



Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
Н. SAUGMANDSGAARD ØE
представено на 19 юли 2016 година¹

Съединени дела C-203/15 и C-698/15

Tele2 Sverige AB
срещу
Post- och telestyrelsen (C-203/15)
и
Secretary of State for the Home Department
срещу
Tom Watson,
Peter Brice,
Geoffrey Lewis (C-698/15),
в присъствието на
Open Rights Group,
Privacy International,
Law Society of England and Wales

(Преюдициални запитвания, отправени от Kammarrätten i Stockholm (Административен апелативен съд Стокхолм, Швеция) и Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение) (Обединеното кралство)

„Преюдициално запитване — Директива 2002/58/ЕО — Обработка на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните съобщения — Национално законодателство, предвиждащо общо задължение за запазване на данните за електронните съобщения — Член 15, параграф 1 — Хартата на основните права на Европейския съюз — Член 7 — Право на зачитане на личния живот — Член 8 — Право на защита на личните данни — Тежка намеса — Обосновка — Член 52, параграф 1 — Условия — Легитимна цел за борба с тежките престъпления — Изискване за правно основание в националното право — Изискване за строга необходимост — Изискване за пропорционалност в едно демократично общество“

Съдържание

I – Въведение	3
II – Правна уредба	4

¹ — Език на оригиналния текст: френски.

А – Директива 2002/58	4
Б – Шведското право	5
1. По обхвата на задължението за запазване	5
2. По достъпа до запазените данни	6
а) LEK	6
б) RB	6
в) Закон 2012:278	7
3. По периода на запазване на данните	7
4. По защитата и сигурността на запазените данни	7
В – Правото на Обединеното кралство	8
1. По обхвата на задължението за запазване	8
2. По достъпа до запазените данни	9
3. По периода на запазване на данните	10
4. По защитата и сигурността на запазените данни	10
III – Споровете в главните производства и преюдициалните въпроси	11
А – Дело C-203/15	11
Б – Дело C-698/15	12
IV – Производство пред Съда	12
V – Анализ на преюдициалните въпроси	13
А – По допустимостта на втория поставен по дело C-698/15 въпрос	14
Б – По съвместимостта на едно общо задължение за запазване на данни с установения с Директива 2002/58 режим	16
1. По въпроса дали общо задължение за запазване на данни попада в приложното поле на Директива 2002/58	16
2. По възможността да се дерогира установеният с Директива 2002/58 режим чрез установяване на общо задължение за запазване на данни	17
В – По приложимостта на Хартата по отношение на общо задължение за запазване на данни	20
Г – По съвместимостта на общо задължение за запазване на данни с изискванията, установени с член 15, параграф 1 от Директива 2002/58, както и с членове 7 и 8 и член 52, параграф 1 от Хартата	21
1. По наличието на правно основание в националното право	23

2. По зачитането на основното съдържание на признатите с членове 7 и 8 от Хартата права	26
3. По наличието на призната от Съюза цел от общ интерес, която може да обоснове общо задължение за запазване на данни	26
4. По подходящия характер на общо задължение за запазване на данни с оглед на борбата с тежките престъпления	28
5. По необходимия характер на общо задължение за запазване на данни с оглед на борбата с тежките престъпления	30
а) По строго необходимия характер на общо задължение за запазване на данни	31
б) По императивния характер на изложените от Съда в точки 60—68 от решение DRI гаранции с оглед на наличието на строга необходимост	34
6. По пропорционалния характер в демократично общество на общо задължение за запазване на данни с оглед на целта за борба с тежките престъпления	39
VI – Заключение	43

I – Въведение

1. През 1788 г. Джеймс Мадисън, един от създателите на Конституцията на Съединените щати, пише следното: „If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself“².

2. Настоящите дела ме поставят в същината на установеното от Мадисън „голямо затруднение“. Техен предмет е съвместимостта с правото на Съюза на национални режими, въвеждащи за доставчиците на обществено достъпни електронни съобщителни услуги (наричани по-нататък „доставчиците“) задължение за запазване на данните за електронните съобщения (наричани по-нататък „данните за съобщенията“), отнасящо се до всички съобщителни средства и до всички ползватели (наричано по-нататък „общото задължение за запазване на данни“).

3. От една страна, запазването на данните за съобщенията позволява на „управлението да контролира управляваните“, като осигурява на компетентните органи средство за разследване, което в известна степен може да бъде полезно в борбата с тежките престъпления, и по-специално в борбата с тероризма. Запазването на тези данни по същество предоставя на органите ограничена възможност да „четат миналото“, като получат достъп до данните за съобщенията на лице дори отпреди да бъде заподозряно, че има връзка с тежко престъпление³.

2 — „Ако хората бяха ангели, не би имало нужда от управление. Ако хората бяха управлявани от ангели, не би бил нужен какъвто и да е външен или вътрешен контрол над управлението. При открояването на границите на управлението, упражнявано от хора спрямо хора, голямото затруднение се състои в следното: първо трябва да се даде възможност на управлението да контролира управляваните; след това то трябва да бъде задължено да контролира само себе си“: *Madison, J. Federalist № 51.* — in *Hamilton, A., Madison, J. et Jay, J., ed. Genovese, M. A. The Federalist Papers.* Palsgrave Macmillan, New York 2009, p. 120 (свободен превод). Мадисън е един от основните създатели и един от 39-имата подписали Конституцията на Съединените щати (1787). Впоследствие става четвъртият президент на САЩ (1809—1817).

3 — Тази ограничена възможност да „четат миналото“ може по-специално да се окаже от много голяма полза с цел установяване на самоличността на евентуални съучастници: вж. т. 178—184 от настоящото заключение.

4. От друга страна обаче е наложително „управлението да бъде задължено да контролира само себе си“ по отношение както на запазването на данни, така и на достъпа до вече запазените данни, с оглед на сериозните рискове, свързани с наличието на такива бази данни, обхващащи всички осъществени на националната територия съобщения. Всъщност тези изключително големи бази данни предоставят на всяко имащо достъп до тях лице възможността незабавно да каталогизира цялото релевантно население⁴. Тези рискове трябва да бъдат внимателно разглеждани по-специално чрез анализ на строгата необходимост и пропорционалност на общо задължение за запазване на данни като разглежданото в спора по всяко едно от главните производства.

5. Така в рамките на настоящите дела Съдът и запитващите юрисдикции трябва да определят точка на равновесие между задължението на държавите членки да гарантират сигурността на намиращите се на тяхната територия лица и зачитането на основните права на личен живот и на защита на личните данни, признати с членове 7 и 8 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“).

6. Именно в светлината на това „голямо затруднение“ ще разгледам поставените на Съда в настоящите дела въпроси. Те по-конкретно се отнасят до съвместимостта на установяващи общо задължение за запазване на данни национални режими с Директива 2002/58/ЕО⁵, както и с членове 7 и 8 от Хартата. За да отговори на тези въпроси, Съдът ще трябва по-специално да уточни какво тълкуване следва да се даде в национален контекст на решение Digital Rights Ireland и др. (наричано по-нататък „решение DRI“)⁶, в което големият състав на Съда приема за невалидна Директива 2006/24/ЕО⁷.

7. Поради мотивите, които ще изложа по-долу, имам впечатлението, че наложено от държава членка общо задължение за запазване на данни може да бъде съвместимо с признатите в правото на Съюза основни права, при условие че е строго ограничено с поредица от гаранции, които ще установя в хода на изложението си.

II – Правна уредба

A – Директива 2002/58

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

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

4 — Вж. т. 252—261 от настоящото заключение.

5 — Директива на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. (ОВ L 337, 2009 г., стр. 11 и поправка в ОВ L 241, 2013 г., стр. 9).

6 — Решение от 8 април 2014 г. (C-293/12 и C-594/12, EU:C:2014:238).

7 — Директива 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).

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

3. Настоящата директива не се прилага за дейности, които попадат извън обхвата на [ДФЕС], като тези[,] обхванати от дялове V и VI от [ДЕС], 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“.

9. Член 15, параграф 1 от Директива 2002/58, озаглавен „Приложение на някои разпоредби от Директива [95/46]“, гласи следното:

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

Б – Шведското право

10. Директива 2006/24, понастоящем приета за невалидна, е транспонирана в шведското право с изменения, внесени в Lagen (2003:389) om elektronisk kommunikation (шведския Закон 2003:389 за електронните съобщения, наричан по-нататък „ЛЕК“) и във Förordningen (2003:396) om elektronisk kommunikation (Наредба 2003:396 за електронните съобщения, наричана по-нататък „FEK“) — текстове, влезли в сила на 1 май 2012 г.

1. По обхвата на задължението за запазване

11. От разпоредбите на глава 6, член 16а от LEK е видно, че доставчиците са длъжни да запазват данните за съобщенията, необходими за идентифициране на източника и местоназначението на съобщението, с цел определяне на неговата дата, време, продължителност и вид и с цел установяване на използваното съобщително оборудване и локализиране на местонахождението на използваното мобилно съобщително оборудване в началото и в края на съобщението. Видовете данни, които следва да се запазват, са предмет на по-подробни разпоредби в членове 38—43 от FEK.

12. Задължението за запазване се прилага за данни, обработени при предоставянето на телефонни услуги, мобилна телефония, система изпращане на електронни съобщения, достъп до интернет, както и при предоставянето на възможност за достъп до интернет.

13. Сред данните, които следва да се запазват, попадат не само тези, за които има такова задължение по Директива 2006/24, но и данните за неуспешни повиквания, както и за местонахождението, където е прекратена мобилната връзка. По подобие на предвидения с тази директива режим задължението за запазване не се отнася за данни, разкриващи съдържанието на съобщенията.

2. По достъпа до запазените данни

14. Достъпът до запазените данни се урежда от три текста, а именно LEK, rättegångsbalken (Съдопроизводствен кодекс, наричан по-нататък „RB“) и lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (шведски Закон 2012:278 за предоставяне на данни за електронни съобщения в хода на разузнавателни действия на правоприлагащи органи).

а) LEK

15. Съгласно разпоредбите на глава 6, член 22, първа алинея, точка 2 от LEK при поискване доставчикът е длъжен да предаде данните за абонати на органа за съдебно преследване, полицията, Säkerhetspolisen (шведската Служба за сигурност, наричана по-нататък „Säpo“) или друг правоприлагащ орган, ако въпросните данни са свързани с подозрение за извършено престъпление. Съгласно тези разпоредби не е наложително да става въпрос за извършване на тежко престъпление.

16. Понятието за данни за абонати се отнася преди всичко до данни за име, длъжност, пощенски адрес, телефонен номер и IP адрес.

17. По силата на LEK предаването на данни за абонати не изисква никакъв предварителен контрол, но може да бъде предмет на последващ административен контрол. Освен това броят на органите, които могат да имат достъп до данните, не е ограничен.

б) RB

18. RB урежда случаите на наблюдение на електронни съобщения в хода на предварително разследване.

19. По същество поставяне под наблюдение на електронни съобщения може да се разпорежда единствено когато може разумно да се подозира, че лице е извършител на престъпление, за което се предвижда наказание лишаване от свобода най-малко шест месеца, или на други конкретно изброени престъпления, ако тази мярка е от съществено значение за разследването.

20. Освен при тези случаи наблюдение може да се извършва за целите на разследване на престъпление, за което се предвижда наказание лишаване от свобода най-малко две години, за да се установи кой би могъл разумно да се подозира в неговото извършване, ако тази мярка е от съществено значение за нуждите на разследването.

21. Съгласно глава 27, член 21 от RB прокурорът по принцип трябва да получи разрешение от компетентния съдия, преди да постави под наблюдение електронни съобщения.

22. Ако обаче получаването на съдебно разрешение за наблюдение на електронни съобщения може да доведе до забавяне или друго затруднение от решаващо значение за разследването, прокурорът може да даде разрешение за мярката до произнасянето на решението на съда. Прокурорът трябва незабавно да уведоми писмено съда за мярката. Компетентният съд следва своевременно да провери дали мярката е обоснована.

в) Закон 2012:278

23. В рамките на събирането на сведения и в приложение на член 1 от Закон 2012:278 националната полиция, Säpo и Tullverket (шведската митническа администрация) могат при предписаните в този закон условия и без знанието на доставчика да започнат събирането на данни за съобщенията.

24. Съгласно членове 2 и 3 от Закон 2012:278 данните могат да се събират, ако с оглед на обстоятелствата мярката е от особено необходима за предотвратяване, възпрепятстване или разкриване на престъпна дейност по осъществяване на едно или няколко престъпления, за които е предвидено наказание лишаване от свобода не по-малко от две години, или престъпление, посочено в член 3 (отнасящ се по-специално до различните форми на саботажи и шпионажи).

25. Решението за предприемане на такава мярка се взема от ръководителя на съответния орган или от служител, на когото той е делегирал правомощия за целта.

26. Решението трябва да съдържа информация за престъпната дейност и съответния период, както и за телефонния номер, друг адрес, оборудване за електронни съобщения или географския му обхват. Периодът на разрешението не може да е по-дълъг от необходимото, като периодът след решението не може да надхвърля един месец.

27. Този вид мерки не изисква предварителен контрол. Съгласно член 6 от Закон 2012:278 обаче Säkerhets- och integritetsskyddsnämnden (Комисия по сигурност и защита на интегритета, Швеция) трябва да бъде информирана за всяко решение за събиране на данни. Съгласно член 1 от lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (Закон 2007:980 за надзор върху някои дейности по правоприлагане) този орган трябва да упражнява надзор върху прилагането на закона от страна на правоприлагащите органи.

3. По периода на запазване на данните

28. От разпоредбите на глава 6, член 16d от LEK е видно, че данните, посочени в член 16a от същата глава, се запазват за период от шест месеца, считано от деня на прекратяване на съобщението. След това те трябва да се унищожат незабавно, освен ако в член 16d, втора алинея (от глава 6) от LEK не е предвидено друго. Съгласно последните разпоредби данни, които са поискани преди края на периода на запазване, но все още не са предадени, трябва да се унищожат веднага след предаването.

4. По защитата и сигурността на запазените данни

29. Глава 6, член 20, първа алинея от LEK забранява на всяко лице разпространяването или използването без разрешение на данните за съобщенията.

30. Съгласно разпоредбите на глава 6, член 3а от LEK доставчиците трябва да вземат специални технически и организационни мерки, необходими за защита на данните в хода на тяхната обработка. Видно от подготвителните работи по приемането на тези разпоредби, не се разрешава равнището на защита да се определя като плод на компромис между съображения, свързани с технологиите, с разходите и с рисковете от хакерски посегателства и от нарушаване на неприкосновеността на личния живот.

31. Допълнителни правила относно защитата на данните се съдържат в член 37 от FEK, както и в наредбите и общите препоръки на Post- och telestyrelsen (шведският Комитет по пощи и далекосъобщения, наричан по-нататък „PTS“) относно мерките за защита при запазване и обработка на данни за целите на борбата с престъпността (PTSFS № 2012:4). В посочените наредби се предвижда по-специално задължение на доставчиците да предприемат мерки, за да се защитят данните от неволно или незаконно унищожаване, от незаконно запазване, обработка или достъп и незаконно разкриване. Доставчиците са задължени също да осъществяват непрекъснати и систематични дейности по сигурността на данните с оглед на специфичните рискове, свързани със задължението за запазване.

32. Шведското законодателство не съдържа разпоредби относно мястото, където трябва да се запазват данните.

33. Съгласно глава 7 от LEK регулаторният орган е оправомощен в случай на неизпълнение на задължение от страна на доставчик да издава заповеди и забрани, които могат да съдържат и санкции, както и да разпорежда цялостно или частично прекратяване на дейността.

В – Правото на Обединеното кралство

34. Разпоредбите, уреждащи запазването на данните, се съдържат в Data Retention and Investigatory Powers Act 2014 (Законът от 2014 г. относно запазването на данните и правомощията по разследване, наричан по-нататък „DRIPA“), в Data Retention Regulations 2014 (SI 2014/2042) (Наредба от 2014 г. относно запазването на данните, наричана по-нататък „Наредбата от 2014 г.“), както и в Retention of Communications [Data] Code of Practice (Кодекс за добри практики относно запазването на данните).

35. Разпоредбите, уреждащи достъпа до данните, се съдържат в част 1, глава 2 от Regulation of Investigatory Powers Act 2000 (Закон от 2000 г. за уреждане на правомощията по разследване, наричан по-нататък „RIPA“), в Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) (Разпореждане от 2010 г. за уреждане на правомощията по разследване в областта на данните за съобщенията), изменено с Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015 (SI 2015/228), както и в Acquisition and Disclosure of Communications Data Code of Practice (Кодекс за добри практики относно получаването и разкриването на данните за съобщенията, наричан по-нататък „Кодексът относно получаването на данните“).

1. По обхвата на задължението за запазване

36. Съгласно раздел 1 от DRIPA Secretary of State for the Home Department (министърът на вътрешните работи на Обединеното кралство, наричан по-нататък „министърът“) може да наложи на доставчиците задължение да запазват всички данни за съобщенията. Това задължение по същество може да засегне всички данни, създадени във връзка със съобщение, пренесено чрез пощенска услуга или далекосъобщителна система, с изключение на съдържанието на съобщението. Тези данни включват по-специално местонахождението на ползвателя на услугата, както и данните, позволяващи да се определи IP адресът (по интернет протокол), или всеки друг идентификатор на изпращача или получателя на съобщението.

37. Сред целите, които могат да обосноват приемането на такава мярка за запазване, са интересите на националната сигурност, предотвратяването или разкриването на престъпления или предотвратяването на нарушаването на обществения ред, интересите, свързани с икономическото благосъстояние на Обединеното кралство, стига тези интереси да са релевантни и за националната сигурност, интересите на обществената сигурност, защитата на общественото здраве, определянето на данъчната основа или събирането на всякакви данъци, вноски или други дължими към публичната администрация суми, предотвратяване на уврежданията на физическото и психическото здраве в случаите на неотложност, сътрудничеството в разследванията на случаи на съдебни грешки, установяването на самоличността на починало лице или на такова, което не е в състояние да направи това само по друг начин, освен вследствие на престъпно или неправомерно деяние (като в случай на природно бедствие или произшествие), упражняването на функции, свързани с уреждането на финансовите услуги и пазари или на финансовата стабилност, както и всяка друга цел, уточнена в установено от министъра разпореждане по силата на раздел 22(2) от DRIPA.

38. Националното законодателство не предвижда изискване, за да бъде приет акт, разпореждащ запазване, да има предварително разрешение от съд или от независимо образувание. Министърът трябва да провери дали задължението за запазване е „необходимо и пропорционално“ с оглед на една или повече цели, за които релевантните данни за съобщенията могат да бъдат запазени.

2. По достъпа до запазените данни

39. Съгласно раздел 22(4) от RIPA публичните органи могат, по силата на акт, да изискват от доставчиците да им разкриват данни за съобщенията. Формата и съдържанието на тези актове са уредени в раздел 23(2) от RIPA. Актовете са ограничени времево посредством разпоредби за тяхната отмяна и подновяване.

40. Получаването на данните за съобщенията трябва да е необходимо и пропорционално с оглед на една или повече от съдържащите се в раздел 22 от RIPA цели, съответстващи на целите, които могат да обосноват запазването на данните, описани в точка 37 от настоящото заключение.

41. От Кодекса относно получаването на данните е видно, че се изисква разпореждане на юрисдикция при искане на достъп, направено с оглед на установяването на журналистически източник, както и в случай на отправено от местни органи искане на достъп.

42. Извън тези хипотези достъпът на публичните органи е подчинен на получаването на разрешение, дадено от лицата, определени за тази цел в рамките на съответния публичен орган. Определено за тази цел лице е лице, изпълняващо установена в рамките на съответния публичен орган функция, степен или длъжност и определено с цел получаване на данните за съобщенията в съответствие с Разпореждането от 2015 г. за уреждане на правомощията по разследване в областта на данните за съобщенията, изменено.

43. Никакво съдебно разрешение или такова на независимо образувание не се изисква конкретно по отношение на достъпа до защитени с професионална тайна данни за съобщенията или до такива, отнасящи се до лекари, членове на Парламента или свещенослужители. В Кодекса относно получаването на данните само се уточнява, че трябва да се обърне особено внимание на необходимостта и пропорционалността на искането на достъп до такива данни.

3. По периода на запазване на данните

44. Раздел 1(5) от DRIPA и разпоредба 4(2) на Наредбата от 2014 г. предвиждат максимален период на запазване на данните от дванадесет месеца. Съгласно Кодекса за добри практики относно запазването на данните периодът трябва да е само толкова дълъг, колкото е необходимо и пропорционално. Разпоредба 6 от Наредбата от 2014 г. изисква от министъра да извършва преразглеждане на актовете, разпореждащи запазването.

4. По защитата и сигурността на запазените данни

45. В приложение на раздел 1 от DRIPA на доставчиците е забранено на разкриват запазените данни, освен ако това разкриване не е в съответствие с част 1, глава 2 от RIPA, със съдебно решение или с каквото и да е друго съдебно разрешение или заповед, или пък с приета от министъра наредба в приложение на раздел 1 от DRIPA.

46. Съгласно разпоредби 7 и 8 от Наредбата от 2014 г. доставчиците трябва да осигурят целостта и сигурността на запазените данни; да ги защитят от случайно или неправомерно унищожаване, случайна загуба или промяна или от неразрешено или неправомерно запазване, обработване, достъп или разкриване; да унищожават данните, така че да е невъзможен достъпът до тях, ако запазването им престане да бъде разрешено; и да въведат системи за сигурност. Разпоредба 9 от Наредбата от 2014 г. вменява на Information Commissioner (комисар по информацията) да проверява запазването на тези задължения от доставчиците.

47. Органите, на които доставчиците предоставят данни за съобщенията, трябва да обработват и запазват по сигурен начин тези данни, както и всички техни копия, извлечения или резюмета. Съгласно Кодекса относно получаването на данните трябва да бъдат спазвани изискванията, съдържащи се в Закона за защита на данните (Data Protection Act, наричан по-нататък „DPA“), с който е транспонирана Директива 95/46.

48. RIPA въвежда Interception of Communications Commissioner (комисарят по прихващане на съобщенията, наричан по-нататък „комисарят по прихващане“), отговарящ за осъществяване на независим надзор върху упражняването и изпълнението на правомощията и задълженията, съдържащи се в част 1, глава II от RIPA. Комисарят по прихващане не извършва надзор върху прилагането на раздел 1 от DRIPA. Той редовно трябва да представя доклади пред обществеността и Парламента (раздел 57(2) и раздел 58 от RIPA) и да посочва какво е запазено и отчетено от публичните органи (Кодекс относно получаването на данните, параграфи 6.1—6.8). Могат да бъдат подавани и жалби пред Investigatory Powers Tribunal (специализиран съд по въпросите на разузнавателните средства), ако има основание да се смята, че данни са били получени по неподходящ начин (раздел 65 от RIPA).

49. От Кодекса относно получаването на данните е видно, че Комисарят по прихващане няма право да сезира посочения съд. Разрешено му е единствено да уведоми лице, че има подозрения за неправомерно използване на компетентност, ако може да „установи, че дадено физическо лице е пострадало вследствие от нарушение, извършено умишлено или поради небрежност“. На Комисаря обаче не е разрешено да разкрива информация, ако това би създавало опасност за националната сигурност, дори и да счита, че е имало нарушение, извършено умишлено или поради небрежност.

III – Споровете в главните производства и преюдициалните въпроси

A – Дело C-203/15

50. На 9 април 2014 г., тоест в деня след постановяването на решение DRI, Tele2 Sverige уведомява PTS за решението си да прекрати запазването на предвидените в глава 6 от LEK данни. Tele2 Sverige щяло да изтрие и вече запазените в приложение на тази глава данни. Според Tele2 Sverige шведското законодателство, транспониращо Директива 2006/24, не е в съответствие с Хартата.

51. На 15 април 2014 г. Rikspolisstyrelsen (Генерална дирекция на националната полиция, наричана по-нататък „RPS“) сезира PTS с жалба, че Tele2 Sverige е спряло да предоставя на службите ѝ данни за някои електронни съобщения. В жалбата си RPS изтъква, че отказът на Tele2 Sverige има сериозни последици за правоприлагащата дейност на полицията.

52. С разпореждане от 27 юни 2014 г. PTS нарежда на Tele2 Sverige да пристъпи към запазване на данните в съответствие с глава 6, член 16а от LEK и членове 37—43 от FEK, не по-късно от 25 юли 2014 г.

53. Tele2 Sverige обжалва решението на PTS пред Förvaltningsrätten i Stockholm (Административен съд Стокхолм, Швеция). С решение от 13 октомври 2014 г. този съд отхвърля жалбата.

54. Tele2 Sverige обжалва решението на Förvaltningsrätten i Stockholm пред запитващата юрисдикция с цел отмяната на спорното решение.

55. Констатирайки, че съществуват доводи както в подкрепа, така и срещу съвместимостта на задължение за запазване на толкова голям обем от данни, като предвидения в глава 6, член 16а от LEK, с разпоредбите на член 15, параграф 1 от Директива 2002/58 и на членове 7 и 8 и член 52, параграф 1 от Хартата, Kammarrätten i Stockholm (Апелативен административен съд Стокхолм, Швеция) решава да спре производството и да постави на Съда следните преюдициални въпроси:

- „1) Съвместимо ли е общо задължение за запазване на данни — което се отнася до всички лица, всички електронни съобщителни средства и всички данни за трафик без никакво разграничаване, ограничаване или изключение за целите на борбата с престъпността [като описаната в точки 13—18 от акта за преюдициално запитване] — с член 15, параграф 1 от Директива 2002/58 с оглед на членове 7 и 8 и член 52, параграф 1 от Хартата?
- 2) При отрицателен отговор на първия въпрос, може ли все пак такава задължение за запазване да бъде разрешено, при условие че:
 - а) достъпът на националните органи до запазените данни е установен съгласно уточнения в точки 19—36 [от акта за преюдициално запитване] начин и
 - б) изискванията за защита и сигурност на данните са уредени съгласно уточнения в точки 38—43 [от акта за преюдициално запитване] начин, и
 - в) всички релевантни данни се запазват за срок от шест месеца, считано от датата на прекратяване на съобщението, и впоследствие се изтриват съгласно изложеното в точка 37 [от акта за преюдициално запитване]?”.

Б – Дело C-698/15

56. Г-н Watson, г-н Brice и г-н Lewis подават пред High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) (Върховен съд (Англия и Уелс), общо гражданско отделение (административен състав) жалби за контрол за законосъобразност („judicial review“) на съдържания се в раздел 1 от DRIPA режим за запазване на данните, оправомощаващ министъра да налага на обществените далекосъобщителни оператори да запазват всички данни за съобщения за максимален период от дванадесет месеца, като се изключва запазването на съдържанието на въпросните съобщения.

57. Open Rights Group, Privacy International и Law Society of England and Wales са допуснати да встъпят по всяка от тези жалби.

58. С решение от 17 юли 2015 г. тази юрисдикция установява, че въпросният режим не е съвместим с правото на Съюза, тъй като не отговаря на поставените с решение DRI изисквания, които тя счита за приложими по отношение на правните уредби на държавите членки в областта на запазването на данните за електронните съобщения и достъпа до такива данни. Министърът обжалва това решение пред запитващата юрисдикция.

59. В решение от 20 ноември 2015 г. Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение), Обединеното кралство) предварително приема, че с решение DRI не се установяват императивни изисквания на правото на Европейския съюз, с които националните законодателства трябва да са в съответствие, а само се открояват и описват видове защита, които не се съдържат в хармонизирания режим на Европейския съюз.

60. Като счита обаче, че отговорите на тези въпроси от правото на Европейския съюз не са ясни, но са необходими, за да се произнесе в посочените производства, Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение) (Обединеното кралство) решава да спре производството и да постави на Съда следните преюдициални въпроси:

- „1) Установява ли решение [DRI] (и конкретно точки 60—62) императивни изисквания на правото на Съюза, приложими по отношение на националния режим на държава членка относно достъпа до запазени в съответствие с националното законодателство данни, за да бъде този режим в съответствие с членове 7 и 8 от [Хартата]?
- 2) Разширява ли решение [DRI] обхвата на членове 7 и/или 8 от Хартата отвъд границите на приложение на член 8 от Европейската конвенция за правата на човека (наричана по-нататък „ЕКПЧ“), определени в практиката на Европейския съд по правата на човека (наричан по-нататък „ЕСПЧ“)“.

IV – Производство пред Съда

61. Преюдициалните запитвания постъпват в секретариата на Съда на 4 май 2015 г. по дело C-203/15 и на 28 декември 2015 г. по дело C-698/15.

62. С определение от 1 февруари 2016 г. Съдът решава да разгледа дело C-698/15 по реда на бързото производство, предвидено в член 105, параграф 1 от неговия процедурен правилник.

63. По дело C-203/15 писмени становища представят Tele2 Sverige, белгийското, чешкото, датското, германското, естонското, ирландското, испанското, френското, унгарското, нидерландското и шведското правителство, правителството на Обединеното кралство и Европейската комисия.

64. По дело C-698/15 писмени становища представят г-н Watson, г-н Brice и г-н Lewis, Open Rights Group, Privacy International, Law Society of England and Wales, чешкото, датското, германското, естонското, ирландското, френското, кипърското, полското и финландското правителство, правителството на Обединеното кралство и Комисията.

65. С решение на Съда от 10 март 2016 г. двете дела са съединени за целите на устната фаза на производството и постановяването на съдебното решение.

66. В съдебното заседание за изслушване на устните състезания на 12 април 2016 г. се явяват представителите на Tele2 Sverige, г-н Watson, г-н Brice и г-н Lewis, Open Rights Group, Privacy International и Law Society of England and Wales, чешкото, датското, германското, естонското, ирландското, испанското, френското, финландското и шведското правителство, правителството на Обединеното кралство и Комисията.

V – Анализ на преюдициалните въпроси

67. С първия въпрос, поставен по дело C-203/15, запитващата юрисдикция иска от Съда да установи дали в светлината на решение DRI член 15, параграф 1 от Директива 2002/58, както и членове 7 и 8 и член 52, параграф 1 от Хартата трябва да се тълкуват в смисъл, че не допускат държава членка да налага на доставчиците общо задължение за запазване на данни като разглежданите в споровете в главните производства, и то независимо дали посоченото задължение е съпътствано от евентуални гаранции.

68. При отрицателен отговор на този въпрос, с втория поставен по дело C-203/15 въпрос и с първия поставен по дело C-698/15 въпрос се иска да се установи дали споменатите разпоредби трябва да се тълкуват в смисъл, че не допускат държава членка да налага на доставчиците общо задължение за запазване на данни, когато това задължение не е съпътствано от всички посочени от Съда в точки 60—68 от решение DRI гаранции за достъпа до данните, периода на запазването им, както и защитата и сигурността им.

69. Тъй като тези три въпроса са тясно свързани, ще ги разгледам заедно по-нататък в изложението си.

70. За сметка на това вторият поставен по дело C-698/15 въпрос се налага да се разгледа отделно. С него запитващата юрисдикция иска от Съда да установи дали решение DRI е разширило приложното поле на членове 7 и/или 8 от Хартата отвъд границите на приложение на член 8 от ЕКПЧ. В следващия раздел ще изложа съображенията, поради които считам, че този въпрос трябва да бъде отхвърлен като недопустим.

71. Преди да пристъпя към анализа на тези въпроси, считам за полезно да напомня какви данни са обхванати от разглежданите в споровете в главните производства задължения за запазване. Съгласно направените от запитващите юрисдикции констатации обхватът на тези задължения по същество е еднакъв с този на задължението по член 5 от Директива 2006/24⁸. Данните за съобщенията, които са предмет на тези задължения за запазване, схематично могат да бъдат разделени в четири категории⁹:

- данни, позволяващи идентифицирането както на източника, така и на местоназначението на съобщението,
- данни, позволяващи локализирането както на източника, така и на местоназначението на съобщението,
- данни, свързани с датата, времето и продължителността на съобщението, и
- данни, позволяващи да се определи видът на съобщението и на използваното оборудване.

72. Също както в член 5, параграф 2 от Директива 2006/24, разглежданите по делата в главните производства общи задължения за запазване на данни не се отнасят до съдържанието на съобщенията.

A – По допустимостта на втория поставен по дело C-698/15 въпрос

73. С втория поставен по дело C-698/15 въпрос от Съда се иска да уточни дали решение DRI разширява приложното поле на членове 7 и/или 8 от Хартата отвъд границите на приложение на член 8 от ЕКПЧ съгласно тълкуването му от ЕСПЧ.

74. Този въпрос по-специално отразява изтъкнат от министъра пред запитващата юрисдикция довод, съгласно който практиката на ЕСПЧ не изисква, от една страна, достъпът до данните да подлежи на предварително разрешение от независим орган, нито, от друга страна, запазването и достъпът до тези данни да бъдат ограничени само за целите на борбата с тежките престъпления.

75. Считам, че този въпрос трябва да бъде отхвърлен като недопустим поради следните съображения. Очевидно е, че постановеното от Съда решение DRI и изложените в него мотиви са от определящо значение за решаването на споровете в главните производства. При все това обаче евентуално разширяване с това решение на приложното поле на членове 7 и/или 8 от Хартата отвъд границите на приложение на член 8 от ЕКПЧ само по себе си е ирелевантно за решаването на тези спорове.

76. В това отношение е важно да се припомни, че в съответствие с член 6, параграф 3 ДЕС основните права, както са гарантирани от ЕКПЧ, са част от правото на Съюза в качеството им на общи принципи. Въпреки това, докато Съюзът не се присъедини към тази конвенция, тя не представлява юридически акт, формално интегриран в правния ред на Съюза¹⁰.

8 — Тази еднаквост е разбираема, тъй като въпросните национални режими имат за цел да транспонират понастоящем обявената за невалидна директива.

9 — Вж. описанието на разглежданите в споровете в главните производства национални режими в т. 11—13 и 36 от настоящото заключение.

10 — Становище 2/13 от 18 декември 2014 г. (EU:C:2014:2454, т. 179) и решение от 15 февруари 2016 г., N. (C-601/15 PPU, EU:C:2016:84, т. 45 и цитираната съдебна практика).

77. Действително, първото изречение на член 52, параграф 3 от Хартата установява тълкувателно правило, съгласно което, доколкото Хартата съдържа права, съответстващи на права, гарантирани от ЕКПЧ, „техният смисъл и обхват са същите като дадените им в посочената Конвенция“.

78. Съгласно второто изречение на член 52, параграф 3 от Хартата обаче „[т]ази разпоредба не пречи правото на Съюза да предоставя по-широка защита“. От това изречение според мен следва, че на Съда е позволено, ако сметне за необходимо в контекста на правото на Съюза, да разшири приложното поле на разпоредбите на Хартата отвъд границите на приложение на съответстващите разпоредби на ЕКПЧ.

79. При условията на евентуалност ще добавя, че член 8 от Хартата, тълкуван от Съда в решение DRI, установява право, което не съответства на никое гарантирано с ЕКПЧ право — а именно правото на защита на личните данни, като това се потвърждава и от разясненията относно член 52 от Хартата¹¹. Следователно установеното в член 52, параграф 3, първо изречение от Хартата тълкувателно правило при всички случаи не е приложимо за тълкуването на член 8 от Хартата, както изтъкват г-н Brice и г-н Lewis, Open Rights Group и Privacy International, Law Society of England and Wales, както и чешкото, ирландското и финландското правителство.

80. От гореизложеното следва, че правото на Съюза допуска членове 7 и 8 от Хартата да предоставят по-широка защита от предвидената в ЕКПЧ. Следователно обстоятелството, че решение DRI евентуално е разширило приложното поле на тези разпоредби на Хартата отвъд границите на приложение на член 8 от ЕКПЧ, само по себе си не е релевантно за решаването на споровете в главните производства. Разрешаването на тези спорове зависи главно от условията, при които общо задължение за запазване на данни може да се счете за съвместимо с член 15, параграф 1 от Директива 2002/58, както и с членове 7 и 8 и член 52, параграф 1 от Хартата, тълкувани в светлината на решение DRI — нещо, което е предмет именно на другите три въпроса по настоящите дела.

81. Съгласно постоянната съдебна практика отправеното от национална юрисдикция запитване може да се отхвърли само ако е съвсем очевидно, че исканото тълкуване на правото на Съюза няма никаква връзка с действителността или с предмета на спора по главното производство или още когато проблемът е от хипотетично естество или ако Съдът не разполага с необходимите данни от фактическа и правна страна, за да бъде полезен с отговора на поставените му въпроси¹².

82. В случая и поради изложените по-горе мотиви ми се струва, че вторият поставен по дело C-698/15 въпрос е само от теоретичен интерес, тъй като евентуален отговор по него не би позволил да се изведат насоки за тълкуване на правото на Съюза, които биха помогнали на запитващата юрисдикция да реши въз основа на това право висящия пред нея спор¹³.

83. При тези условия считам, че въпросът трябва да бъде отхвърлен като недопустим, както правилно изтъкват г-н Watson, Law Society of England and Wales и чешкото правителство.

11 — Съгласно член 6, параграф 1, трета алинея ДЕС и член 52, параграф 7 от Хартата разясненията по нея трябва да се вземат предвид при тълкуването ѝ (вж. решения от 26 февруари 2013 г., Åkerberg Fransson, C-617/10, EU:C:2013:105, т. 20 и от 15 февруари 2016 г., N., C-601/15 PPU, EU:C:2016:84, т. 47). Съгласно тези разяснения член 7 от Хартата съответства на член 8 от ЕКПЧ, а член 8 от нея не съответства на никакво право от последната.

12 — Вж. по-специално решения от 9 ноември 2010 г., Volker und Markus Schecke и Eifert (C-92/09 и C-93/09, EU:C:2010:662, т. 40 и цитираната съдебна практика), както и от 24 април 2012 г., Kamberaj (C-571/10, EU:C:2012:233, т. 42 и цитираната съдебна практика).

13 — Вж. по-специално решение от 16 септември 1982 г., Vlaeminck (132/81, EU:C:1982:294, т. 13), определение от 24 март 2011 г., Abt и др. (C-194/10, EU:C:2011:182, т. 36 и 37 и цитираната съдебна практика) и решение от 24 октомври 2013 г., Стоилов и Ко (C-180/12, EU:C:2013:693, т. 46 и цитираната съдебна практика).

Б – По съвместимостта на едно общо задължение за запазване на данни с установения с Директива 2002/58 режим

84. В настоящия раздел се разглежда дали държавите членки могат да използват предоставената им с член 15, параграф 1 от Директива 2002/58 възможност, за да наложат общо задължение за запазване на данни. В раздела обаче не се разглеждат конкретните изисквания, които трябва да бъдат изпълнени от държавите членки, желаещи да използват тази възможност, като те ще бъдат подробно анализирани в последващ раздел¹⁴.

85. Всъщност Open Rights Group и Privacy International изтъкват, че такова задължение е несъвместимо с установения с Директива 2002/58 хармонизиран режим, при това независимо дали са спазени изискванията по член 15, параграф 1 от същата директива, тъй като то би обезсмислило установените с нея права и режим.

86. Преди да бъде разгледан този довод, следва да се провери дали общо задължение за запазване на данни попада в приложното поле на тази директива.

1. По въпроса дали общо задължение за запазване на данни попада в приложното поле на Директива 2002/58

87. Някоя от страните, представили становища пред Съда, не оспорва факта, че общо задължение за запазване на данни като разглежданите в споровете в главните производства попада в обхвата на понятието „обработка[...] на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в [Съюза]“ по смисъла на член 3 от Директива 2002/58.

88. При все това чешкото, френското и полското правителство и правителството на Обединеното кралство поддържат, че общо задължение за запазване на данни попада в обхвата на изключението по член 1, параграф 3 от Директива 2002/58. От една страна, националните разпоредби, уреждащи достъпа до данните и тяхното използване от полицейските или съдебните органи на държавите членки, се отнасяли до обществената сигурност, отбраната или сигурността на държавата или най-малкото до областта на наказателното право. От друга страна, самата цел на запазването на данните била да се позволи на тези полицейски или съдебни органи да имат достъп до тях и да ги използват. Съгласно цитираната разпоредба следователно задължение за запазване на данни не попадало в приложното поле на Директивата.

89. Тази обосновка не е убедителна за мен поради следните мотиви.

90. На първо място, самият текст на член 15, параграф 1 от Директива 2002/58 потвърждава, че наложените от държавите членки задължения за запазване попадат в приложното ѝ поле. Съгласно тази разпоредба всъщност „държавите членки могат, *inter alia*, да одобряват законодателни мерки, предвиждащи [запазването] на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф“. Най-малкото ми се струва трудно да се поддържа, че задълженията за запазване са изключени от приложното поле на тази директива, при положение че член 15, параграф 1 от нея урежда възможността за приемане на такива задължения.

14 — Вж. т. 126—262 от настоящото заключение.

91. Всъщност, както изтъкват и г-н Watson, г-н Brice, г-н Lewis, белгийското, датското, германското, финландското правителство и Комисията, общо задължение за запазване на данни като разглежданите в споровете в главните производства представлява прилагане на член 15, параграф 1 от Директива 2002/58.

92. На второ място, това, че разпоредбите, уреждащи достъпа, могат да попадат в обхвата на установеното в член 1, параграф 3 от Директива 2002/58 изключение¹⁵, не налага задължението за запазване също да попада в него и следователно да излиза извън приложното поле на тази директива.

93. В това отношение Съдът вече е имал възможността да уточни, че упоменатите в член 3, параграф 2, първо тире от Директива 95/46/ЕО дейности¹⁶, чийто текст е с обхват, еднакъв с този на член 1, параграф 3 от Директива 2002/58, са присъщи на държавите или на държавните органи и не се отнасят до областите на дейност на частноправните субекти¹⁷.

94. Разглежданите в споровете в главните производства задължения за запазване обаче са наложени на частни оператори в рамките на частни дейности по предоставяне на електронни съобщителни услуги, както изтъква Комисията. Освен това въпросните задължения се налагат независимо от каквото и да е искане на достъп от страна на полицейските или съдебните органи, както и, по-общо, на каквото и да е акт на държавните органи, отнасящ се до обществената сигурност, отбраната, сигурността на държавата или до наказателното право.

95. На трето място, приетото от Съда в решение Ирландия/Парламент и Съвет потвърждава, че едно задължение за запазване на данни не попада в наказателноправната област¹⁸. Съдът всъщност приема, че Директива 2006/24, която установява такова задължение, не се отнася до наказателноправната област, а до функционирането на вътрешния пазар, така че член 95 ЕО (понастоящем член 114 ДФЕС) представлява подходящото правно основание за нейното приемане.

96. За да стигне до този извод, Съдът по-специално установява, че разпоредбите на тази директива се ограничават основно до дейността на доставчиците и не уреждат достъпа до данни, нито тяхното използване от полицейските или съдебните органи на държавите членки¹⁹. От това заключавам, че разпоредби на националното право, установяващи задължение за запазване, подобно на предвиденото с Директива 2006/24, също не се отнасят до наказателноправната област.

97. С оглед на гореизложеното съм на мнение, че общо задължение за запазване на данни не попада в приложното поле на установеното в член 1, параграф 3 от Директива 2002/58 изключение, а следователно в това на самата директива.

2. По възможността да се дерогира установеният с Директива 2002/58 режим чрез установяване на общо задължение за запазване на данни

98. Тук е моментът да се определи дали общо задължение за запазване на данни е съвместимо с установения с Директива 2002/58 режим.

15 — Вж. т. 123—125 от настоящото заключение.

16 — 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).

17 — Решение от 6 ноември 2003 г., Lindqvist (C-101/01, EU:C:2003:596, т. 43 и 44).

18 — Решение от 10 февруари 2009 г. (C-301/06, EU:C:2009:68).

19 — Решение от 10 февруари 2009 г., Ирландия/Парламент и Съвет (C-301/06, EU:C:2009:68, т. 80).

99. Въпросът, който възниква в това отношение, е дали държава членка може да използва предоставената с член 15, параграф 1 от Директива 2002/58 възможност с цел налагане на такова задължение.

100. Четири довода са изтъкнати срещу такава възможност, по-специално от страна на Open Rights Group и Privacy International.

101. Съгласно първия довод предоставянето на държавите членки на правомощието да приемат общо задължение за запазване на данни щяло да постави под въпрос целта за хармонизиране, с оглед на която всъщност била приета Директива 2002/58. Член 1, параграф 1 от нея предвиждал 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 сектора на електронните комуникации и да се осигури свободно движение на такива данни и оборуване за електронни съобщения и услуги в Съюза.

102. Ето защо член 15, параграф 1 от Директива 2002/58 не можел да се тълкува в смисъл, че предоставя на държавите членки право да приемат толкова значимо изключение от установения с Директивата режим, че усилието за хармонизиране да бъде лишено от каквото и да е полезно действие.

103. Според втория довод текстът на член 15, параграф 1 от Директива 2002/58 не допускал и също толкова широко тълкуване на правомощието на държавите членки да правят изключение от установения с Директивата режим. Съгласно тази разпоредба всъщност „[д]ържавите членки могат да приемат законодателни мерки, за да *ограничат обхвата* на правата и задълженията, предвидени в членове 5 и 6, член 8, параграф[и] 1, 2, 3[...] и 4 и член 9 от [тази] директива“ (курсивът е мой).

104. Общо задължение за запазване на данни обаче нямало да се сведе до „ограничаване на обхвата“ на упоменатите в тази разпоредба права и задължения, а щяло да ги стесни до тяхното заличаване. Същото се отнасяло и до:

- задължението да се гарантира поверителността на данните за трафика и задължението съхраняването на информацията да бъде подчинено на съгласието на ползвателя, предвидени съответно в член 5, параграфи 1 и 3 от Директива 2002/58,
- задължението за изтриване или анонимизиране на данните за трафика, вписано в член 6, параграф 1 от тази директива, и
- задължението за анонимизиране на данните за местонахождението или за получаване на съгласието на ползвателя за обработването на тези данни, наложено с член 9, параграф 1 от Директивата.

105. Струва ми се, че тези първи два довода трябва да бъдат отхвърлени поради следните мотиви.

106. От една страна, в текста на член 15, параграф 1 от Директива 2002/58 е посочена възможността държавите членки да одобрят „законодателни мерки, предвиждащи [запазването] на данни за ограничен период“. Това изрично посочване на задълженията за запазване на данни потвърждава, че сами по себе си те не са несъвместими с установения с Директива 2002/58 режим. Макар формулировката да не предвижда изрично възможността за приемане на *общо* задължение за запазване на данни, налага се изводът, че в нея също така не се съдържа и забрана за тях.

107. От друга страна, в съображение 11 от Директива 2002/58 се уточнява, че 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 [тази] директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право“. Следователно „директива[та] не засяга възможността на държавите членки да провеждат законно прихващане на електронни [съобщения] или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с [ЕКПЧ]“.

108. От това съображение 11 според мен следва, че намерението на законодателя на Съюза не е било да накърнява възможността на държавите членки да приемат предвидените в член 15, параграф 1 от Директива 2002/58 мерки, а да я подчини на някои изисквания, свързани по-специално с преследваните цели и пропорционалността на мерките. С други думи, считам, че общо задължение за запазване на данни не е несъвместимо с установения с тази директива режим, при условие че отговаря на някои условия.

109. Съгласно третия довод член 15, параграф 1 от Директива 2002/58 представлявал изключение от установения с тази директива режим и като такова трябвало да се тълкува стриктно, при това в съответствие с установено от постоянната практика на Съда правило. Това стриктно тълкувателно правило забранявало въпросната разпоредба да се тълкува в смисъл, че предлага възможност за налагане на общо задължение за запазване на данни.

110. В това отношение оставам с впечатлението, че предвидената в член 15, параграф 1 от Директива 2002/58 възможност не може да се квалифицира като изключение и поради това, както правилно изтъква и Комисията, не следва да се тълкува стриктно. Всъщност ми се струва трудно тази възможност да се квалифицира като изключение с оглед на цитираното по-горе съображение 11, съгласно което Директивата не накърнява възможността на държавите членки да приемат предвидените в тази разпоредба мерки. Освен това следва да се изтъкне, че член 15 от Директивата е озаглавен „Приложение на някои разпоредби от Директива 95/46“, докато член 10 от нея изрично е озаглавен „Изключения“. Тези заглавия са в подкрепа на схващането ми, че предвидената във въпросния член 15 възможност не може да се квалифицира като „изключение“.

111. Съгласно четвъртия и последен довод несъвместимостта на общо задължение за запазване на данни с установения с Директива 2002/58 режим се потвърждавала с добавянето на член 15, параграф 1а от Директивата при приемането на Директива 2006/24, обявена за невалидна с решение DRI. По силата на този довод именно въпросната несъвместимост накарала законодателя на Съюза да обяви член 15, параграф 1 от Директива 2002/58 за неприложим по отношение на общия режим за запазване, предвиден с Директива 2006/24.

112. Струва ми се, че при този довод има погрешно схващане на обхвата на член 15, параграф 1а от Директива 2002/58. Съгласно тази разпоредба „[член 15, параграф 1 от Директива 2002/58] не се прилага по отношение на данни, специално изисквани от Директива [2006/24], които се запазват за целите, посочени в член 1, параграф 1 от [тази] директива“.

113. Прочитът ми на тази разпоредба е следният. Що се отнася до данните, чието запазване се е изисквало с Директива 2006/24 с оглед на постигане на установените с нея цели, държавите членки са губели предвидената в член 15, параграф 1 от Директива 2002/58 възможност да ограничат в по-голяма степен обхвата на правата и задълженията, предвидени с тази разпоредба, по-специално посредством допълнителни задължения за запазване на данни. С други думи, член 15, параграф 1а е предвиждал изчерпателно хармонизиране по отношение на данните, чието запазване се е изисквало с Директива 2006/24 и за установените с нея цели.

114. Потвърждение на това тълкуване намирам в съображение 12 от Директива 2006/24, съгласно което „[ч]лен 15, параграф 1 от Директива [2002/58] *продължава да се прилага за данни, включително и такива, свързани с неуспешни опити за повиквания, запазването на които не се изисква изрично в настоящата директива, и които следователно са извън нейния обхват, също и за запазването на данни за цели, включително и съдебни, които са различни от тези, предмет на настоящата директива*“ (курсивът е мой).

115. В този смисъл добавянето на член 15, параграф 1а от Директива 2002/58 потвърждава не съвместимостта на общо задължение за запазване на данни с установения с тази директива режим, а желанието на законодателя на Съюза за изчерпателно хармонизиране с приемането на Директива 2006/24.

116. С оглед на гореизложеното считам, че общо задължение за запазване на данни е съвместимо с установения с Директива 2002/58 режим и че следователно е възможно държава членка да използва предоставената с член 15, параграф 1 от тази директива възможност, за да наложи подобно задължение²⁰. Прибягването до тази възможност обаче е подчинено на спазването на строги изисквания, произтичащи не само от въпросната разпоредба, но и от релевантните разпоредби на Хартата, разглеждани в светлината на решение DRI, които ще бъдат анализирани в друг раздел по-нататък²¹.

В – По приложимостта на Хартата по отношение на общо задължение за запазване на данни

117. Преди да се пристъпи към анализ на съдържанието на наложените с Хартата изисквания, във връзка с член 15, параграф 1 от Директива 2002/58, ако държава реши да въведе общо задължение за запазване на данни, следва първо да се провери дали Хартата в действителност е приложима по отношение на такова задължение.

118. Приложимостта на Хартата по отношение на общо задължение за запазване на данни зависи главно от приложимостта по отношение на него на Директива 2002/58.

119. Всъщност съгласно член 51, параграф 1, първо изречение от Хартата „[р]азпоредбите на [Хартата] се отнасят за [...] държавите членки[...] единствено когато те прилагат правото на Съюза“. Разясненията по член 51 от Хартата в това отношение препращат към практиката на Съда, съгласно която задължението да се зачитат основните права, определени в рамките на Съюза, обвързва държавите членки единствено когато те действат в приложното поле на правото на Съюза²².

20 — Тъй като Директива 2002/58 може да се квалифицира като „lex specialis“ спрямо Директива 95/46 (в това отношение вж. член 1, параграф 2 от Директива 2002/58), не считам за необходимо да проверявам съвместимостта на общо задължение за запазване на данни с установения с Директива 95/46 режим, който впрочем не е предмет на поставените на Съда въпроси. За изчерпателност обаче държа да уточня, че текстът на член 13, параграф 1 от Директива 95/46 предоставя по-голяма свобода на действие на държавите членки от член 15, параграф 1 от Директива 2002/58, където се уточнява обхватът ѝ в рамките на предоставянето на обществено достъпни електронни съобщителни услуги. Тъй като предвидената в член 15, параграф 1 от Директива 2002/58 възможност позволява на държава членка да приеме общо задължение за запазване на данни, от това заключавам, че член 13, параграф 1 от Директива 95/46 също позволява това.

21 — Вж. т. 126—262 от настоящото заключение.

22 — Всъщност от постоянната практика на Съда следва, че основните права, гарантирани в правния ред на Съюза, трябва да се прилагат във всички случаи, уредени от правото на Съюза, но не и извън тези случаи. В тази връзка Съдът вече е припомнял, че не може да преценява с оглед на Хартата национална правна уредба, която не попада в обхвата на правото на Съюза. От друга страна, когато такава уредба попада в обхвата на посоченото право, във връзка с преюдициалното запитване Съдът трябва да даде всички насоки за тълкуване, необходими за преценката на националната юрисдикция относно това дали тази правна уредба е съобразена с основните права, чието спазване Съдът гарантира (вж. решение от 26 февруари 2013 г., Åkerberg Fransson, C-617/10, EU:C:2013:105, т. 19 и цитираната съдебна практика).

120. Чешкото, френското и полското правителство и правителството на Обединеното кралство, които оспорват приложимостта на Директива 2002/58 по отношение на общо задължение за запазване на данни²³, поддържат, че по отношение на него не е приложима и Хартата.

121. Вече изложих причините, поради които считам, че с общо задължение за запазване на данни се прилага възможност, предвидена в член 15, параграф 1 от Директива 2002/58²⁴.

122. Поради това съм на мнение, че разпоредбите на Хартата са приложими по отношение на националните мерки, въвеждащи такова задължение, по силата на член 51, параграф 1 от Хартата, както твърдят също и г-н Watson, г-н Brice, г-н Lewis, Open Rights Group, Privacy International, датското, германското и финландското правителство и Комисията²⁵.

123. Този извод не може да се обори с факта, че националните разпоредби, уреждащи достъпа до запазените данни, не попадат като такива в приложното поле на Хартата.

124. Действително, доколкото засягат „дейности[...] на държавата в областта на наказателното право“, националните разпоредби, уреждащи достъпа до запазените от полицейските или съдебните органи данни с цел борба с тежките престъпления според мен попадат в обхвата на предвиденото в член 1, параграф 3 от Директива 2002/58 изключение²⁶. Следователно такива национални разпоредби не прилагат правото на Съюза, поради което и Хартата не е приложима спрямо тях.

125. Все пак причината за съществуването на задължение за запазване на данни е да се позволи на правоприлагащите органи да имат достъп до запазените данни, така че проблемът със запазването и този с достъпа не могат да бъдат напълно отделени. Както правилно подчертава Комисията, разпоредбите, уреждащи достъпа, са от определящо значение за преценката на съвместимостта с Хартата на разпоредбите, въвеждащи общо задължение за запазване на данни, които прилагат член 15, параграф 1 от Директива 2002/58. По-конкретно, разпоредбите, уреждащи достъпа, трябва да бъдат взети предвид при преценката на необходимостта и пропорционалността на подобно задължение²⁷.

Г – По съвместимостта на общо задължение за запазване на данни с изискванията, установени с член 15, параграф 1 от Директива 2002/58, както и с членове 7 и 8 и член 52, параграф 1 от Хартата

126. Сега остава да разгледам трудния въпрос за съвместимостта на общо задължение за запазване на данни с изискванията, установени с член 15, параграф 1 от Директива 2002/58, както и с членове 7 и 8 и член 52, параграф 1 от Хартата в светлината на решение DRI. Този въпрос по-общо се отнася до нуждата от адаптиране на правната уредба към умножилите се с развитието на технологиите средства за наблюдение, с които държавите разполагат²⁸.

23 — Вж. т. 88 от настоящото заключение.

24 — Вж. т. 90—97 от настоящото заключение.

25 — По-точно, член 51, параграф 1, второ изречение от Хартата предвижда, че държавите членки са длъжни да зачитат гарантираните с нея права, когато прилагат правото на Съюза.

26 — По обхвата на това изключение вж. т. 90—97 от настоящото заключение.

27 — Вж. т. 185—262 от настоящото заключение.

28 — Вж. по-специално Съвет на ООН по правата на човека, Доклад на специалния докладчик относно насърчаването и защитата на правото на свобода на мнение и изразяване, 17 април 2013 г., A/HRC/23/40, бр. 33: „Технологичното развитие позволява на държавата да извършва дейности по наблюдение, които вече не са ограничени от критерии, свързани с мащаба или продължителността. [...] Вследствие на това държавата понастоящем разполага повече от всякога с големи средства за провеждане на дейности по наблюдение, които са едновременни, накърняващи личния живот, целенасочени и широкомащабни. [...]“. Вж. също бр. 50: „По принцип законодателството не е следвало ритъма на технологичните промени. В повечето държави правните норми или липсват, или са неподходящи за справяне със съвременните условия за наблюдение на съобщенията. [...]“.

127. В този контекст първият етап от анализа е да се констатира намеса в правата по Директива 2002/58 и в основните права по членове 7 и 8 от Хартата.

128. Всъщност такова задължение представлява тежка намеса в правото на зачитане на личния живот по член 7 от Хартата и в правото на защита на личните данни по член 8 от нея. Не намирам за необходимо да се спирам по-подробно на тази констатация за намеса, която е ясно изложена от Съда в точки 32—37 от решение DRI²⁹. По същия начин общо задължение за запазване на данни представлява намеса в няколко признати с Директива 2002/58 права³⁰.

129. Вторият етап от анализа е да се определи дали и при какви условия тази тежка намеса в правата по Директива 2002/58, както и в основните права по членове 7 и 8 от Хартата може да бъде обоснована.

130. Две разпоредби установяват условията, които трябва да бъдат изпълнени, за да бъде обоснована тази двойна намеса: член 15, параграф 1 от Директива 2002/58, който предвижда възможността за държавите членки да ограничават обхвата на някои установени с Директивата права, и член 52, параграф 1 от Хартата, разглеждан в светлината на решение DRI, който обхваща всички ограничения на упражняването на признатите с Хартата права.

131. Държа да подчертая, че тези изисквания са *кумулятивни*. Всъщност спазването на установените в член 15, параграф 1 от Директива 2002/58 изисквания само по себе си не означава, че предвидените в член 52, параграф 1 от Хартата изисквания са изпълнени, и обратното³¹. Поради това общо задължение за запазване на данни може да се счете за съвместимо с правото на Съюза само ако отговаря едновременно на изискванията по член 15, параграф 1 от Директива 2002/58 и на тези по член 52, параграф 1 от Хартата, както подчертава и Law Society of England and Wales³².

132. Съвместно, тези две разпоредби установяват шест изисквания, които трябва да бъдат изпълнени, за да е обоснована намесата, до която води общо задължение за запазване на данни:

- задължението за запазване трябва да има правно основание,
- то трябва да зачита основното съдържание на признатите с Хартата права,
- трябва да преследва цел от общ интерес,
- трябва да е подходящо за преследването на тази цел,
- трябва да е необходимо за преследването на целта и
- трябва да е пропорционално на преследването на целта в демократично общество.

29 — Все пак ще се върна на конкретните рискове, породени от образуването на бази данни от такъв мащаб в рамките на изискването за пропорционалност в демократично общество на общо задължение за запазване на данни като разглежданите в споровете в главните производства: вж. т. 252—261 от настоящото заключение.

30 — Вж. в това отношение изтъкнатия от Open Rights Group и Privacy International довод, резюмиран в т. 104 от настоящото заключение.

31 — Потвърждение за кумулативността на изискванията намирам в последното изречение на член 15, параграф 1 от Директива 2002/58, съгласно което „[в]сички мерки, упоменати в [този] параграф, трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф[и] 1 и 2 [ДЕС]“. По силата на член 6, параграф 1 ДЕС „Съюзът зачита правата, свободите и принципите, определени в [Хартата], която има същата юридическа сила като Договорите“.

32 — От кумулативността на изискванията логично следва, че доколкото установените с тези две разпоредби изисквания се припокриват, трябва да се приложи най-строгото изискване или, с други думи, изискването, което в най-голяма степен защитава разглежданите права.

133. Няколко от тези условия вече са посочени от Съда в решение DRI. За яснота и предвид особеностите на настоящите дела спрямо решение DRI, все пак бих искал да се спра на всяко от тях, като разгледам по-подробно изискванията, свързани с правното основание и с необходимия и пропорционалния характер в демократично общество на общо задължение за запазване на данни.

1. По наличието на правно основание в националното право

134. Както член 52, параграф 1 от Хартата, така и член 15, параграф 1 от Директива 2002/58 установяват изисквания във връзка с правното основание, което трябва да бъде използвано от държава членка с цел налагането на общо задължение за запазване на данни.

135. На първо място, всяко ограничение на упражняването на признатите с Хартата права трябва да бъде „предвидено в закон“ съгласно член 52, параграф 1 от нея. Ще уточня, че това изискване формално не е разгледано от Съда в решение DRI, отнасящо се до предвидена в директива намеса.

136. До постановяването наскоро на решение WebMindLicenses³³ Съдът не беше се произнасял по точния обхват на въпросното изискване, дори и когато изрично установява, че то е било³⁴ или не е било³⁵ изпълнено. В точка 81 от посоченото решение трети състав на Съда се произнася по следния начин:

„В това отношение следва да се подчертае, че изискването всяко ограничение на упражняването на това право да бъде предвидено в закон означава, че правното основание, позволяващо използването на посочените в предходната точка доказателства от данъчната администрация, трябва да бъде достатъчно ясно и точно и че, определяйки самото то обхвата на ограничението на гарантираното в член 7 от Хартата право, това правно основание дава известна защита срещу евентуални произволни нарушения от страна на тази администрация (вж. по-специално ЕСПЧ, решения Malone с/у Обединеното кралство, 2 август 1984 г., серия А, № 82, т. 67 и Gillan и Quinton с/у Обединеното кралство, 12 януари 2010 г., № 4158/05, т. 77, CEDH 2010)“.

137. Приканвам големия състав на Съда да потвърди това тълкуване в настоящите дела поради следните мотиви.

138. Както правилно посочва генералният адвокат Cruz Villalón в своето заключение по дело Scarlet Extended³⁶, ЕСПЧ е създад богата практика във връзка с това изискване в контекста на ЕКПЧ, която е в смисъл, че терминът „закон“ следва да се разбира в „материалноправен“, а не във формален смисъл³⁷.

33 — Решение от 17 декември 2015 г. (C-419/14, EU:C:2015:832).

34 — Вж. по-специално решения от 17 октомври 2013 г., Schwarz (C-291/12, EU:C:2013:670, т. 35) (намеса, предвидена с европейски регламент), от 27 май 2014 г., Spasic (C-129/14 PPU, EU:C:2014:586, т. 57) (намеса, предвидена с Конвенцията за прилагане на споразумението от Шенген от 14 юни 1985 година между правителствата на държавите от Икономическия съюз Бенелюкс, Федерална република Германия и Френската република за постепенното премахване на контрола по техните общи граници, подписана в Шенген на 19 юни 1990 г. и влязла в сила на 26 март 1995 г.), от 6 октомври 2015 г., Delvigne (C-650/13, EU:C:2015:648, т. 47) (намеса, предвидена с френските Изборен и Наказателен кодекс), и от 17 декември 2015 г., Neptune Distribution (C-157/14, EU:C:2015:823, т. 69) (намеса, предвидена с европейски регламент и директива).

35 — Решение от 1 юли 2010 г., Knauf Gips/Комисия (C-407/08 P, EU:C:2010:389, т. 87—92) (намеса без правно основание).

36 — C-70/10, EU:C:2011:255, т. 94—100.

37 — Вж. по-специално ЕСПЧ, 14 септември 2010 г., Sanoma Uitgevers B.V. с/у Нидерландия, CE:ECHR:2010:0914JUD003822403, т. 83.

139. Съгласно тази съдебна практика изразът „предвидено в закон“ налага правното основание да бъде достатъчно достъпно и предвидимо, тоест формулирано с достатъчно точност, за да може лицето, при необходимост прибегвайки до компетентен съвет, да съобрази поведението си. Това правно основание трябва да осигурява и подходяща защита от произвол и следователно да определя достатъчно ясно обхвата и условията за упражняване на правомощието, предоставено на компетентните органи (принцип на върховенство на правото)³⁸.

140. Според мен е необходимо на използвания в член 52, параграф 1 от Хартата израз „предвидено в закон“ да се придаде същия смисъл като на съответстващия му израз от ЕКПЧ поради следните причини.

141. От една страна, съгласно член 53 от Хартата и разясненията относно този член предоставяната от Хартата степен на закрила никога не може да бъде по-ниска от тази, гарантирана с ЕКПЧ. Забраната да се преминава „прагът ЕКПЧ“ налага Съдът да тълкува използвания в член 52, параграф 1 от Хартата израз „предвидено в закон“ поне толкова строго, колкото и ЕСПЧ е направил това в контекста на ЕКПЧ³⁹.

142. От друга страна, с оглед на хоризонталното естество на това изискване, което може да се приложи спрямо множество видове намеса както в контекста на Хартата, така и на ЕКПЧ⁴⁰, би било неуместно държавите членки да бъдат подчинени на различни критерии в зависимост от това дали намесата бива анализирана с оглед на единия или другия от тези актове⁴¹.

143. Следователно считам, както изтъкват естонското правителство и Комисията, че записаният в член 52, параграф 1 от Хартата израз „предвидено в закон“ трябва да бъде тълкуван, в светлината на практиката на ЕСПЧ, обобщена в точка 139 от настоящото заключение, в смисъл, че правното основание на общо задължение за запазване на данни като разглежданите в споровете в главните производства трябва да е достатъчно достъпно и предвидимо, от една страна, и да осигурява подходяща защита от произвол, от друга страна.

144. На второ място, следва да се определи съдържанието на наложените с член 15, параграф 1 от Директива 2002/58 изисквания, що се отнася до правното основание, което трябва да бъде използвано от държава членка, желаеща да приложи предоставената с тази разпоредба възможност.

145. В това отношение следва да отбележа съществуващите различия в първото изречение на тази разпоредба в текстовете ѝ на различни езици.

146. В текстовете на английски („*legislative measures*“), френски („*mesures législatives*“), италиански („*disposizioni legislative*“), португалски („*medidas legislativas*“), румънски език („*măsuri legislative*“) и шведски език („*genom lagstiftning vidta åtgärder*“), член 15, параграф 1, първо изречение от Директива 2002/58 според мен налага приемането на мерки, произтичащи от законодателната власт.

38 — Вж. по-специално ЕСПЧ, 26 март 1987 г., *Leander c/y Швеция*, SE:ECHR:1987:0326JUD000924881, т. 50-51, ЕСПЧ, 26 октомври 2000 г., *Хасан и Чауш c/y България*, SE:ECHR:2000:1026JUD003098596, т. 84, ЕСПЧ, 4 декември 2008 г., *S. и Marger c/y Обединеното кралство*, SE:ECHR:2008:1204JUD003056204, т. 95, ЕСПЧ, 14 септември 2010 г., *Sanoma Uitgevers B.V. c/y Нидерландия*, SE:ECHR:2010:0914JUD003822403, т. 81—83, ЕСПЧ, 31 март 2016 г., *Стоянов и др. c/y България*, SE:ECHR:2016:0331JUD005538810, т. 124—126.

39 — За да бъде по-конкретен, Съдът според мен не може да възприеме тълкуване на това изискване, по-свободно от това на ЕСПЧ, нещо, което би имало за последица да се позволи по-голям брой видове намеса от произтичащия от тълкуването на това изискване от ЕСПЧ.

40 — Изразът „предвиден[о] в закон[...]“ е използван в член 8, параграф 2 (право на зачитане на личния и семейния живот), член 9, параграф 2 (свобода на мисълта, съвестта и религията), член 10, параграф 2 (свобода на изразяване на мнение) и член 11, параграф 2 (свобода на събранията и сдружаването) от ЕКПЧ. В контекста на Хартата член 52, параграф 1 се прилага по отношение на всяко ограничение на упражняването на признатите с нея права, ако се предположи, че такова ограничение е разрешено.

41 — Вж. в този смисъл *Peers, S. Article 52 – Scope of guaranteed rights.* — in *Peers, S. et al. The EU Charter of Fundamental Rights: a Commentary.* Oxford, OUP, 2014, № 52.39.

147. За сметка на това текстовете на датски („*retsforskrifter*“), немски („*Rechtsvorschriften*“), нидерландски („*wettelijke maatregelen*“) и испански език („*medidas legales*“) на това изречение могат да бъдат тълкувани като изискващи приемането или на мерки от законодателната власт, или на подзаконовни мерки от изпълнителната власт.

148. Съгласно постоянната съдебна практика необходимостта от еднакво прилагане, а следователно и от еднакво тълкуване на акт на Съюза, изключва възможността той да се разглежда отделно в текста на един от езиците, а напротив, изисква да се тълкува в зависимост както от действителната воля на неговия автор, така и от преследваната от този автор цел, в светлината по-специално на текстовете на всички останали официални езици. В случай на несъответствия между тях въпросната разпорежба трябва да се тълкува в зависимост от общата структура и целите на правната уредба, от които тя е част⁴².

149. В случая член 15, параграф 1 от Директива 2002/58 урежда възможността за държавите членки да дерогират основни права, които са признати с членове 7 и 8 от Хартата и чиято защита Директивата гарантира. Поради това считам за уместно изискването за правно основание, наложено с член 15, параграф 1 от Директива 2002/58, да се тълкува в светлината на Хартата, и по-специално на член 52, параграф 1 от нея.

150. Така „мерките“, изисквани по член 15, параграф 1 от Директива 2002/58, императивно трябва да имат качествата на достъпност, предвидимост и подходяща защита от произвол, изтъкнати в точка 143 от настоящото заключение. От тези качества, и конкретно от изискването за подходяща защита от произвол, по-специално следва, че въпросните мерки трябва да са *задължителни* за националните органи, на които се предоставя право на достъп до запазените данни. Не би могло по-специално да е достатъчно гаранциите, съпътстващи достъпа до данните, да бъдат предвидени във вътрешни кодекси или насоки, които нямат такъв задължителен характер, както правилно подчертава това Law Society of England and Wales.

151. Освен това ми се струва, че изразът „[Д]ържавите членки могат да приемат [...] мерки“, общ за текстовете на всичките езици на член 15, параграф 1, първо изречение от Директива 2002/58, изключва възможността национална съдебна практика, била тя и постоянна, да може да представлява достатъчно правно основание за прилагане на въпросната разпорежба. Следва да подчертая, че в това отношение разпоредбата надхвърля изискванията, произтичащи от практиката на ЕСПЧ⁴³.

152. В допълнение бих искал да посоча, че ми се струва желателно, с оглед на тежестта на намесата, до която води общо задължение за запазване на данни в признатите с членове 7 и 8 от Хартата основни права, основното съдържание на разглеждания режим, и по-специално това на гаранциите, съпътстващи задължението, да бъде прието с мярка на законодателната власт, като на изпълнителната власт бъде възложено да уточни условията и реда за неговото прилагане.

153. С оглед на гореизложеното считам, че член 15, параграф 1 от Директива 2002/58 и член 52, параграф 1 от Хартата трябва да се тълкуват в смисъл, че режим, въвеждащ общо задължение за запазване на данни като разглежданите в споровете в главните производства, трябва да е уреден със законови или подзаконовни актове, притежаващи качествата достъпност и предвидимост и предоставящи подходяща защита от произвол.

42 — Вж. по-специално решение от 30 май 2013 г., *Asbeek Brusse и de Man Garabito* (C-488/11, EU:C:2013:341, т. 26), от 24 юни 2015 г., *Hotel Sava Rogaška* (C-207/14, EU:C:2015:414, т. 26), и от 26 февруари 2015 г., *Christie's France* (C-41/14, EU:C:2015:119, т. 26).

43 — Вж. по-специално ЕСПЧ, 14 септември 2010 г., *Sanoma Uitgevers B.V. с/у Нидерландия*, SE:ECHR:2010:0914JUD003822403, т. 83: „[терминът „закон“, съдържащ се в членове 8—11 от ЕКПЧ, обхваща] „писаното право“, включващо както подзаконовни текстове, така и регулаторни актове, приети от професионална организация по силата на законова делегация, предоставяща ѝ право да издава нормативни актове, и „неписаното право“. „Законът“ трябва да се разбира като обхващащ писания текст и „правото, установено“ от съдиите“.

154. Запитващите юрисдикции следва да проверят дали това изискване е спазено, с оглед на привилегированото им положение при преценката на съответните техни национални режими.

2. По зачитането на основното съдържание на признатите с членове 7 и 8 от Хартата права

155. Съгласно член 52, параграф 1 от Хартата всяко ограничение на упражняването на признатите от нея права трябва „да зачита основното съдържание на същите права“⁴⁴. Струва ми се, че този аспект, който е разгледан от Съда в точки 39 и 40 от решение DRI в контекста на Директива 2006/24, не поражда конкретен проблем в рамките на настоящите дела, както изтъкват това испанското и ирландското правителство и Комисията.

156. В точка 39 от решение DRI Съдът приема, че тази директива не засяга същественото съдържание на правото на зачитане на личния живот и на останалите права, признати от член 7 от Хартата, тъй като тя не позволява да се разкрива самото съдържание на електронните съобщения.

157. Тази преценка според мен може е относима и към разглежданите в главните производства национални режими, тъй като и те не позволяват да се разкрива самото съдържание на електронните съобщения⁴⁵.

158. В точка 40 от решение DRI Съдът приема, че Директива 2006/24 не засяга същественото съдържание на основното право на защита на личните данни, признато в член 8 от Хартата, с оглед на принципите във връзка със защитата и сигурността на данните, които доставчиците трябва да спазват по силата на член 7 от тази директива, съгласно които държавите членки следят за приемането на подходящи технически и организационни мерки, недопускащи случайното или незаконно унищожаване или случайната загуба или промяна на данните.

159. И тази преценка считам за приложима към разглежданите в главните производства национални режими, тъй като ми се струва, че те включват сравними гаранции във връзка със защитата и сигурността на запазените от доставчиците данни, като тези гаранции трябва да позволяват ефикасната защита на личните данни от рисковете от злоупотреба, както и от всеки незаконен достъп до тях или използване⁴⁶.

160. Все пак запитващите юрисдикции следва да установят дали разглежданите в споровете в главните производства национални режими действително спазват основното съдържание на признатите с членове 7 и 8 от Хартата права, в светлината на изложените по-горе съображения.

3. По наличието на призната от Съюза цел от общ интерес, която може да обоснове общо задължение за запазване на данни

161. Както член 15, параграф 1 от Директива 2002/58, така и член 52, параграф 1 от Хартата изискват всяка намеса в признатите в тези актове права да преследва цел от общ интерес.

44 — Подобно изискване не произтича от текста на член 15, параграф 1 от Директива 2002/58, нито от структурата на тази директива поради изложените в точки 99—116 от настоящото заключение причини.

45 — Вж. описанието на разглежданите в споровете в главните производства национални режими, по-специално в т. 13 и 36 от настоящото заключение.

46 — Решение DRI, т. 54. Вж. описанието на разглежданите в споровете в главните производства национални режими в т. 29—33, както и в т. 45 и 46 от настоящото заключение.

162. В точки 41—44 от решение DRI Съдът приема, от една страна, че наложеното с Директива 2006/24 общо задължение за запазване на данни допринася за „борбата с тежките престъпления, а с това в крайна сметка и за повишаване на обществената сигурност“, и от друга страна, че тази борба представлява цел от общ интерес за Съюза.

163. От практиката на Съда всъщност е видно, че цел от общ интерес за Съюза е борбата с международния тероризъм с оглед на опазване на международния мир и сигурност. Същото се отнася и за борбата с тежките престъпления с цел да се гарантира обществената сигурност. В допълнение в това отношение следва да се изтъкне, че член 6 от Хартата провъзгласява правото на всеки не само на свобода, но също така и на сигурност⁴⁷.

164. Тази преценка е приложима към разглежданите в споровете в главните производства общи задължения за запазване на данните, които могат да бъдат обосновани с целта за борба с тежките престъпления.

165. Все пак с оглед на някои представени на Съда доводи следва да се установи дали такова задължение може да бъде обосновано с цел от общ интерес, различна от тази за борба с тежките престъпления.

166. В това отношение текстът на член 52, параграф 1 от Хартата излага по общ начин „признати[те] от Съюза цели от общ интерес“ и „необходимостта да се защитят правата и свободите на други хора“.

167. Текстът на член 15, параграф 1 от Директива 2002/58 е по-точен, що се отнася до целите, които могат да обосноват намеса в установените с тази директива права. Всъщност съгласно тази разпоредба въпросните мерки трябва да допринесат за „гарантира[не на] национална[та] сигурност (т.е. държавна[та] сигурност), отбрана[та], обществена[та] безопасност и [предотвратяването], разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна [съобщителна] система, както е посочено в член 13, параграф 1 от Директива 95/46“.

168. Освен това в решение Promusicae⁴⁸ Съдът приема, че тази разпоредба трябва да се тълкува в светлината на член 13, параграф 1 от Директива 95/46, който позволява изключенията от предвидените в нея права, когато са обосновани със „защита на правата и свободите на трети лица“. Вследствие на това Съдът приема, че член 15, параграф 1 от Директива 2002/58 предлага на държавите членки възможността да предвидят задължението за доставчика да разкрива лични данни, за да се установи в рамките на гражданско производство дали са засегнати авторските права върху музикални и аудиовизуални записи.

169. Правителството на Обединеното кралство извежда довод от това решение, за да изтъкне, че общо задължение за запазване на данни може да бъде обосновано с всяка една от целите, упоменати или в член 15, параграф 1 от Директива 2002/58, или в член 13, параграф 1 Директива 95/46. Според това правителство подобно задължение би могло да бъде обосновано с ползата от запазените данни в борбата с „обикновените“ престъпления (за разлика от „тежките“) или дори в контекста на ненаказателни производства във връзка с упоменатите в тези разпоредби цели.

170. Този довод не ми звучи убедително поради следните причини.

47 — Решение DRI, т. 42 и цитираната съдебна практика.

48 — Решение от 29 януари 2008 г. (C-275/06, EU:C:2008:54, т. 50—54).

171. На първо място и както правилно подчертават г-н Watson и Open Rights Group и Privacy International, възприетият от Съда в решение Promusicae⁴⁹ подход не може да се приложи към настоящите дела, тъй като това решение се отнася до искане за достъп от страна на сдружение на притежатели на авторски права до данни, запазени в хода на дейността на доставчик, а именно Telefónica de España. С други думи, посоченото решение не се отнася до цели, можещи да обосноват тежка намеса в основните права като тази, която налага общо задължение за запазване на данни като разглежданите в споровете в главните производства.

172. На второ място, считам, че изискването за пропорционалност в демократичното общество изключва възможността борбата с обикновените престъпления или правилното провеждане на ненаказателни производства да обоснове общо задължение за запазване на данни. Всъщност значителните рискове, свързани с подобно задължение, са несъразмерни спрямо предимствата, които то би предоставило в борбата с обикновените престъпления или в контекста на ненаказателни производства⁵⁰.

173. С оглед на гореизложеното считам, че член 15, параграф 1 от Директива 2002/58 и член 52, параграф 1 от Хартата трябва да се тълкуват в смисъл, че борбата с тежките престъпления представлява цел от общ интерес, която може да обоснове общо задължение за запазване на данни, за разлика от борбата с обикновените престъпления или правилното провеждане на ненаказателни производства.

174. Поради това следва да се разгледа подходящият, необходим и пропорционален характер на подобно задължение в светлината на целта за борба с тежките престъпления.

4. По подходящия характер на общо задължение за запазване на данни с оглед на борбата с тежките престъпления

175. Изискванията във връзка с подходящия, необходим⁵¹ и пропорционален⁵² характер произтичат както от член 15, параграф 1 от Директива 2002/58, така и от член 52, параграф 1 от Хартата.

176. По силата на първото от тези изисквания общо задължение за запазване на данни като разглежданите в споровете в главните производства трябва да може да допринесе за определената по-горе цел от общ интерес, а именно борбата с тежките престъпления.

177. Това изискване не поражда особено затруднение в контекста на настоящите дела. Както Съдът изтъква по същество в точка 49 от решение DRI, запазените данни позволяват на компетентните по наказателноправните въпроси национални органи да разполагат с допълнително средство за разследване с цел предотвратяване или разкриване на тежките престъпления. Следователно такова задължение допринася за борбата с този вид престъпления.

178. Все пак държа да уточня ползата, която може да има от общо задължение за запазване на данни за целите на борбата с тежките престъпления. Както правилно изтъква френското правителство, такова задължение в известна степен позволява на правоприлагащите органи „да четат миналото“ чрез извършване на справки в запазените данни, при това отделно от целевите мерки за наблюдение.

49 — Решение от 29 януари 2008 г. (C-275/06, EU:C:2008:54).

50 — Вж. т. 252—261 от настоящото заключение.

51 — По необходимия характер вж. т. 185—245 от настоящото заключение.

52 — По пропорционалния характер *stricto sensu* вж. т. 246—262 от настоящото заключение.

179. Целевите мерки за наблюдение са насочени към лица, за които предварително е установено, че могат да имат връзка, макар косвена или далечна, с тежко престъпление. Такива целеви мерки позволяват на компетентните органи да имат достъп до данните за съобщенията, осъществени от тези лица, дори и до съдържанието на тези съобщения. Този достъп би могъл да се отнася само до съобщенията, осъществени от такива лица, след установяването им като евентуално имащи връзка с тежко престъпление.

180. Общото задължение за запазване на данни пък е насочено към всички съобщения, осъществени от всички ползватели, без да се изисква каквато и да е връзка с тежко престъпление. Подобно задължение позволява на компетентните органи да имат достъп до хронологията на осъществените от дадено лице съобщения, преди да е било установено, че то може да има такава връзка. Именно в този смисъл подобно задължение дава на правоприлагащите органи ограничена възможност да четат миналото, като им предоставя достъп до съобщенията, извършени от такива лица *преди* установяването на споменатата възможна връзка⁵³.

181. С други думи, ползата от общо задължение за запазване на данни с цел борба с тежките престъпления се състои в тази ограничена възможност за четене на миналото посредством данни, очертаващи хронологията на осъществените от дадено лице съобщения дори преди да е било заподозряно, че има връзка с тежко престъпление⁵⁴.

182. При представянето на предложението за приемане на Директива 2006/24 Комисията онагледява тази полза с помощта на няколко конкретни примера за разследвания, отнасящи се по-специално до терористични актове, убийства, отвлечения и детска порнография⁵⁵.

183. Няколко подобни примера са изложени пред Съда в рамките на настоящите дела, по-специално от френското правителство, което подчертава положителното задължение на държавите членки да гарантират сигурността на намиращите се на тяхна територия лица. Според това правителство в рамките на разследванията във връзка с унищожаването на мрежите, организиращи заминаването на френски граждани в зони на конфликт в Ирак или Сирия, достъпът до запазените данни играе определяща роля за установяване на лицата, подпомогнали подобно заминаване. Това правителство добавя, че достъпът до данните за съобщенията на лицата, замесени в неотдавнашните терористични атентати от януари и ноември 2015 г. във Франция, е бил изключително полезен за разследващите с цел разкриване на съучастниците на извършителите на атентатите. Освен това в рамките на издирването на изчезнало лице данните, свързани с локализирането му при осъществените съобщения преди изчезването му, биха могли да играят определяща роля за целите на разследването.

53 — Комисията подчертава също, че добавената стойност на общо задължение за запазване на данни спрямо целевото им запазване се състои в тази ограничена възможност за четене на миналото: вж. Commission Staff Working Document, представен в приложение към предложението за директива, довело до приемането на Директива 2006/24, SEC(2005) 1131, 21 септември 2005 г., № 3.6, „Data Preservation versus Data Retention“: „[W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects“.

54 — В това отношение френското правителство се позовава на доклада на Conseil d'État. *Le numérique et les droits fondamentaux*. 2014, 209–210. Conseil d'État (Франция) подчертава, че механизъм на целеви мерки по наблюдение „би бил отчетливо по-малко ефективен от систематичното запазване от гледна точка на националната сигурност и издирването на извършителите на престъпление. Всъщност той не би позволил никакъв ретроспективен достъп до обмена, осъществен преди органът да установи заплахата или престъплението: оперативният му характер следователно би зависил от възможността на органите да предприемат предварителни мерки по установяването на самоличността на лицата, чиито данни за връзката биха могли да са полезни — нещо, което е невъзможно в рамките на съдебната полиция. Що се отнася например до престъпление, съдебният орган не би могъл да има достъп до предхождащите го съобщения — данни, при все това ценни и понякога дори наложителни за установяване на извършителя му и неговите съучастници, както това стана ясно в няколко скоростни дела за терористични атентати. В рамките на предотвратяването на засягането на националната сигурност новите технически програми се основават на възможността за засичане на слабите сигнали, несъвместима със схващането за предварителното целево наблюдение на опасните лица“.

55 — Commission Staff Working Document, представен в приложение към предложението за директива, довело до приемането на Директива 2006/24, SEC(2005) 1131, 21 септември 2005 г., № 1.2, „The importance of traffic data for law enforcement“.

184. С оглед на гореизложените съображения считам, че общо задължение за запазване на данни е в състояние да допринесе за борбата с тежките престъпления. Все пак остава да се провери дали такова задължение е същевременно необходимо и пропорционално на тази цел.

5. По необходимия характер на общо задължение за запазване на данни с оглед на борбата с тежките престъпления

185. Съгласно постоянната съдебна практика мярка може да се приеме за необходима само при липсата на каквато и да била друга мярка, която би била също толкова подходяща, като обаче е по-слабо ограничителна⁵⁶.

186. Изискването, свързано с подходящия характер, следва да даде оценка за „абсолютната“ ефективност — независимо от всяка друга възможна мярка — на общо задължение за запазване на данни с оглед на борбата с тежките престъпления. Що се отнася до изискването за необходимост, то води до преценка на ефикасността — или „относителната“ ефективност, тоест в сравнение с всяка друга възможна мярка — на подобно задължение⁵⁷.

187. В контекста на настоящите дела проверката за необходимост налага да се провери, от една страна, дали други мерки не биха могли да бъдат също толкова ефективни, колкото и общо задължение за запазване на данни, в борбата с тежките престъпления, и от друга страна, дали тези евентуални мерки не накърняват в по-малка степен признатите с Директива 2002/58 и членове 7 и 8 от Хартата права⁵⁸.

188. Освен това ще припомня постоянната съдебна практика, посочена в точка 52 от решение DRI, съгласно която защитата на основното право на личен живот изисква дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на „строгото необходимото“⁵⁹.

189. Страните, представили становища пред Съда, разискват подробно две групи въпроси, свързани с изискването за строга необходимост в контекста на настоящите дела, като по същество те съответстват на двата поставени от запитващата юрисдикция по дело C-203/15 въпроса:

— От една страна, в светлината на точки 56—59 от решение DRI, трябва ли общо задължение за запазване на данни само по себе си да се счита за надхвърлящо границите на строго необходимото за целите на борбата с тежките престъпления, при това независимо от евентуалните съпътстващи го гаранции?

56 — Вж. по-специално решения от 22 януари 2013 г., *Sky Österreich* (C-283/11, EU:C:2013:28, т. 54—57), от 13 ноември 2014 г., *Reindl* (C-443/13, EU:C:2014:2370, т. 39), и от 16 юли 2015 г., *ЧЕЗ Разпределение България* (C-83/14, EU:C:2015:480, т. 120—122). В рамките на доктрината вж. по-специално *Pirker*, B. *Proportionality Analysis and Models of Judicial Review*. Europa Law Publishing, Groningen 2013, p. 29: „Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value“.

57 — Вж. *Rivers*, J. *Proportionality and variable intensity of review*. 65(1) *Cambridge Law Journal* (2006) 174, p. 198: „The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights — enjoyment without reducing the level of realisation of some other constitutional interest“.

58 — По наличието на тези два компонента в рамките на проверката за необходимост вж. *Barak*, A. *Proportionality: Constitutional Rights and their Limitations*. Cambridge University Press, Cambridge 2012, 323—331.

59 — Вж. по-специално решения от 9 ноември 2010 г., *Volker und Markus Schecke и Eifert* (C-92/09 и C-93/09, EU:C:2010:662, т. 77 и 86), и от 7 ноември 2013 г., *IPI* (C-473/12, EU:C:2013:715, т. 39).

— От друга страна, ако се предположи, че такова задължение може да се счете за ненадхвърлящо само по себе си границите на строго необходимото, трябва ли да бъде съпътствано от всички гаранции, изтъкнати от Съда в точки 60—68 от решение DRI, с цел да ограничи до строго необходимото накърняването на правата, признати с Директива 2002/58 и членове 7 и 8 от Хартата?

190. Преди да разгледам тези въпроси, считам за уместно да отхвърля един изтъкнат от правителството на Обединеното кралство довод, съгласно който установените в решение DRI критерии са ирелевантни в контекста на настоящите дела, тъй като въпросното решение се отнася не до национален режим, а до такъв, установен от законодателя на Съюза.

191. В това отношение ще подчертая, че в решение DRI са тълкувани членове 7 и 8 и член 52, параграф 1 от Хартата и че тези разпоредби са предмет и на въпросите, поставени в споровете в главните производства. Според мен обаче не е възможно разпоредбите на Хартата да се тълкуват различно в зависимост от това дали разглежданият режим е установен на равнището на Съюза или на национално равнище, както правилно подчертават това г-н Vriscе, г-н Lewis и Law Society of England and Wales. При констатация, че Хартата е приложима, какъвто е случаят в настоящите дела⁶⁰, тя трябва да се приложи по един и същ начин, без оглед на разглеждания режим. Следователно изведените от Съда критерии в решение DRI са релевантни за преценката на разглежданите в настоящите дела режими, както изтъкват по-специално датското и ирландското правителство и Комисията.

а) По строго необходимия характер на общо задължение за запазване на данни

192. Според първия подход, защитаван от Tele2 Sverige и от Open Rights Group и Privacy International, общо задължение за запазване на данни трябва — след постановяването на решение DRI — да се счита за надхвърлящо само по себе си границите на строго необходимото за целите на борбата с тежките престъпления, при това независимо от евентуалните съпътстващи това задължение гаранции.

193. Според втория подход, поддържан от повечето от останалите представили становище пред Съда страни, такова задължение не надхвърля границите на строго необходимото, при условие че е съпътствано от някои гаранции във връзка с достъпа до данните, периода на запазване, защитата и сигурността им.

194. Изложените по-долу причини ме карат да възприема втория подход.

195. На първо място, съгласно прочита, който правя на решение DRI, Съдът приема, че общо задължение за запазване на данни надхвърля границите на строго необходимото, когато то *не е съпътствано* от строги гаранции във връзка с достъпа до данните, периода на запазване, защитата и сигурността им. За сметка на това Съдът не се е произнесъл по съвместимостта с правото на Съюза на общо задължение за запазване на данни, което би било *съпътствано* от такива гаранции, тъй като подобен режим не е бил предмет на въпроси, поставени на Съда по това дело.

196. В това отношение ще подчертая, че в точки 56—59 от решение DRI Съдът не е посочил нищо в смисъл, че общо задължение за запазване на данни само по себе си би надхвърляло границите на строго необходимото.

60 — Вж. т. 117—125 от настоящото заключение.

197. В точки 56 и 57 от това решение Съдът установява, че предвиденото в Директива 2006/24 задължение за запазване се отнася до всички електронни съобщителни средства, всички ползватели и всички данни за трафика, без да се прави никакво разграничение, ограничение или изключение с оглед на целта за борба с тежките престъпления.

198. В точки 58 и 59 от посоченото решение Съдът излага по-подробно практическите последици от тази липса на разграничение. От една страна, въпросното задължение за запазване се отнася дори до лица, за които липсват каквито и да е улики, от които да се счете, че поведението им може да има връзка, дори и косвена или далечна, с тежки престъпления. От друга страна, тази директива не изисква никаква връзка между данните, чието запазване се предвижда, и заплахата за обществената сигурност, и по-специално тя не е ограничена до запазване, отнасящо се или до данни за времеви период, и/или определена географска зона, и/или определен кръг от лица, които може да бъдат замесени по един или друг начин в тежко престъпление.

199. Така Съдът приема, че общо задължение за запазване на данни се характеризира с липса на разграничаване в зависимост от целта за борба с тежките престъпления. Той обаче не постановява, че такава липса на разграничаване означава, че такова задължение само по себе си превишава границите на строго необходимото.

200. Всъщност едва в края на анализа на предвидения с Директива 2006/24 режим и след като установява липсата на някои гаранции, които ще разгледам по-долу⁶¹, Съдът приема в точка 69 от решение DRI следното:

„С оглед на всички предходни съображения следва да се приеме, 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“ (курсивът е мой).

201. Както изтъкват германското и нидерландското правителство, ако самото общо запазване на данните бе достатъчно да доведе до невалидността на Директива 2006/24, Съдът нямаше да има нужда да разглежда, при това подробно, липсата на изложените в точки 60—68 от въпросното решение гаранции.

202. Следователно общото задължение за запазване на данни, предвидено с Директива 2006/24, само по себе си не е надхвърляло границите на строго необходимото. Тази директива е надхвърляла границите на строго необходимото поради *съвместното действие* на общото запазване на данните и липсата на гаранции, целящи да ограничат до строго необходимото накръняването на признатите с членове 7 и 8 от Хартата права. Поради това съвместно действие Директивата е трябвало да бъде обявена за невалидна в нейната цялост⁶².

203. На второ място, потвърждение на това тълкуване намирам и в точка 93 от решение Schrems⁶³, която възпроизвеждам по-долу:

„Следователно не се ограничава до строго необходимото правна уредба, която общо разрешава [запазването] на всички лични данни на всички лица, чиито данни са били прехвърлени от Съюза към Съединените щати, *без да въвежда* никакво разграничаване, ограничаване или изключение с оглед на преследваната цел и *без да предвижда* обективен критерий, позволяващ

61 — Вж. т. 216—245 от настоящото заключение.

62 — Вж. решение DRI, т. 65: „Следователно трябва да се констатира, че от тази директива произтича особено обширна и тежка за правния ред на Съюза намеса в тези основни права, *без тази намеса да е точно уредена с разпоредби, които да могат да гарантират, че тя действително се свежда до строго необходимото*“ (курсивът е мой).

63 — Решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650).

да се ограничи достъпът на публичните органи до данните и тяхното последващо използване за конкретни цели, които са строго ограничени и могат да обосноват намесата, каквато съдържат достъпът и използването на тези данни [в този смисъл, що се отнася до Директива 2006/24, вж. решение DRI, т. 57—61]“ (курсивът е мой).

204. И тук Съдът не приема, че разглежданият в това дело режим надхвърля границите на строго необходимото, само поради мотива че с него се разрешава общо запазване на личните данни. В случая границите на строго необходимото са били надхвърлени поради съвместното действие на възможността за такова общо запазване и липсата на гаранция за достъпа с оглед на намаляване на намесата до строго необходимото.

205. От гореизложеното заключавам, че общо задължение за запазване на данни не трябва винаги да се счита само по себе си за надхвърлящо границите на строго необходимото за целите на борбата с тежките престъпления. Такова задължение обаче надхвърля границите на строго необходимото винаги когато не е съпътствано от гаранции за достъпа до данните, периода на запазване, защитата и сигурността им.

206. На трето място, впечатлението ми в това отношение се потвърждава от нуждата да се провери конкретно спазването на изискването за строга необходимост в контекста на разглежданите в споровете в главните производства национални режими.

207. Както изтъкнах в точка 187 от настоящото заключение, изискването за строга необходимост налага да се разгледа дали други мерки биха могли да са също толкова ефективни, колкото и общо задължение за запазване на данни, в борбата с тежките престъпления, като същевременно накърняват в по-малка степен признатите с Директива 2002/58 и членове 7 и 8 от Хартата права.

208. Подобна преценка обаче трябва да се извърши в конкретния контекст на всеки национален режим, предвиждащ общо задължение за запазване на данни. От една страна, преценката изисква да се сравни ефективността на това задължение с тази на всяка друга възможна мярка на национално равнище, като се отчете фактът, че задължението осигурява на компетентните органи ограничена възможност за четене на миналото чрез запазените данни⁶⁴.

209. С оглед на изискването за строга необходимост е наложително юрисдикциите да не се ограничат само до проверка на ползата от общо задължение за запазване на данни, а стриктно да проверят дали друга мярка или съчетание от мерки, и по-специално целево задължение за запазване на данни, съпътствано от други инструменти за разследване, не може да бъде също така ефективно в борбата с тежките престъпления. В това отношение ще подчертая, че в редица представени на вниманието на Съда изследвания се оспорва необходимостта от този вид задължение за целите на борбата с тежките престъпления⁶⁵.

210. От друга страна, дори и да се предположи, че други мерки могат да бъдат също толкова ефективни в борбата с тежките престъпления, запитващите юрисдикции също така ще трябва да установят дали те не накърняват в по-малка степен разглежданите основни права в сравнение с общо задължение за запазване на данни, в приложение на припомнената в точка 185 от настоящото заключение съдебна практика.

64 — Вж. т. 178—183 от настоящото заключение.

65 — Вж. комисар по правата на човека на Съвета на Европа, „Issue paper on the rule of law on the Internet and in the wider digital world“, декември 2014 г., CommDH/IssuePaper(2014)1, стр. 115; Съвет на ООН по правата на човека, Доклад на Върховния комисариат на ООН за правата на човека относно правото на личен живот в цифровата епоха, 30 юни 2014 г., A/HRC/27/37, бр. 26; Общо събрание на ООН, доклад на специалния докладчик относно насърчаването и защитата на правата на човека и основните свободи в борбата с тероризма, 23 септември 2014 г., A/69/397, бр. 18 и 19.

211. В светлината на точка 59 от решение DRI националните юрисдикции следва по-специално да разгледат възможността да се ограничи материалният обхват на задължението за запазване, като същевременно се съхрани ефективността на тази мярка в борбата с тежките престъпления⁶⁶. Такива задължения всъщност могат да имат по-голям или по-малък материален обхват в зависимост от това към какви ползватели, географски зони и съобщителни средства са насочени⁶⁷.

212. Според мен по-специално би било желателно, в случай че технологиите позволяват това, от задължението за запазване да се изключат особено чувствителните данни с оглед на разглежданите в настоящите дела основни права, каквито са данните, обхванати от професионалната тайна, или тези, позволяващи установяването на журналистическите източници.

213. Трябва все пак да се има предвид, че съществено ограничаване на обхвата на общо задължение за запазване на данни създава опасност от значително намаляване на ползата от такъв режим в борбата с тежките престъпления. От една страна, няколко правителства подчертават затруднението, дори невъзможността, предварително да се определят данните, които биха могли да имат връзка с тежко престъпление. Следователно подобно ограничение е в състояние да изключи запазването на данни, които биха могли да се окажат релевантни в борбата с тежки престъпления.

214. От друга страна, както изтъква естонското правителство, тежката престъпност е динамично явление, годно да се адаптира към инструментите на разследване, с които разполагат правоприлагащите органи. В този смисъл ограничение до определена географска зона или съобщително средство би създавало опасност от изместване на свързаните с тежките престъпления дейности към географска зона и/или съобщително средство, които не са обхванати от този режим.

215. Тъй като изисква сложна преценка на разглежданите в споровете в главните производства национални режими, считам, че този анализ трябва да се извърши от националните юрисдикции, както подчертават чешкото, естонското, ирландското, френското и нидерландското правителство и Комисията.

б) По императивния характер на изложените от Съда в точки 60—68 от решение DRI гаранции с оглед на наличието на строга необходимост

216. Ако се предположи, че общо задължение за запазване на данни може да се счете за строго необходимо в контекста на разглеждания национален режим — нещо, което националният съд следва да прецени, трябва също да се установи дали подобно задължение се налага да бъде съпътствано от всички изложени от Съда в точки 60—68 от решение DRI гаранции с оглед ограничаване до строго необходимото на накръняването на признатите с Директива 2002/58 и членове 7 и 8 от Хартата права.

217. Тези гаранции се отнасят до правилата, уреждащи достъпа и използването на запазените данни от компетентните органи (т. 60—62 от решение DRI), периода на запазване на данните (т. 63 и 64 от решението), както и сигурността и защитата на данните, запазени от доставчиците (т. 66—68 от решението).

66 — Тази забележка е насочена единствено спрямо общите задължения за запазване на данни (които могат да се отнасят до всяко лице, без оглед на каквато и да е връзка с тежко престъпление), а не целевите мерки за наблюдение (насочени към лицата, предварително установени като имащи връзка с тежко престъпление): по това разграничение вж. т. 178—183 от настоящото заключение.

67 — В съдебното заседание за изслушване на устните състезания германското правителство по-специално уточнява, че германският парламент е изключил електронните писма от наложеното от германското законодателство задължение за запазване, но че този режим обхваща всички ползватели и цялата национална територия.

218. В рамките на представените пред Съда становища се противопоставят две тези по отношение на естеството на тези гаранции.

219. Съгласно първата теза, защитавана от г-н Watson, г-н Brice и г-н Lewis и от Open Rights Group и Privacy International, изложените от Съда в точки 60—68 от решение DRI гаранции са императивни. Според тази теза Съдът е установил минимални гаранции, *всички* от които трябва да бъдат изпълнени от разглеждания национален режим, за да се ограничи накърняването на основните права до строго необходимото.

220. Съгласно втората теза, поддържана от германското, естонското, ирландското и френското правителство и правителството на Обединеното кралство, изложените от Съда в точки 60—68 от решение DRI гаранции са само указателни. Съдът извършил „свкупна преценка“ на гаранциите, липсващи в предвидения в Директива 2006/24 режим, като никоя от тях не може поотделно да се счете за императивна с оглед на изискването за строга необходимост. Германското правителство онагледява тази теза с примера на „скачените съдове“, като посочва, че също като при тях, по-смекчен подход по отношение на някой от трите установени от Съда аспекта (например достъпа до запазените данни) би могъл да се компенсира с по-строг подход при останалите два аспекта (периода на запазване, сигурността и защитата на данните).

221. Имам убеждението, че тази теза за „скачените съдове“ трябва да бъде отхвърлена и че *всички* изложени от Съда в точки 60—68 от решение DRI гаранции трябва да се считат за императивни поради следните причини.

222. На първо място, в използваната от Съда формулировка при анализа му на строгата необходимост на установения с Директива 2006/24 режим не се прави такова тълкуване. По-специално, в точки 60—68 от това решение Съдът никъде не посочва каквато и да е възможност за „компенсиране“ на по-смекчен подход при един от трите установени от Съда аспекта с по-строг подход по отношение на останалите два аспекта.

223. Всъщност ми се струва, че при тезата за „скачените съдове“ изискването за необходимост се бърка с това за пропорционалност *stricto sensu*, което Съдът не разглежда в решение DRI. Всъщност, както посочих в точка 186 от настоящото заключение, изискването за необходимост се състои в отхвърляне на всяка неефективна мярка. В този контекст не може да става въпрос за извършване на „свкупна преценка“, „компенсиране“ или „претегляне“, които настъпват едва на етапа на пропорционалността *stricto sensu*⁶⁸.

224. На второ място, тази теза за „скачените съдове“ би заличила полезното действие на изложените от Съда в точки 60—68 от решение DRI гаранции така, че лицата, чиито данни са били запазени, вече не биха разполагали с достатъчни гаранции, позволяващи ефективно да се защитят личните им данни срещу рисковете от злоупотреба и срещу всеки незаконосъобразен достъп и използване на тези данни, както това се изисква в точка 54 от посоченото решение.

225. Деструктивното действие на тази теза лесно може се онагледя с помощта на следните примери. Национален режим, строго ограничаващ достъпа само за целите на борба с тероризма и свеждащ периода на запазване до три месеца (строг подход по отношение на достъпа и периода на запазване), който обаче не задължава доставчиците да запазват данните на националната територия и в криптиран формат (смекчен подход по отношение на сигурността), би изложил цялото население на повишен риск от незаконен достъп до запазените данни. По

68 — Вж. Barak, A. Proportionality: Constitutional Rights and their Limitations. Cambridge University Press, Cambridge 2012, p. 344: „The first three components of proportionality deal mainly with the relation between the limiting law’s purpose and the means to fulfil that purpose. [...] Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing.* The test of proportionality *stricto sensu* is different. [...] It focuses on the relation between the benefit in fulfilling the law’s purpose and the harm caused by limiting the constitutional right. *It is based on balancing*“ (курсивът е мой).

същия начин, национален режим, предвиждащ период на запазване от три месеца, както и запазване на данните на националната територия и в криптиран формат (строг подход по отношение на продължителността и на сигурността), който обаче позволява на всеки служител на всички публични органи да имат достъп до запазените данни (смекчен подход по отношение на достъпа), би изложил цялото население на повишена опасност от злоупотреби от страна на националните органи.

226. Според мен от тези примери следва, че запазването на полезното действие на изложените от Съда в точки 60—68 от решение DRI гаранции изисква *всяка* от тях да се приеме за императивна. ЕСПЧ също подчертава основополагащото значение на тези гаранции в наскоро постановеното решение Szabó и Vissy c/y Унгария, като изрично се позовава на решение DRI⁶⁹.

227. На трето място, струва ми се, че прилагането на тези гаранции от държавите членки, желаещи да наложат общо задължение за запазване на данни, не поражда големи практически затруднения. Според мен тези гаранции всъщност в много аспекти са „минимални“, както изтъква г-н Watson.

228. Голяма част от тези гаранции бяха обсъдени пред Съда поради вероятната им липса в разглежданите в главните производства национални режими.

229. Първо, от точки 61 и 62 от решение DRI е видно, че достъпът и последващото използване на запазените данни трябва строго да бъдат ограничени до целите за предотвратяване и разкриване на точно определени тежки престъпления или до наказателното преследване във връзка с тях.

230. Според Tele2 Sverige и Комисията това изискване не било спазено в разглеждания по дело C-203/15 шведски режим, който позволявал достъпа до запазените данни с оглед на борбата с обикновените престъпления. Подобна критика се изтъква от г-н Vrce и г-н Lewis, както и от г-н Watson, по отношение на разглеждания по дело C-698/15 режим на Обединеното кралство, който разрешавал достъпа с оглед на борбата с обикновените престъпления и дори при липсата на престъпление.

231. Макар Съдът да не следва да се произнася по съдържанието на тези национални режими, налага се да определи целите от общ интерес, които са в състояние да обосноват тежката намеса в признатите с Директивата и с членове 7 и 8 от Хартата права. В случая вече изложих причините, поради които считам, че *единствено* борбата с тежките престъпления може да обоснове такава намеса⁷⁰.

232. Второ, съгласно точка 62 от решение DRI достъпът до запазените данни следва да се предоставя след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, чието решение следва да има за цел да ограничи достъпа до данните и тяхното използване само до строго необходимото за постигането на преследваната цел. Този предварителен контрол освен това трябва да се постановява след мотивирана молба на тези органи, подадена в рамките на наказателни производства за предотвратяване, разкриване или наказателно преследване на престъпления.

69 — ЕСПЧ, 12 януари 2016 г., Szabó и Vissy c/y Унгария, CE:ECHR:2016:0112JUD003713814, т. 68: „Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens’ trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens’ private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities’ enhanced technical possibilities to intercept private information“.

70 — Вж. т. 170—173 от настоящото заключение.

233. Съгласно становищата на Tele2 Sverige и Комисията тази гаранция за независим и предварителен контрол на достъпа частично липсвала в разглеждания по дело C-203/15 шведски режим. Същата констатация правят г-н Brice, г-н Lewis, г-н Watson, Open Rights Group и Privacy International по отношение на разглеждания по дело C-698/15 режим на Обединеното кралство, като истинността ѝ не се оспорва от правителството на Обединеното кралство.

234. Не виждам никакъв мотив за смекчаване на изискването за предварителен контрол от независимо образование, безспорно произтичащо от използваната от Съда в точка 62 от решение DRI формулировка⁷¹. Най-напред, това изискване е продиктувано от тежестта на намесата и от рисковете, свързани със създаването на бази данни, обхващащи почти цялото съответно население⁷². Ще отбележа, че редица експерти в областта на защитата на правата на човека в борбата с тероризма критикуват настоящата тенденция, състояща се в заместване на традиционните процедури по независимо разрешаване и действително проследяване със системите за „самостоятелно разрешаване“ на достъпа до данните от службите на разузнаването и полицията⁷³.

235. По-нататък, независим и предварителен контрол на достъпа до данните е необходим, за да позволи обработването във всеки отделен случай на особено чувствителните данни с оглед на разглежданите в настоящите дела основни права, каквито са данните, обхванати от професионалната тайна, или пък тези, позволяващи да се установят журналистическите източници, както подчертават това Law Society of England and Wales, френското и германското правителство. Този предварителен контрол на достъпа е още по-необходим в хипотезата, при която всички тези данни е технически трудно да се изключат на етапа на запазването⁷⁴.

236. Накрая ще добавя, че от практическа гледна точка никоя от трите засегнати при искане за достъп страни не е в състояние да упражни ефективен контрол относно достъпа до запазените данни. Компетентните правоприлагащи органи имат пълен интерес да искат възможно най-широк достъп до тези данни. Доставчиците, които не са запознати с преписката по разследването, не могат да проверят дали искането за достъп е ограничено до строго необходимото. Колкото до лицата, за чиито данни се прави справка, те не разполагат с никакво средство да узнаят, че са обект на такава мярка по разследване, при това дори в случай на злоупотреба или неправомерно използване, както подчертават г-н Watson, г-н Brice и г-н Lewis. Така очертаната конфигурация на интереси според мен налага намеса на независимо образование преди извършването на справка със запазените данни, за да могат лицата, чиито данни се запазват, да бъдат защитени от всяка злоупотреба при достъп от страна на компетентните органи.

71 — Все пак ще уточня, че това изискване за предварителен и независим контрол според мен не може да намери източник в член 8, параграф 3 от Хартата, тъй като тя не е приложима като такава по отношение на националните разпоредби, уреждащи достъпа до запазените данни: вж. т. 123—125 от настоящото заключение.

72 — Вж. т. 252—261 от настоящото заключение.

73 — Съвет на ООН по правата на човека, доклад на специалния докладчик относно насърчаването и защитата на правата на човека и основните свободи в борбата с тероризма, 28 декември 2009 г., A/HRC/13/37, № 62: „Не следва да има никаква тайна система за наблюдение, която да не е подчинена на надзора на ефективна контролна инстанция, нито каквато и да е намеса, която да не е разрешена посредством независим орган“ (вж. също № 51). Вж. също Общо събрание на ООН, доклад на специалния докладчик относно насърчаването и защитата на правата на човека и основните свободи в борбата с тероризма, 23 септември 2014 г., A/69/397, № 61.

74 — Вж. т. 212 от настоящото заключение. Колкото до журналистическите източници, ЕСПЧ подчертава нуждата от предварително разрешение от независимо образование, тъй като контрол a posteriori не позволява да се възстанови поверителността на такива източници: вж. ЕСПЧ, 22 ноември 2012 г., Telegraaf Media Nederland Landelijke Media B.V. и др. c/y Нидерландия, SE:ECCHR:2012:1122JUD003931506, т. 101, и ЕСПЧ, 12 януари 2016 г., Szabó и Vissy c/y Унгария, SE:ECCHR:2016:0112JUD003713814, т. 77. В решение Корп c/y Швейцария, отнасящо се до наблюдението на телефонните линии на адвокат, ЕСПЧ отправя критики по отношение на факта, че служител от администрацията е бил отговорен, без контрол от независим магистрат, да филтрира информацията, обхваната от професионалната тайна: вж. ЕСПЧ, 25 март 1998 г., Корп c/y Швейцария, SE:ECCHR:1998:0325JUD002322494, т. 74.

237. Предвид това ми се струва разумно да се приеме, че точни положения на крайна неотложност, изтъкнати от правителството на Обединеното кралство, могат да обосноват незабавния достъп до запазените от правоприлагащите органи данни, без предварителен контрол, за да се предотврати извършването на тежки престъпления или да се преследват техните извършители⁷⁵. Във възможно най-голяма степен е наложително да се запази изискването за предварително разрешение, като се въведе спешна процедура в рамките на независимото образувание с цел обработката на този вид искане за достъп. Ако обаче самото сезиране на това образувание с искане за достъп изглежда несъвместимо с крайната неотложност на положението, достъпът и използването на данните трябва да са предмет на контрол *a posteriori* от това образувание, при това в най-кратки срокове.

238. Трето, в точка 68 от решение DRI се установява задължение за доставчиците да запазват данните на територията на Съюза, за да се гарантира изискваният по член 8, параграф 3 от Хартата контрол от независим орган на спазването на изискванията за защита и сигурност, изведени в точки 66 и 67 от това решение.

239. Tele2 Sverige и Комисията изтъкват, че запазването на данните на националната територия не било гарантирано в рамките на разглеждания по дело C-203/15 шведски режим. Същата критика е отправена и от г-н Brice, г-н Lewis и г-н Watson срещу разглеждания по дело C-698/15 режим на Обединеното кралство.

240. В това отношение, от една страна, не виждам никаква причина за отслабване на това изведено в точка 68 от решение DRI изискване, тъй като запазването на данните извън територията на Съюза не би позволило на лицата, чиито данни се запазват, да се гарантира степента на защита, предоставена с Директива 2002/58 и членове 7 и 8 и член 52, параграф 1 от Хартата⁷⁶.

241. От друга страна, ми се струва разумно това изискване, изразено от Съда в контекста на Директива 2006/24, да се адаптира за контекста на националните режими, като се предвиди запазване на данните на националната територия, както изтъкват германското и френското правителство и Комисията. Всъщност съгласно член 8, параграф 3 от Хартата всяка държава членка е длъжна да гарантира контрола, посредством независим орган, върху спазването на изискванията за защита и сигурност от доставчиците, предвидени в нейния национален режим. При липсата на координация на равнището на Съюза обаче такъв национален орган би могъл да се окаже в невъзможност да изпълнява задачите си по контрол на територията на друга държава членка.

242. Четвърто, що се отнася до периода на запазване, запитващите юрисдикции трябва да приложат критериите, определени от Съда в точки 63 и 64 от решение DRI. От една страна, тези юрисдикции трябва да установят дали запазените данни могат да бъдат разграничени в зависимост от ползата им и евентуално дали периодът на запазване е бил пригоден спрямо този критерий. От друга страна, тези юрисдикции трябва да проверят дали периодът на запазване е основан на обективни критерии, позволяващи да се гарантира неговото ограничаване до строго необходимото.

75 — Вж. в това отношение механизма, описан в т. 22 от настоящото заключение. Подчертавам, че тази проблематика не е разглеждана от Съда в решение DRI.

76 — В това отношение вж. решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650).

243. Ще подчертая, че в неотдавнашното решение Роман Захаров с/у Русия ЕСПЧ приема за разумен максимален период на запазване от шест месеца, като същевременно изразява съжаление за липсата на задължение за незабавно унищожаване на данните, нямащи връзка с целта, заради която са били събрани⁷⁷. В това отношение ще добавя, че разглежданите в споровете в главните производства национални режими трябва да предвиждат задължение за безвъзвратно унищожаване на всички запазени данни, след като те вече не са строго необходими в борбата с тежките престъпления. Това задължение трябва да бъде спазвано не само от доставчиците, които запазват данните, но и от органите, имащи достъп до такива данни.

244. С оглед на гореизложените съображения считам, че всички изложени от Съда в точки 60—68 от решение DRI гаранции са с императивен характер и поради това трябва да съпътстват общо задължение за запазване на данни, за да се ограничи до строго необходимото накръняването на признатите с Директива 2002/58 и членове 7 и 8 от Хартата права.

245. Запитващите юрисдикции следва да проверят дали разглежданите в споровете в главните производства национални режими съдържат всяка от тези гаранции.

6. По пропорционалния характер в демократично общество на общо задължение за запазване на данни с оглед на целта за борба с тежките престъпления

246. След като проверят дали разглежданите в главните производства национални режими са необходими, запитващите юрисдикции ще трябва да проверят и дали те са пропорционални в демократично общество с оглед на целта за борба с тежките престъпления. Този аспект не е разглеждан от Съда в решение DRI, тъй като установеният с Директива 2006/24 режим е надхвърлял границите на строго необходимото за целите на борбата с тежките престъпления.

247. Това изискване за пропорционалност в демократично общество — или пропорционалност „*stricto sensu*“ — произтича едновременно от член 15, параграф 1 от Директива 2002/58, член 52, параграф 1 от Хартата и постоянната съдебна практика. Съгласно последната мярка, накръняваща основни права, може да се счита за пропорционална само ако породените неудобства не са несъразмерни с преследваните цели⁷⁸.

77 — Вж. в това отношение ЕСПЧ, 4 декември 2015 г., Роман Захаров с/у Русия, СЕ:ЕCHR:2015:1204JUD004714306, т. 254 и 255. Съгласно руското право унищожаването на прихванатите елементи следва да настъпва при изтичането на шестмесечния срок на запазване, ако на съответното лице не е било повдигнато обвинение за престъпление. ЕСПЧ приема за разумен максималния период на запазване, а именно шест месеца, определен в руското право за такива данни. Той все пак изразява съжаление за липсата на задължение за незабавно унищожаване на данните, нямащи връзка с целта, за която са били събрани, като уточнява, че автоматичното запазване в продължение на шест месеца на данни, които очевидно не представляват интерес, не може да се приеме за обосновано с оглед на член 8 от ЕКПЧ.

78 — Вж. по-специално решения от 15 февруари 2016 г., N. (C-601/15 PPU, EU:C:2016:84, т. 54; необходимият характер е разгледан в т. 56—67, пропорционалният — в т. 68 и 69), от 16 юли 2015 г., ЧЕЗ Разпределение България (C-83/14, EU:C:2015:480, т. 123; необходимият характер е разгледан в т. 120—122, пропорционалният — в т. 123—127), и от 22 януари 2013 г., Sky Österreich (C-283/11, EU:C:2013:28, т. 50; необходимият характер е разгледан в т. 54—57, пропорционалният — в т. 58—67).

248. За разлика от изискванията за подходящ и необходим характер на разглежданата мярка, с които се оценява ефективността ѝ за постигане на преследваните цели, изискването за пропорционалност *stricto sensu* налага да се направи равностойка, от една страна, на предимствата ѝ с оглед на преследваната легитимна цел, и от друга страна, на недостатъците ѝ с оглед на признатите в демократичното общество основни права⁷⁹. Така въпросното изискване повдига дебат за ценностите, които трябва да преобладават в демократичното общество, и в крайна сметка за това в какво общество искаме да живеем⁸⁰.

249. Поради това, както посочих и в точка 223 от настоящото заключение, цялостна преценка на разглеждания режим следва да се направи именно на етапа на анализа на пропорционалността в тесен смисъл, а не на този на необходимостта, както твърдят защитниците на тезата за „скачените съдове“⁸¹.

250. Съгласно припомнената в точка 247 от настоящото заключение съдебна практика следва да се направи равностойка на предимствата и недостатъците в демократично общество на общо задължение за запазване на данни. Тези предимства и недостатъци, които в известен смисъл разкриват светлата и тъмната страна на такова задължение, са тясно свързани с неговата най-съществена характеристика, а именно че се отнася за всички съобщения на всички ползватели, без да се изисква каквато и да било връзка с тежко престъпление.

251. От една страна, в точки 178—183 от настоящото заключение вече изложих предимствата, които запазването на данните за всички осъществени на националната територия съобщения предоставя за борбата с тежките престъпления.

252. От друга страна, недостатъците на общо задължение за запазване на данни произтичат от факта, че огромна част от запазените данни се отнасят до лица, които никога няма да имат връзка с тежко престъпление. В това отношение е важно да се уточни естеството на неудобствата, които ще засегнат въпросните лица. Естеството на тези неудобства обаче е различно в зависимост от степента на намеса в техните основни права на зачитане на личния живот и на защита на личните данни.

253. В рамките на „индивидуална“ намеса, засягаща определено лице, неудобствата, до които води общо задължение за запазване на данни, са описани много точно от генералния адвокат Cruz Villalón в точки 72—74 от неговото заключение по дело DRI⁸². Съгласно използваната от него формулировка анализът на тези данни прави възможно „надеждно и изчерпателно „картографиране“ на важна част от поведението на дадено лице, която се отнася стриктно до личния му живот, а дори и за изготвяне на пълен и точен портрет на самоличността му“.

79 — Вж. *Rivers* J. Proportionality and variable intensity of review. 65(1) Cambridge Law Journal (2006) 174, p. 198: „It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights - enjoyment combined with the achievement of other interests is good or acceptable“.

80 — Вж. *Pirker* B. Proportionality Analysis and Models of Judicial Review. Europa Law Publishing, Groningen 2013, p. 30: „In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail“.

81 — Спецификата на изискването за пропорционалност *stricto sensu* в сравнение с изискванията за уместен и необходим характер може да бъде онагледена със следния пример. Да си представим, че държава членка налага инжектирането на електронен чип за геолокализиране на всяко пребиваващо на нейната територия лице, като този чип позволява на органите да проследяват движението на носителя му през изтеклата година. Подобна мярка би могла да се счете за „необходима“, ако никоя друга мярка не позволява да се постигне същото равнище на ефективност в борбата с тежките престъпления. Според мен обаче такава мярка би била непропорционална в демократично общество, тъй като недостатъците, произтичащи от накарването на правата на физическа неприкосновеност, зачитане на личния живот и защита на личните данни, биха били несъразмерни спрямо произтичащите от нея предимства в борбата с тежките престъпления.

82 — C-293/12 и C-594/12, EU:C:2013:845. Вж. също решение DRI (т. 27 и 37).

254. С други думи, на индивидуално равнище общо задължение за запазване на данни позволява намеса, която е също толкова тежка, колкото и при целевите мерки за наблюдение, в това число и при тези от тях, при които се засича и съдържанието на осъществените съобщения.

255. Макар тежестта на подобни намеси на индивидуално равнище да не може да се подценява, все пак ми се струва, че конкретните рискове, свързани с общо задължение за запазване на данни, се разкриват в контекста на „масовите“ намеси.

256. Всъщност, за разлика от целевите мерки за наблюдение, такава задължение може значително да улесни масовите намеси, тоест онези, засягащи съществена част или дори цялото релевантно население, нещо, което може да бъде онагледено с помощта на следните примери.

257. Да предположим, на първо място, че лице с достъп до запазените данни има намерението да установи всички лица от населението на държавата членка, които са с психични разстройства. За целта анализът на съдържанието на всички осъществени на националната територия съобщения би изискал значителни ресурси. За сметка на това използването на базите данни за съобщенията би позволило незабавно да се установят всички лица, свързали се с психолог в периода на запазване на данните⁸³. Ще добавя, че обхватът на тази техника би могъл да се разшири към всяка от медицинските специалности, регистрирани в дадена държава членка⁸⁴.

258. Да предположим, на второ място, че същото това лице иска да установи лицата, противопоставящи се на политиката на действащото правителство. И тук за целта анализът на съдържанието на съобщенията би изискал значителни ресурси. За сметка на това употребата на данните за съобщенията би позволила да се установят всички лица, абониращи в списъци за разпространение на електронни писма, в които се критикува правителствената политика. Освен това въпросните данни биха позволили да се установят и лицата, участващи в която и да е опозиционна на правителството обществена проява⁸⁵.

259. Държа да подчертая, че рисковете, свързани с достъпа до данните за съобщенията (или „метаданните“), могат да бъдат равнозначни или дори по-големи от произтичащите от достъпа до съдържанието на тези съобщения, както отбелязват Open Rights Group и Privacy International, Law Society of England and Wales и както се посочва в скорошен доклад на

83 — Запазените данни всъщност включват установяване на източника и на получателя на съобщението — данни, които би било достатъчно да се съпоставят със списъка с телефонните номера на действащите на националната територия психолози.

84 — Вж. в това отношение Съвет на ООН по правата на човека, доклад на специалния докладчик относно насърчването и защитата на правата на човека и основните свободи в борбата с тероризма, 28 декември 2009 г., A/HRC/13/37, № 42: „[П]роучвания в Германия показват тревожна последица от политиките на запазване на данните: 52 % от запитаните лица са посочили, че е малко вероятно да използват далекосъобщения, за да се свържат с токсиколог, психотерапевт или брачен консултант поради законите за запазване на данните“.

85 — Тъй като запазените данни включват локализирането на източника и на получателя на съобщението, самоличността на всяко лице, иницииращо или получаващо съобщение по време на проява, би могла лесно да се установи благодарение на запазените данни. В това отношение Marc Goodman, експерт във ФБР и Интерпол в областта на рисковете, свързани с новите технологии, подробно излага, че неотдавна по време на проява на опозицията украинското правителство е установило всички мобилни телефони, намиращи се в близост до улични сблъсъци между силите на реда и противниците на правителството. Тогава всички тези телефони са получили съобщение, което авторът описва като възможно най-„оруделско“ съобщение, изпратено някога от правителство: „Уважаеми абонат, Вие сте регистрирани като участник в тежко нарушаване на обществения ред“ (Goodman, M. Future Crimes. Anchor Books, New York 2016, p. 153, свободен превод). Вж. също Съвет на ООН по правата на човека, доклад на специалния докладчик относно насърчването и защитата на правото на свобода на мнение и изразяване, 17 април 2013 г., A/HRC/23/40, № 75, и Съвет на ООН по правата на човека, Доклад на Върховния комисариат на ООН за правата на човека относно правото на личен живот в цифровата епоха, 30 юни 2014 г., A/HRC/27/37, № 3.

Върховния комисариат на ООН за правата на човека⁸⁶. По-специално и както показват посочените по-горе примери, „метаданните“ позволяват почти незабавното каталогизиране на дадено население в неговата цялост — нещо, което съдържанието на съобщенията не позволява.

260. Ще добавя, че рисковете от достъп с цел злоупотреба или от незаконен достъп до запазените данни изобщо не са теоретични. От една страна, рискът от достъп с цел злоупотреба от компетентните органи трябва да се свърже с изключително високия брой искания за достъп, посочен в представените пред Съда становища. По отношение на шведския режим Tele2 Sverige отбелязва, че получава около 10 000 искания за достъп месечно, без да се включват исканията, получени от други активни доставчици на шведска територия. Колкото до режима на Обединеното кралство, г-н Watson цитира редица откъси от официален доклад, съгласно който за 2014 г. са дадени 517 236 разрешения и 55 346 спешни устни разрешения. От друга страна, рискът от незаконен достъп от което и да е лице е неразделно свързан със самото наличие на бази данни, запазени на информационни носители⁸⁷.

261. Според мен запитващите юрисдикции следва да преценят дали неудобствата, причинени от разглежданите в споровете в главните производства общи задължения за запазване на данни, не са несъразмерни, в демократично общество, спрямо предвидените цели, в приложение на припомнената в точка 247 от настоящото заключение съдебна практика. В рамките на тази преценка въпросните юрисдикции ще трябва да направят равностойна на рисковете и предимствата, свързани с такова задължение, а именно:

- от една страна, предимствата, свързани с предоставянето на отговарящите за борбата с тежките престъпления органи на ограничена възможност за четене на миналото⁸⁸, и
- от друга страна, сериозните рискове, произтичащи, в демократично общество, от правомощието за картографиране на личния живот на дадено лице и от правомощието за каталогизиране на население в неговата цялост.

262. Тази преценка трябва да се направи с оглед на всички релевантни характеристики на разглежданите в споровете в главните производства национални режими. В това отношение ще подчертая, че изложените от Съда в точки 60—68 от решение DRI императивни гаранции са само минимални гаранции с цел ограничаване до строго необходимото на накърняването на признатите с Директива 2002/58 и членове 7 и 8 от Хартата права. Следователно не е изключено национален режим, съдържащ всички тези гаранции, да трябва все пак да се счете за непропорционален в демократично общество поради несъразмерността между сериозните рискове, свързани с това задължение в демократично общество, и произтичащите от него предимства в борбата с тежките престъпления.

86 — Вж. в това отношение Съвет на ООН по правата на човека, Доклад на Върховния комисариат на ООН за правата на човека относно правото на личен живот в цифровата епоха, 30 юни 2014 г., A/HRC/27/37, № 19: „В същия ред на мисли, някои поддържат, че прихващането — или събирането — на данни за дадено съобщение, а не за съдържанието му, само по себе си не представлява намеса в личния живот. От гледна точка на правото на личен живот обаче това разграничаване не е убедително. Натрупванията на информация, наричана общо „метаданни“, могат да дадат сведения за поведението на дадено лице, социалните му връзки, личните му предпочитания и самоличността му, които значително надхвърлят това, което се получава при достъпа до съдържанието на едно лично съобщение“ (курсивът е мой). Вж. също Общо събрание на ООН, доклад на специалния докладчик относно насърчаването и защитата на правата на човека и основните свободи в борбата с тероризма, 23 септември 2014 г., A/69/397, № 53.

87 — Вж. по-специално Съвет на ООН по правата на човека, доклад на специалния докладчик относно насърчаването и защитата на правото на свобода на мнение и изразяване, 17 април 2013 г., A/HRC/23/40, № 67: „Съобщителните бази данни стават уязвими на кражба, измама и случайно разкриване“.

88 — Вж. т. 178—183 от настоящото заключение.

VI – Заключение

263. С оглед на гореизложеното предлагам на Съда да отговори на поставените от Kammarrätten i Stockholm (Апелативен административен съд Стокхолм, Швеция) и от Court of Appeal (England & Wales) (Civil Division) (Апелативен съд (Англия и Уелс) (гражданско отделение) (Обединеното кралство) 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 година, както и членове 7 и 8 и член 52, параграф 1 от Хартата на основните права на Европейския съюз трябва да се тълкуват в смисъл, че допускат държава членка да наложи на доставчиците на обществено достъпни електронни съобщителни услуги задължение да запазват всички данни за съобщенията, осъществени от ползвателите на техните услуги, когато са изпълнени всички посочени по-долу условия — нещо, което запитващите юрисдикции следва да проверят в светлината на всички релевантни характеристики на разглежданите в споровете в главните производства национални режими:

- това задължение и съпътстващите го гаранции трябва да бъдат предвидени посредством законови или подзаконови мерки, които имат свойството да са достъпни, да са предвидими и да осигуряват подходяща защита от произвол,
- това задължение и съпътстващите го гаранции трябва да зачитат основното съдържание на правата, признати с членове 7 и 8 от Хартата на основните права,
- това задължение трябва да е стриктно необходимо за борбата с тежките престъпления, което означава, че никаква друга мярка или съчетание от мерки не трябва да могат да са също толкова ефективни в борбата с тежките престъпления и същевременно да накърняват в по-малка степен правата, признати с Директива 2002/58 и с членове 7 и 8 от Хартата на основните права,
- това задължение трябва да бъде съпътствано от всички гаранции, изложени от Съда в точки 60—68 от решение от 8 април 2014 г., Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238), относно достъпа до данните, периода на запазване, както и защитата и сигурността им, с цел да се ограничи до стриктно необходимото накърняването на правата, признати с Директива 2002/58 и членове 7 и 8 от Хартата на основните права, и
- това задължение трябва да е пропорционално в демократично общество на целта за борба с тежките престъпления, което означава, че рисковете, до които води в демократично общество, не трябва да са несъразмерни на предимствата, които предоставя за борбата с тежките престъпления“.