Дело C-793/19

Резюме на преюдициалното запитване съгласно член 98, параграф 1 от Процедурния правилник на Съда

Дата на постъпване в Съда:

29 октомври 2019 г.

Запитваща юрисдикция:

Bundesverwaltungsgericht (Германия)

Дата на акта за преюдициално запитване:

25 септември 2019 г.

Ищец в първоинстанционното производство и ответник в производството по ревизионно обжалване:

SpaceNet AG

Ответник в първоинстанционното производство и жалбоподател в производството по ревизионно обжалване:

Bundesrepublik Deutschland

Предмет на главното производство

Иск да се признае за установено, че SpaceNet не е длъжно да съхранява посочените в член 113b, параграф 3 от TKG далекосъобщителни данни за трафик на своите клиенти, на които осигурява достъп до интернет.

Предмет и правно основание на преюдициалното запитване

Тълкуване на правото на Съюза, и по-специално на член 15, параграф 1 от Директива 2002/58, както и на решение Tele2 Sverige и Watson, и др.; член 267 ДФЕС.

Преюдициален въпрос

Трябва ли член 15 от Директива 2002/58/ЕО във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз, от

една страна, и с член 6 от Хартата на основните права на Европейския съюз, както и с член 4 от Договора за Европейския съюз, от друга страна, да се тълкува в смисъл, че не допуска национална правна уредба, която задължава доставчиците на обществено достъпни електронни съобщителни услуги да съхраняват данните за трафик и данните за местонахождението на крайните потребители на тези услуги, когато

– за това задължение не е необходимо да е налице конкретно основание от гледна точка на място, време или пространство;

– предмет на задължението за съхраняване при предоставянето на обществено достъпни телефонни услуги, включително при предаването на кратки, мултимедийни или подобни съобщения, както и на повиквания без отговор или на неуспешни повиквания, са следните данни:

  – телефонният номер или друг идентификатор на линията, от която се извършва повикването, и на линията, която приема повикването, както и на всяка друга участваща линия в случай на препращане или прехвърляне,

  – дата и час на началото и на края на връзката или, в случай на предаване на кратки, мултимедийни или подобни съобщения – времето на изпращането и на получаването на съобщението, и посочване на съответната часова зона,

  – информация за използваната услуга, когато в рамките на телефонната услуга могат да се ползват различни услуги;

  – в случая на мобилни телефонни услуги също и

    – международните идентификатори на абонатите на мобилни услуги на линията, от която се осъществява повикването и на линията, която приема повикването,

    – международният идентификатор на крайното съоръжение, от което се осъществява повикването и с което се приема повикването,

    – дата и час на първото активиране на услугата и посочване на съответната часова зона, когато услугите са предплатени,

    – знаците на клетките, които се използват от осъществяващата и от приемащата повикването линия в началото на връзката,

  – в случая на интернет телефония също и адресите по интернет протокол на осъществяващата и на приемащата повикването линия и присвоените на ползвателите идентификатори,

- предмет на задължението за съхраняване при предоставянето на обществено достъпни услуги за достъп до интернет са следните данни:
  - адрес по интернет протокол, който е присвоен на абоната за ползване на интернет,
  - уникален идентификатор на линията, чрез която се осъществява ползването на интернет, както и присвоен на ползвателя идентификатор,
  - дата и час на началото и на края на ползването на интернет с присвоения адрес по интернет протокол, с посочване на съответната часова зона,
  - при мобилно ползване: знаците на клетката, която се използва в началото на интернет връзката,
- не се допуска съхраняването на следните данни:
  - съдържанието на съобщенията,
  - данни за посетени интернет страници,
  - данни за услуги за електронна поща,
  - данни, които указват връзките от и към някои линии на лица, органи и организации в социалния сектор или в църковната сфера;
- срокът на съхраняване на данните за местонахождение, т.е. знаците на клетката, е четири седмици за използваната клетка и десет седмици за останалите данни,
- е осигурена ефективна защита на съхранените данни срещу рискове от злоупотреба, както и срещу всякакъв неразрешен достъп, и
- съхранените данни могат да се използват само за наказателното преследване на особено тежки престъпления и за предотвратяване на конкретна заплаха за телесната неприкосновеност, живота или свободата на дадено лице или за съществуването на федерацията или на дадена провинция, с изключение на адреса по интернет протокол, присвоен на даден абонат за ползване на интернет, чието използване е допустимо в рамките на справка със съхраняваните данни за целите на наказателното преследване на всякакви престъпления, предотвратяването на заплаха за обществения ред и сигурност, както и за изпълнението на функциите на разузнавателните служби?

Разпоредби от правото на Съюза, на които се прави позоваване

Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“), членове 6, 7, 8, 11 и 52

Договор за Европейския съюз (ДЕС), членове 4 и 6

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), в редакцията, изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (наричана по-нататък „Директива 2002/58“), членове 5, 6, 8, 9, и по-специално член 15, както и съображение 11

Разпоредби на националното право, на които се прави позоваване

Telekommunikationsgesetz (TKG) (Закон за далекосъобщенията, наричан по-нататък „Telekommunikationsgesetz“ или „TKG“), член 113a, параграф 1, първо изречение („Задължени лица“), член 113b („Задължения за съхранение на данни за трафик“), член 113c („Използване на данните“), член 113d („Gewährleistung der Sicherheit der Daten“ („Гарантиране на сигурността на данните“), член 113e („Протоколиране“ [от страна на задълженото лице на достъпите до съхранените данни]), член 113f („Списък с изисквания“ [по отношение на техническите средства и други мерки]), член 99, параграф 2 („„Подробна фактура“,органи, указването на които е изключено в подробните фактури)

Strafprozessordnung (StPO) (Наказателно-процесуален кодекс, наричан по-нататък „StPO“), член 100g, параграф 2 („Събиране на данни за трафик“ съгласно член 113b от TKG)

Цитирана практика на Съда

Решение на Съда на Европейския съюз от 21 декември 2016 г., Tele2 Sverige и Watson, и др., C-203/15 и C-698/15, EU:C:2016:970 (наричано по-нататък „решение Tele2 Sverige и Watson и др.“)

Решение от 8 април 2014 г., Digital Rights Ireland и Seitlinger и др., C-293/12 и C-594/12, EU:C:2014:238 (наричано по-нататък „решение Digital Rights Ireland и др.“)

Становище 1/15 от 26 юли 2017 г., EU:C:2017:592

Също така: решения от 29 юли 2019 г., Funke Medien (C-469/17, EU:C:2019:623), от 9 март 1978 г., Simmenthal (106/77, EU:C:1978:49), от

3 май 2005 г., Berlusconi и др. (C-387/02, C-391/02 и C-403/02, EU:C:2005:270), от 22 юни 2010 г., Melki и Abdeli (C-188/10 и C-189/10, EU:C:2010:363), от 18 септември 2014 г., Vueling Airlines (C-487/12, EU:C:2014:2232).

Кратко представяне на фактическата обстановка и на производството

1 Ищецът в първоинстанционото производство, SpaceNetAG (наричан по-нататък „ищецът“ или „SpaceNet“) предоставя обществено достъпни услуги за достъп до интернет. Той оспорва наложеното му по силата на член 113a, параграф 1 във връзка с член 113b от Telekommunikationsgesetz (TKG), в редакцията на закона от 10 декември 2015 г., задължение, считано от 1 юли 2017 г. да съхранява далекосъобщителните данни за трафик на своите клиенти.

2 В производството пред първа инстанция Verwaltungsgericht (Административен съд) установява, че SpaceNet не дължно да съхранява посочените в член 113b, параграф 3 от TKG далекосъобщителни данни за трафик на своите клиенти, на които предоставя достъп до интернет. Ответникът в първоинстанционното производство, Федерална република Германия (наричан по-нататък „ответникът“), обжалва това решение с пряка ревизионна жалба.

3 Ревизионната жалба ще бъде уважена, само ако уреденото в посочените разпоредби на TKG задължение на доставчиците на обществено достъпни далекосъобщителни услуги (наричани по-нататък „доставчици на далекосъобщителни услуги“) да съхраняват далекосъобщителни данни за трафик, не нарушава правото на Съюза.

4 Това задължение на доставчиците на далекосъобщителни услуги да съхраняват определени данни за трафик за ограничен срок е предмет на нова уредба с Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Закон за въвеждане на срок за съхраняване и на максимален срок за съхраняване по отношение на данни за трафик) от 10 декември 2015 г. (наричан по-нататък „Закон от 10 декември 2015 г.).

5 Новата уредба е станала необходима, след като с решение на Bundesverfassungsgericht (Федерален конституционен съд) от 2010 г. предишните разпоредби, уреждащи съхраняването на данни, са обявени за нищожни поради нарушение на основните права, и след като освен това Директива 2006/24, за чието транспониране са приети по-ранните разпоредби, през 2014 г. е обявена за невалидна. Законът от 10 декември 2015 г. е приет, за да се запълнят пропуски в наказателното преследване и в сигурността и същевременно да се вземат предвид произтичащите от посочените решения изисквания съгласно конституционното право и правото на Съюза.

6 За да се отговори на въпроса дали задължението за съхраняване, наложено с член 113a, параграф 1 във връзка с член 113b от TKG, нарушава правото на Съюза, е необходимо Съдът да тълкува Директива 2002/58, и по-специално да разясни как следва да се разбира решението Tele2 Sverige и Watson, и др.

Кратко изложение на мотивите за преюдициалното запитване

7 Уреденото в член 113a, параграф 1, първо изречение във връзка с член 113b от TKG задължение за съхраняване на далекосъобщителните данни за трафик ограничава правата по член 5, параграф 1, член 6, параграф 1 и член 9, параграф 1 от Директива 2002/58.

8 То представлява намеса в защитената по силата на член 5, параграф 1, първо изречение от директивата поверителност на електронните комуникации и е в противоречие с принципа, че по правило е забранено други лица освен потребителите да съхраняват, без съгласието на последните, данни за трафик, свързани с електронните комуникации.

9 Освен това то не е съобразено с предвиденото в член 6 от директивата условие, че обработването и съхраняването на данни за трафик се разрешава само до необходимите степен и продължителност за целите на фактурирането на услугите, пускането им на пазара и за доставката на услуги с добавена стойност.

10 За случай че могат да бъдат обработени данни за местонахождение, различни от данни за трафик, отнасящи се до потребители или абонати на обществени комуникационни мрежи или обществено достъпни комуникационни услуги, в член 9, параграф 1, първо изречение от Директива 2002/58 се предвижда, че такива данни могат да бъдат обработени, само когато се направят анонимни или със съгласието на потребители или абонати, до степен и продължителност, необходими за предоставяне на услуга с добавена стойност. Законовата уредба се отклонява и от това изискване, доколкото съгласно член 113b, параграф 1, точка 2 във връзка с член 4 от TKG следва да се съхраняват и посочените там данни за местонахождение.

11 Ограничаването на правата по член 5, параграф 1, член 6, параграф 1 и член 9, параграф 1 от Директива 2002/58/ЕО е обосновано само ако разпоредбата на член 113a, параграф 1, първо изречение във връзка с член 113b от TKG може да се основе на член 15, параграф 1 от Директива 2002/58.

12 Съгласно този член държавите членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в членове 5, 6, 8, параграфи 1, 2, 3, член 4 и член 9 от тази директива, когато съгласно член 13, параграф 1 от Директива 95/46 такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на

демократично общество, за да се гарантира национална сигурност (т.е държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и наказателното преследване на престъпления или неразрешено използване на електронна комуникационна система. В тази връзка държавите членки могат, inter alia, да приемат законодателни мерки, предвиждащи съхранението на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф. Всички мерки, упоменати в този параграф, трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително упоменатите в член 6, параграф 1 и 2 от Договора за Европейския съюз (ДЕС).

13 Съгласно съображенията на Съда в решение Tele2 Sverige и Watson и др., и по-специално в точки 82 и сл. и 108 и сл. от това решение, за да е допустима национална правна разпоредба по силата на член 15, параграф 1 от Директива 2002/58, е необходимо да е налице достатъчно основание. Това означава, че в обхвата ѝ могат да попадат само онези лица, за които е налице основание да се счита, че са свързани с тежки престъпления, че обхватът ѝ се ограничава до региона, периода и до комуникационните средства, които са релевантни за случая, и че се съхраняват само онези данни, които са абсолютно необходими за разкриването на съответните престъпления.

14 Разбирането на ответника, че самото обстоятелство, че се ползват услуги за достъп до интернет или телефонни услуги, следвало да се счита за достатъчно основание за съхраняването, очевидно не е в съответствие с изложеното по-горе. Позоваването от страна на ответника на становището на Съда от 26 юли 2017 г. относно споразумението между Канада и Европейския съюз относно предаването на резервационни данни на пътниците във въздушния транспорт също не поставя под въпрос изразеното в решение Tele2 Sverige и Watson и др. разбиране, че всяко съхраняване на данни без основание принципно противоречи на правото на Съюза,. Действително Съдът изтъква в контекста на необходимостта от свързаното със споразумението посегателство върху основни права като правото на зачитане на личния живот и правото на защита на личните данни, че предаването на PNR данните на Канада се извършва без оглед на това дали са налице обективни критерии, позволяващи да се приеме, че пътниците могат да представляват заплаха за обществената сигурност в Канада. Въпреки това обаче не е налице съхраняване на данни, за което липсва основание, тъй като съхраняването и предаването се извършват във връзка с граничен контрол, на който съгласно канадското право подлежат всички пътници във въздушния транспорт, които желаят да влязат в Канада или да напуснат Канада. Когато пътниците във въздушния транспорт напуснат страната, това основание за съхраняване отпада. Затова за по-нататъшното съхраняване след този момент е необходимо да са налице — като ново основание — обективни обстоятелства, позволяващи да се приеме, че съответните пътници във въздушния транспорт биха могли да представляват заплаха от гледна точка на борбата с тероризма и с тежката трансгранична престъпност.

15 Ако практиката на Съда трябва да се тълкува в смисъл, че съхраняването на данни без основания при никакви обстоятелства не е съвместимо с правото на Съюза, ревизионната жалба на ответника срещу обжалваното съдебно решение на административния съд не може да бъде уважена. Това се дължи на обстоятелството, че също като шведските и британските разпоредби относно съхраняването, които се разглеждат в решение Tele2 Sverige и Watson и др., член 113a, параграф 1, първо изречение във връзка с член 113b от TKG не изисква да е налице основание за съхраняването, което надхвърля обикновеното ползване на услуги за достъп до интернет или на телефонни услуги, нито изисква да е налице връзка между съхраняваните данни и дадено престъпление или дадена заплаха за обществената сигурност. Напротив, става въпрос за разпоредба, която изисква общо съхраняване на голяма част от всички релевантни далекосъобщителни данни за трафик без основание и без оглед на лицето, периода или географското място.

16 Независимо от изложеното в решение Tele2 Sverige и Watson и др. запитващата юрисдикция обаче счита, че не е изключено, че уреденото в член 113a, параграф 1, първо изречение във връзка с член 113b от TKG задължение за съхраняване на далекосъобщителни данни за трафик без основание да може да се основе на член 15, параграф 1 от Директива 2002/58, по-специално по следните причини:

17 Първо, уредбата във въпросните разпоредби на TKG не изисква съхраняването на всички далекосъобщителни данни за трафик на всички абонати и регистрирани потребители на всички електронни комуникационни средства. От задължението за съхраняване е изключено не само съдържанието на комуникацията, а не се допуска и съхраняването на данни относно посетени интернет страници, данни от услуги за електронна поща, както и на данни, които указват връзките от и към някои линии в социалния сектор и в църковната сфера (вж. член 113b, параграфи 5 и 6 от TKG). Въпреки че изключването на някои комуникационни средства или категории от данни от обхвата на задължението за съхраняване не премахва опасността от съставянето на подробен профил на засегнатото лице, то поне значително я намалява.

18 Второ, според запитващата юрисдикция е налице още по-значителна разлика между разглежданите в случая разпоредби на TKG и предишната разпоредба от Директива 2006/24 и приетите въз основа на нея шведски и британски разпоредби, които се разглеждат в решение Tele2 Sverige и Watson, и др., поради обстоятелството, че съгласно член 113b, параграф 1 от TKG сроковете за съхранение от шест месеца до две години (вж. член 6 от Директива 2006/24) са съществено съкратени до четири и съответно десет седмици.

19 Следва да се приеме, че колкото по-кратки са сроковете, през които се съхраняват данните за трафик, толкова по-малка е опасността от съставянето на подробен профил. Колкото по-кратък е срокът на съхраняване, толкова

по-непълен става по необходимост личностният профил и толкова по-малко интензивно е посегателството върху основните права.

20 Трето, разглежданите в случая разпоредби на TKG подлежат на стриктни ограничения, що се отнася до съхраняваните данни и на достъпа до тях. От една страна, с изискванията, уредени в членове 113d и сл. от TKG, се осигурява ефективна защита на съхраняваните данни срещу рискове от злоупотреба, както и срещу всякакъв неразрешен достъп. Освен това съгласно член 113c, параграф 1 от TKG съхраняваните данни могат да се използват само за борба с тежки престъпления или за предотвратяване на конкретна заплаха за телесната неприкосновеност, живота или свободата на дадено лице или за съществуването на федерацията или на дадена провинция.

21 Съгласно член 100g, параграф 2 от StPO, за да се допусне събирането на данни за трафик за целите на наказателното преследване, е необходимо да е налице подозрение за изрично посочено в закона особено тежко престъпление, като и в конкретния случай престъплението следва да е особено тежко, разследването на обстоятелствата или установяването на местопребиваването на заподозряното лице по друг начин да би било значително затруднено или невъзможно и събирането на данни да е пропорционално на значението на случая. Съгласно член 100g, параграф 4 от StPO не се допуска събирането или използването на данни за трафик, принадлежащи на посочените в член 53, параграф 1, първо изречение, точки 1—5 от StPO лица, които са длъжни да пазят професионална тайна и към които спадат адвокати, лекари или журналисти. Член 101a, параграф 1 от StPO освен това урежда съдебна резерва за събирането на данни за трафик по член 100g от StPO.

22 Действително тези ограничаващи достъпа разпоредби не се прилагат по отношение на адреса по интернет протокол, който е присвоен на абоната за ползване на интернет. Причината за това е, че съгласно член 113c, параграф 1, точка 3 от TKG този адрес може да бъде използван и в рамките на справка със съхраняваните данни за целите на наказателното преследване на всякакви престъпления, предотвратяването на заплахи за обществения ред и сигурност, както и по принцип за изпълнението на функциите на разузнавателните служби. Може да се приеме обаче, че информацията кой абонат на линия е бил регистриран в интернет с вече известен адрес по интернет протокол, не позволява съставянето на личностни профили и профили на движението.

23 Дори ако се приемат доводите на SpaceNet и се допусне, че се използват все повече технически методи, при които адресът по интернет протокол не може еднозначно да се свърже с определена далекосъобщителна линия, а само с по-голяма група от линии и по тази причина справката в съхраняваните данни се е превърнала в мярка, засягаща значителен брой лица, интензивността на посегателството посредством такава справка в

съхраняваните данни е значително по-малка, отколкото при достъп до самите далекосъобщителни данни за трафик и използването им.

24 Четвърто, предположението, че уреденото в член 113a, параграф 1, първо изречение във връзка с член 113b от TKG задължение за съхраняване на далекосъобщителни данни за трафик, без за това да е необходимо конкретно основание, може да се основе на член 15, параграф 1 от Директива 2002/58, се подкрепя и от обстоятелството, че с тази разпоредба националният законодател е изпълнил задълженията си за действие, произтичащи за държавите членки от гарантираното в член 6 от Хартата право на сигурност. В решението Digital Rights Ireland и др. Съдът изрично споменава Хартата и в тази връзка посочва, че борбата с международния тероризъм с оглед на опазване на международния мир и сигурност е цел от общ интерес за Съюза и че същото се отнася и за борбата с тежките престъпления с цел да се гарантира обществената сигурност.

25 Предвид това положение запитващата юрисдикция изпитва съмнения дали досегашната съдебна практика на Съда трябва да се разбира в смисъл, че съхраняване на данните без основание по принцип не може да се основава на член 15, параграф 1 от Директива 2002/58, а не само в конкретния вид, намерил израз в Директива 2006/24 и в основаните на тази директива шведски и британски разпоредби. Всъщност основният замисъл на съхраняването на данни не може да се приведе в съответствие с формулираното без ограничения изискване от страна на Съда съхраняването на данни да е диференцирано според лицата, периодите и географските области.

26 Според запитващата юрисдикция тезата, че съхраняване на данни за трафик без основание само по себе си не е съвместимо с Хартата, се опровергава и от изискването да се постигне равновесие между задълженията на държавите членки да гарантират сигурността на пребиваващите на тяхна територия лица, от една страна, и, от друга страна, да спазват закрепените в членове 7 и 8 от Хартата основни права.

27 Поради това запитващата юрисдикция не може въз основа на практиката на Съда да направи еднозначния извод, че националните законодатели вече нямат възможност на базата на цялостна преценка да въвеждат съхраняване на данни без основание, като евентуално го допълнят със строги правила за достъп, с цел да отчетат специфичния рисков потенциал, свързан с новите далекосъобщителни средства.

28 Пето, в случай че съхраняване на данни без основание принципно не може да се основе на член 15, параграф 1 от Директива 2002/58 и че следователно нямат значение конкретните разпоредби, уреждащи обхванатите комуникационни средства, категориите съхранявани данни, срока на съхраняване, условията за достъп до съхраняваните данни и защитата срещу рискове от злоупотреба, запитващата юрисдикция изтъква, че значително би

била ограничена свободата на действие на националния законодател в областта на наказателното преследване и на обществената сигурност, която съгласно член 4, параграф 2, трето изречение от ДЕС остава единствено в рамките на отговорността на всяка държава членка.

29 Накрая, шесто, запитващата юрисдикция счита, че не е изяснено дали съображенията на Съда в решение Tele2 Sverige и Watson, и др. трябва да се разбират като адресирана до държавите членки забрана да основават на член 15, параграф 1 от Директива 2002/58 въвеждането на задължение за съхраняване на далекосъобщителни данни за трафик без основание, и с оглед на по-новата съдебна практика на Европейския съд по правата на човека (наричан по-нататък „ЕСЧП“).

30 ЕСПЧ неотдавна постанови в решение от 19 юни 2018 г., че шведските правни разпоредби относно цялостния контрол на трансграничния трафик на данни са в съответствие с член 8 от Европейската конвенция за правата на човека (ЕКПЧ). Предвид заплахите, пред които са изправени държавите понастоящем, включително бича на глобалния тероризъм и на други тежки престъпления като трафикът на наркотици, трафикът на хора, сексуалната експлоатация на деца и престъпността в кибернетичното пространство, както и поради техническия напредък, който улеснява терористи и престъпници да избегнат разкриването им в интернет, а също и непредвидимостта на пътищата за предаване на електронни данни, решението за въвеждане на система за цялостен контрол с цел идентифициране на непознати досега заплахи за националната сигурност, продължавало да е в сферата на преценката на държавата (ЕСПЧ, решение от 19 юни 2018 г. – № 35252/08 [ECLI: CE:ECHR:2018:0619JUD003525208], Centrum för Rättvisa/Швеция – т. 112). Доколкото ЕСПЧ изтъква непредвидимостта на пътищата за предаване на електронни данни, както и техническия напредък, който улеснявал терористи и престъпници да избегнат разкриването им в интернет, той подчертава по-настойчиво отколкото Съдът на Европейския съюз, специфичния рисков потенциал, свързан с новите далекосъобщителни средства.

31 Запитващата юрисдикция се позовава на съображение 11 от Директива 2002/58 и на член 52, параграф 3 от Хартата, от които произтича, че следва да се създаде необходимата съгласуваност между закрепените в Хартата основни права и съответните гарантирани от ЕКПЧ права, без това да накърнява самостоятелността на правото на Съюза и на Съда на Европейския съюз.

32 В заключение запитващата юрисдикция посочва други висящи производства по преюдициални запитвания, в които става въпрос за тълкуването на решението Tele2 Sverige и Watson, и др., т.е. дали то съдържа принципна забрана за съхраняване на данни без основание, която не може да бъде преодоляна нито с оглед на сериозността на заплахите за обществената сигурност, срещу които трябва да се води борба, нито в рамките на

„компенсация“ чрез строги правила за достъп и високи изисквания за сигурност.

33 Посочват се преюдициалните запитвания, отправени от Investigatory Powers Tribunal – Лондон (Обединено кралство) (C-623/17), преюдициалните запитвания, отправени от Conseil d’État (Франция) (C-511/18 и C-512/18) и преюдициалните запитвания, отправени от белгийския конституционен съд (C-520/18).