива 2002/58, както и точки 94—96 и 116 от решение Tele2.

130 Вж. по-специално, освен разпоредбите, посочени в бележки под линия 125 и 126 от настоящото заключение, Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 година относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления (ОВ L119, 2016 г., стр. 132), член 3, точка 9 от която дефинира „тежките престъпления“ като „престъпленията, изброени в приложение II, които са наказуеми с лишаване от свобода или с мярка за задържане за максимален срок от най-малко три години съгласно националното право на държава членка“.

131 Вж. точка 97 от настоящото заключение.

132 Вж. точка 101 от настоящото заключение.

133 Промените са упоменати в точка 15 и сл. от настоящото заключение.

134 Вж. и точка 115 от настоящото заключение.

120. Накрая, подчертавам, че подходът, който се предлага като цяло в настоящия раздел, според мен е в съзвучие с възприетия от ЕСПЧ в практиката му относно защитата на личните данни. Действително, както отбелязват ирландското правителство и Комисията, този съд е преценил като достатъчно ясни национални законодателства, определящи „тежките“ престъпления, които могат да обосноват намеса в личния живот, позовавайки се на наказание от най-малко три години лишаване от свобода<sup>135</sup>. Независимо от това считам, че той не е въздигнал споменатия размер на наказанието в абсолютен и неизменяем критерий за целите на това определение, като се има предвид, че практиката му според мен се съсредоточава около изискването за достатъчна предвидимост и яснота за гражданите с оглед не толкова на предвиденото наказание, а по-скоро на естеството на престъпленията, които позволяват подобна намеса<sup>136</sup>. Освен това, макар ЕСПЧ да признава на държавите определена свобода на преценка относно наличието и обхвата на необходимостта от подобна намеса, той все пак подчинява тази свобода на преценка на контрол, упражняван на европейско равнище<sup>137</sup>. По-специално той следи да не се допуска риск от злоупотреби в резултат от законодателства, препращащи към толкова широк списък от престъпления, че в крайна сметка водят до възможността повечето престъпления да могат да обосноват налагането на ограничителни мерки<sup>138</sup>.

121. В заключение считам, че ако Съдът постанови — в разрез с това, което препоръчвам — че за да се квалифицира престъплението като „тежко“ по смисъла на неговата практика, установена с решение *Digital Rights*, следва да се отчита единствено предвиденото наказание, на втория преюдициален въпрос би следвало да се отговори, че държавите членки са свободни да определят минималния размер на съответното наказание за целта, стига да спазват изискванията, произтичащи от правото на Съюза, и по-специално онези изисквания, съгласно които намесата в основните права, гарантирани с членове 7 и 8 от Хартата, трябва да остане изключение и да бъде съобразена с принципа на пропорционалност.

## V. Заключение

122. С оглед на изложените съображения предлагам на Съда да отговори на поставените от *Audiencia Provincial de Tarragona* (съд на провинция Тарагона, Испания) преюдициални въпроси по следния начин:

„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 и 8 и член 52, параграф 1 от Хартата на основните права на Европейския съюз, трябва да се тълкува в смисъл, че мярка, която за целите на борбата с престъпленията дава на компетентните национални органи достъп до идентификационните данни на ползвателите на телефонни номера, активирани с определен мобилен телефон през ограничен период, при обстоятелства като разглежданите в главното производство води до намеса в

135 Вж. в този смисъл ЕСПЧ, 18 май 2010 г., *Kennedy c/y Обединено кралство* (СЕ:ЕCHR:2010:0518JUD002683905, §§ 34 и 159) и ЕСПЧ, 4 декември 2015 г., *Roman Zakharov c/y Русия* (СЕ:ЕCHR:2015:1204JUD004714306, § 244).

136 Вж. точка 106 от настоящото заключение.

137 Вж. по-специално ЕСПЧ, 6 септември 1978 г., *Klass и др. c/y Германия* (СЕ:ЕCHR:1978:0906JUD000502971, § 49) и ЕСПЧ, 18 май 2010 г., *Kennedy c/y Обединено кралство* (СЕ:ЕCHR:2010:0518JUD002683905, §§ 153 и 154).

138 Вж. ЕСПЧ, 10 февруари 2009 г., *Iordachi и др. c/y Молдова* (СЕ:ЕCHR:2009:0210JUD002519802, § 44), където се приема, че молдовското законодателство се отличава с липса на яснота, по-специално тъй като над половината престъпления, предвидени в Наказателния кодекс, попадат в категорията престъпления, които могат да доведат до мярка, свързана с прихващането на телефонни съобщения. Вж. и ЕСПЧ, 4 декември 2015 г., *Roman Zakharov c/y Русия* (СЕ:ЕCHR:2015:1204JUD004714306, § 248).

гарантираните от споменатата директива и Хартата основни права, която не е толкова сериозна, че да налага такъв достъп да се предоставя само в случаите, в които съответното престъпление е тежко“.