Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
M. CAMPOS SÁNCHEZ-BORDONA
представено на 15 януари 2020 година[1]

Дело C-623/17

Privacy International
срещу
Secretary of State for Foreign and Commonwealth Affairs
Secretary of State for the Home Department
Government Communications Headquarters
Security Service
Secret Intelligence Service

(Преюдициално запитване, отправено от Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство)

„Преюдициално запитване — Обработване на лични данни и зачитане на личния живот в областта на електронните съобщения — Директива 2002/58/ЕО — Приложно поле — Член 1, параграф 3 — Член 15, параграф 3 — Харта на основните права на Европейския съюз — Членове 7, 8, 51 и член 52, параграф 1 — Член 4, параграф 2 ДЕС — Общо и неизбирателно предаване на службите за сигурност на данните за свързване на потребителите на електронна съобщителна услуга“

1. През последните години Съдът се придържа към една постоянна линия в практиката си относно запазването на лични данни и достъпа до тях, като се открояват следните решения:

– решение от 8 април 2014 г., Digital Rights Ireland и др.[2], в което Директива 2006/24/ЕО[3] се приема за невалидна, тъй като допуска непропорционална намеса в правата, гарантирани с членове 7 и 8 от Хартата на основните права на Европейския съюз,

– решение от 21 декември 2016 г., Tele2 Sverige и Watson и др.[4], в което Съдът тълкува член 15, параграф 1 от Директива 2002/58/ЕО[5],

– решение от 2 октомври 2018 г., Ministerio Fiscal[6], в което Съдът потвърждава тълкуването на същата разпоредба от Директива 2002/58.

1 Език на оригиналния текст: испански.

2 Решение по дела C-293/12 и C-594/12, наричано по-нататък „решение Digital Rights“, EU:C:2014:238.

3 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).

4 Решение по дела C-203/15 и C-698/15, наричано по-нататък „решение Tele2 Sverige и Watson“, EU:C:2016:970.

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).

6 Решение по дело C-207/16, наричано по-нататък „решение Ministerio Fiscal“, EU:C:2018:788.

2. Тези съдебни решения (особено второто) притесняват властите на някои държави членки, тъй като според тях имат за последица да ги лишат от средство, което тези държави членки смятат за необходимо за запазването на националната сигурност и за борбата с тероризма. Ето защо някои от тях настояват за изоставянето или за нюансирането на въпросната съдебна практика.

3. Някои юрисдикции на държавите членки изтъкват същите опасения в четири преюдициални запитвания[7], по които представям заключенията си днес.

4. В четирите дела се поставя преди всичко въпросът за прилагането на Директива 2002/58 спрямо дейностите, свързани с националната сигурност и борбата с тероризма. Ако посочената директива се прилага в този контекст, на следващо място трябва да се изясни доколко държавите членки могат да ограничават защитаваните с нея права на неприкосновеност на личния живот. На последно място, следва да се анализира до каква степен различните национални правни уредби (на Обединеното кралство[8], на Белгия[9] и на Франция[10]) в тази област съответстват на правото на Съюза, тълкувано от Съда.

I. Правна уредба

А. Правото на Съюза

5. Препращам към съответните точки от заключението си по дела C-511/18 и C-512/18.

Б. Националното право (приложимо към разглеждания случай)

1. Telecommunications Act 1984[11]

6. Съгласно член 94 министрите могат да дават на оператор на обществена електронна съобщителна мрежа общи или конкретни указания, които според тях са необходими в интерес на националната сигурност или на връзките с правителството на страна или територия извън Обединеното кралство.

2. Data Retention and Investigatory Powers Act 2014[12]

7. Член 1 предвижда:

„(1) Министърът може с разпореждане да задължи обществен далекосъобщителен оператор да запазва релевантни данни за съобщения, ако прецени, че това е необходимо и пропорционално с оглед на една или няколко от целите по член 22, параграф 2, букви a)—h) от Regulation of Investigatory Powers Act 2000 [Закон за уреждане на правомощията по разследване от 2000 г., наричан по-нататък „RIPA“].

7 Освен за настоящото дело става въпрос за дела C-511/18 и C-512/18, La Quadrature du Net и др., и за дело C-520/18, Ordre des barreaux francophones et germanophone и др.

8 Дело Privacy International, C-623/17.

9 Дело Ordre des barreaux francophones et germanophone и др., C-520/18.

10 Дело La Quadrature du Net и др., C-511/18 и C-512/18.

11 Закон за далекосъобщенията от 1984 г., наричан по-нататък „Законът от 1984 г.“

12 Закон за запазването на данните и правомощията по разследване от 2014 г., наричан по-нататък „DRIPA“.

(2) Разпореждането за запазване на данни може:

a) да се отнася до конкретен оператор или до определена категория оператори;

b) да налага запазване на всички данни или на определена категория данни;

c) да определя период или периоди на запазване на данните;

d) да налага други изисквания или ограничения във връзка със запазването на данните;

e) да предвижда различни разпоредби за различни цели;

f) да се отнася до данни, които съществуват или не към момента на издаване или влизане в сила на разпореждането.

(3) Министърът може с наредба да приема допълнителни разпоредби относно запазването на релевантни данни за съобщенията.

(4) Тези разпоредби могат по-специално да уреждат:

a) предварителните изисквания във връзка с приемането на разпореждане за запазване;

b) максималния период, за който трябва да се пазят данните съгласно разпореждане за запазване;

c) съдържанието, приемането, влизането в сила, обжалването, изменението или отмяната на разпореждане за запазване;

d) неприкосновеността, сигурността или защитата на запазените съгласно настоящия член данни, достъпа до тях, както и разкриването или унищожаването им;

e) прилагането на релевантните изисквания или ограничения и проверката дали тези изисквания или ограничения се спазват;

f) кодекс за добри практики относно релевантните изисквания, ограничения или правомощия;

g) възстановяването от министъра (при определени условия или безусловно) на разходите на обществените далекосъобщителни оператори за изпълнение на релевантните изисквания или ограничения;

[…]

(5) Максималният период по параграф 4, буква b) не трябва да надвишава дванадесет месеца, считано от датата, посочена за съответните данни в наредбата по параграф 3.

(6) Обществен далекосъобщителен оператор, който запазва релевантни данни за съобщенията в съответствие с настоящия член, не може да разкрива тези данни, освен:

a) по силата на:

(i) част 1, глава 2 от [RIPA] или

(ii) съдебно решение, друго съдебно разрешение или съдебна заповед, или

b) ако това е предвидено в наредбата по параграф 3.

(7) С наредба на министъра може да се предвидят разпоредби — съответстващи на която и да е от разпоредбите, които са приети (или може да бъдат приети) по силата на параграф 4, букви d) —g) или с параграф 6 — във връзка с данните за съобщения, запазени от доставчиците на далекосъобщителни услуги в съответствие с кодекс за добри практики по член 102 от Закона за противодействие на тероризма, тежката престъпност и за сигурността от 2001 г. [Anti-terrorism, Crime and Security Act 2001]“.

3. RIPA

8. Член 21 гласи:

„[…]

(4) В тази глава „данни за съобщения“ означава:

a) всякакви данни за трафик, съдържащи се във или приложени към съобщение (от подателя или по друг начин) за целите на всякаква пощенска услуга или далекосъобщителна система, чрез която те се предават или могат да бъдат предадени;

b) всякаква информация, която не включва никаква част от съдържанието на съобщението (освен информацията по буква a) и се отнася до използването от което и да е лице на:

(i) всякаква пощенска или далекосъобщителна услуга или

(ii) всякаква част от далекосъобщителна система във връзка с доставката или използването от което и да е лице на всякаква далекосъобщителна услуга;

c) всякаква информация извън тази по букви a) или b), която лице, предоставящо пощенска или далекосъобщителна услуга, притежава или получава във връзка с лицата, на които предоставя услугата.

[…]

(6) В този раздел „данни за трафика“ (във връзка с всяко съобщение) означава:

a) всякакви данни, които идентифицират или могат да идентифицират всяко лице, оборудване или местонахождение, до което или от което се предава или може да се предаде съобщение;

b) всякакви данни, които идентифицират или определят, или които могат да идентифицират или определят оборудването, чрез което се предава или може да се предаде съобщението;

c) всякакви данни, включващи сигнали за задействане на оборудването, използвано в далекосъобщителната система за целите на предаването на всякакви съобщения; и

d) всякакви данни, които идентифицират данните, съдържащи се във или приложени към конкретно съобщение, или други данни като данни, съдържащи се във или приложени към конкретно съобщение.

[…]“.

9. Член 22 предвижда:

„(1) Този член се прилага в случаите, когато отговорно лице по тази глава счита за необходимо да получи данни за съобщения по съображенията, посочени в параграф 2.

(2) Получаването на данни е необходимо, когато се налага по следните съображения:

a) в интерес е на националната сигурност;

b) служи за предотвратяване или разкриване на престъпления или предотвратяване на нарушения на обществения ред;

c) в интерес е на икономическото благосъстояние на Обединеното кралство, стига този интерес да е релевантен и с оглед на гарантирането на националната сигурност;

d) в интерес е на обществената сигурност;

e) служи за защита на общественото здраве;

f) служи за определяне на данъчната основа или за събиране на данъци, мита, такси или други дължими на публичната администрация налози, вноски или суми;

g) служи за предотвратяване в спешни случаи на смърт, нараняване или друго увреждане на физическото или психическото здраве на лице или за ограничаване на нараняване или увреждане на физическото или психическото здраве на лице;

h) служи за други цели (извън посочените в букви a)—g), посочени в заповед на министъра съгласно член 22, параграф 2, буква h) от [DRIPA].

(4) При условията на параграф 5 съответното отговорно лице може, ако счита, че далекосъобщителен или пощенски оператор разполага, би могъл да разполага или би могъл да получи определени данни, да задължи този далекосъобщителен или пощенски оператор:

a) да получи данните, ако още не разполага с тях, и

b) при всяко положение, да му разкрие всички данни, с които разполага или които е получил впоследствие.

5) Отговорното лице дава разрешение по параграф 3 или издава разпореждане по параграф 4 само ако счита, че получаването на въпросните данни в резултат на действията, разрешени или разпоредени с разрешението или разпореждането, е пропорционално на преследваната с получаването на данните цел“.

10. Съгласно член 65, ако има причини да се смята, че определени данни са получени неправомерно, следва да бъде сезиран Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство).

II. Фактите и преюдициалните въпроси

11. Според запитващата юрисдикция главното производство се отнася до получаването и използването от United Kingdom Security and Intelligence Agencies (служби за сигурност и разузнаване на Обединеното кралство, наричани по-нататък „ССР“) на масиви с данни за съобщения.

12. Тези данни се отнасят до това „кой“ използва телефон и интернет и „кога, къде, как и с кого“ ги използва. Те включват и местонахождението на мобилните и фиксираните телефони, от които са направени или са приети обаждания, както и на компютрите, които са използвани за достъп до интернет. Не включват съдържанието на съобщенията, което може да бъде получено само въз основа на съдебно решение.

13. Жалбоподателят в главното производство (Privacy International, неправителствена организация за защита на правата на човека) е сезирал запитващата юрисдикция, тъй като счита, че получаването и използването на посочените данни от ССР накърняват правото на зачитане на личния живот, закрепено в член 8 от Европейската конвенция за защита на правата на човека и основните свободи (наричана по-нататък „ЕКПЧ“), и противоречат на правото на Съюза.

14. Ответниците [13] твърдят, че упражняването на правомощията им в тази област е законно и е от съществено значение по-специално за защитата на националната сигурност.

15. Видно от информацията, съдържаща се в акта за преюдициално запитване, в съответствие с указанията, дадени от министъра съгласно член 94 от Закона от 1984 г., ССР получават масиви с данни за съобщенията, осъществени посредством операторите на обществените електронни съобщителни мрежи.

16. Тези данни включват информация за трафика и за местонахождението, както и за обществените, търговските и финансовите дейности, съобщенията и пътуванията на потребителите. Щом се сдобият с тях, ССР съхраняват тези данни по надежден начин, използвайки техники (като например филтриране и агрегация), които не са целеви, тоест, не са насочени към конкретни, известни обекти.

17. Запитващата юрисдикция приема за доказано, че тези техники са от съществено значение за работата на ССР в областта на борбата със сериозни заплахи за обществената сигурност, по-специално с тероризма, шпионажа и разпространението на ядрени оръжия. Според тази юрисдикция възможността на ССР да получават и използват данните, е от ключово значение за защитата на националната сигурност на Обединеното кралство.

18. Запитващата юрисдикция смята, че спорните мерки съответстват на вътрешното право и на член 8 от ЕКПЧ. Тя обаче има съмнения относно съвместимостта им с правото на Съюза с оглед на решение Tele2 Sverige и Watson.

19. В този контекст запитващата юрисдикция отправя до Съда следните преюдициални въпроси:

„1) Попада ли — предвид член 4 ДЕС и член 1, параграф 3 от Директива 2002/58 […] — в обхвата на правото на Съюза и на Директива [2002/58] съдържащо се в указание на министър до доставчик на електронна съобщителна мрежа разпореждане, съгласно което последният трябва да предоставя масиви с данни за съобщения на службите за сигурност и разузнаване на държава членка (ССР)?

2) Ако отговорът на първия въпрос е утвърдителен, прилагат ли се по отношение на такова указание на министър някои от изискванията съгласно решение Watson [14] или някакви други изисквания, освен предвидените в ЕКПЧ? Ако това е така, как и до каква степен се прилагат

13 Secretary of State for Foreign and Commonwealth Affairs (министър на външните работи и на Общността на нациите), Secretary of State for the Home Department (министър на вътрешните работи) и трите ССР на Обединеното кралство, а именно Government Communications Headquarters (Централа за правителствените комуникации, наричана по-нататък „GCHQ“), Security Service (Служба за сигурност, наричана по-нататък „MI5“) и Secret Intelligence Service (Служба за тайно разузнаване, наричана по-нататък „MI6“).

14 Тоест съдебната практика, установена с решение Tele2 Sverige и Watson.

тези изисквания, като се имат предвид съществената необходимост ССР да прибягват до масово събиране и техники за автоматизирана обработка с цел защита на националната сигурност и степента, в която тези иначе съответстващи на ЕКПЧ възможности могат да бъдат сериозно възпрепятствани от налагането на такива изисквания?“.

20. Запитващата юрисдикция поставя въпросите си в следния контекст:

„а) възможностите ССР да използват предоставени им [масиви с данни за съобщения] са от съществено значение за защитата на националната сигурност на Обединеното кралство, включително в областта на борбата с тероризма, шпионажа и разпространението на ядрени оръжия;

б) ССР използват [тези данни] основно за разкриването на неизвестни до момента заплахи за националната сигурност чрез техники за нецелево събиране, разчитащи на натрупването на [тези данни] на едно място. Главната полза от това е бързото идентифициране и разработка на обекта, както и осигуряването на основа за действие при наличието на непосредствена заплаха;

в) впоследствие (след изтичане на срока съгласно обичайните си търговски изисквания) доставчикът на електронна съобщителна мрежа не е длъжен да пази въпросните данни, които се запазват от самата държава (ССР);

г) националната юрисдикция приема (без това да предрешава отговора на някои въпроси, които ще бъдат разгледани допълнително), че гаранциите, свързани с използването на [тези данни] от ССР, съответстват на изискванията на ЕКПЧ, и

д) националната юрисдикция приема, че налагането на изискванията, определени в [решение Tele2 Sverige и Watson], доколкото са приложими, би осуетило вземаните от ССР мерки за гарантиране на националната сигурност, като по този начин би изложило на опасност националната сигурност на Обединеното кралство“.

III. Производството пред Съда

21. Преюдициалното запитване постъпва в Съда на 31 октомври 2017 г.

22. Писмени становища представят правителството на Обединеното кралство, германското, белгийското, чешкото, кипърското, испанското, естонското, френското, унгарското, ирландското, латвийското, нидерландското, норвежкото, полското, португалското и шведското правителство, както и Комисията.

23. Открито съдебно заседание е проведено на 9 септември 2019 г. съвместно със заседанията по дела C-511/18, C-512/18 и C-520/18, като се явяват или съответно са представлявани страните в главните производства по четирите преюдициални запитвания, посочените по-горе правителства, както и Комисията и Европейският надзорен орган по защита на данните.

IV. Анализ

A. Относно приложното поле на Директива 2002/58 и изключването на националната сигурност (първи преюдициален въпрос)

24. В заключението си от днешна дата по дела C-511/18 и C-512/18 разяснявам причините, поради които според мен Директива 2002/58 „по принцип се прилага, когато доставчиците на електронни съобщителни услуги са задължени от закона да запазват данните на своите абонати и да позволяват на публичните органи да имат достъп до тях. Този извод не се променя от обстоятелството, че задълженията се налагат на доставчиците от съображения за национална сигурност“ [15].

25. При излагане на съображенията ми във въпросното заключение разглеждам отражението на решение на Съда от 30 май 2006 г., Парламент/Съвет и Комисия [16], и на решение Tele2 Sverige и Watson, като предлагам съгласувано тълкуване на тези две решения [17].

26. В същото заключение, след като потвърждавам приложимостта на Директива 2002/58, анализирам въпроса за предвиденото в тази директива изключване на националната сигурност и за отражението на член 4, параграф 2 ДЕС [18].

27. Без да се засягат съображенията, които ще изложа по-долу, препращам към вече изложеното в посоченото заключение и в това по дело C-520/18.

1. Прилагане на Директива 2002/58 в разглеждания случай

28. Съгласно спорните разпоредби доставчиците на електронни съобщителни услуги имат задължение не само за запазване, но и за обработване на данните, с които разполагат във връзка с услугата, която предоставят на потребителите на обществените съобщителни мрежи на Съюза [19].

29. Всъщност посочените оператори трябва задължително да предават тези данни на ССР. Поставя се въпросът дали член 15, параграф 1 от Директива 2002/58 допуска това предаване, с оглед на целта му, да се изключи автоматично от обхвата на правото на Съюза.

30. Не мисля, че това е така. Запазването на въпросните данни и последващото им предаване могат да се квалифицират като обработване на лични данни от доставчиците на електронни съобщителни услуги, поради което естествено попадат в приложното поле на Директива 2002/58.

15 Вж. заключението по дела C-511/18 и C-512/18, т. 42.

16 Дела C-317/04 и C-318/04, EU:C:2006:346.

17 Вж. заключението по дела C-511/18 и C-512/18, т. 44—76.

18 Пак там, т. 77—90.

19 Съгласно член 2 от Директива 2002/58 за целите на тази директива се прилагат дефинициите от Директива 95/46. Съгласно член 2, буква б) от последната „обработване на лични данни“ е „всяка операция или набор от операции, извършвани или не с автоматични средства, прилагани към личните данни, като събиране, запис, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, *разкриване чрез предаване*, разпространяване или *друга форма на предоставяне на данните*, [подреждане] или комбиниране, блокиране, изтриване или унищожаване“ (курсивът е мой).

31. Съображенията за национална сигурност не могат да засегнат този извод, както твърди запитващата юрисдикция, така че спорното задължение да остане извън приложното поле на правото на Съюза. Според мен, повтарям, на доставчиците се налага задължение за обработване на данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществените съобщителни мрежи на Съюза, което е именно приложното поле на Директива 2002/58 съгласно член 3, параграф 1 от нея.

32. Изхождайки от тази предпоставка, фокусът се измества и вече не е върху дейностите на ССР (които, както вече посочих, биха могли да попадат извън обхвата на правото на Съюза, ако не засягат операторите на електронни съобщителни услуги), а върху запазването и последващото предаване на наличните при тези оператори данни. От тази гледна точка се намесват основните права, гарантирани от Съюза.

33. Ключовият фактор за разрешаването на настоящия спор отново е задължението за общо и неизбирателно запазване на данните, до които публичните органи получават достъп.

2. Позоваването на националната сигурност

34. Тъй като в разглеждания случай запитващата юрисдикция специално набляга на дейностите на ССР, засягащи националната сигурност, в това отношение си позволявам да възпроизведа няколко точки от заключението ми от днешна дата по дела C-511/18 и C-512/18:

„77. Националната сигурност […] е разгледана на две места в Директива 2002/58. От една страна, тя съставлява основание за изключване (на прилагането на тази директива) на всички онези дейности на държавите членки, „отнасящи се“ по-специално до нея. От друга страна, тя присъства и като основание за ограничаване — което трябва да се извърши посредством закон — на правата и задълженията, предвидени в Директива 2002/58, тоест що се отнася до частноправни или търговски по естеството си дейности, които са чужди на властническите дейности на държавата.

78. До кои дейности се отнася член 1, параграф 3 от Директива 2002/58? Според мен самият Conseil d'État (Държавен съвет) дава добър пример, като споменава членове L. 851-5 и L. 851-6 от Кодекса за вътрешната сигурност, които се отнасят до „използваните пряко от държавата средства за събиране на разузнавателна информация, без да уреждат дейностите на доставчиците на електронни съобщителни услуги, като им налагат конкретни задължения“ […].

79. Смятам, че именно тук се крие ключът за определянето на обхвата на изключването по член 1, параграф 3 от Директива 2002/58. Режимът по нея не се прилага спрямо *дейностите*, които са насочени към запазване на националната сигурност и които се извършват от публичните органи за тяхна сметка, без да е необходимо съдействие от страна на частноправни субекти и следователно без на последните да се налагат задължения във връзка с управлението на тяхната дейност.

80. Наборът от дейности на публичните органи, които са изключени от общия режим за обработване на личните данни, трябва обаче да се тълкува ограничително. По-конкретно понятието за *национална сигурност*, която в съответствие с член 4, параграф 2 ДЕС остава единствено в рамките на отговорността на всяка държава членка, не може да се разпростира към други области на обществения живот, повече или по-малко близки.

[…]

82. […] считам, че за ориентир може да послужи критерият по Рамково решение 2006/960/ПВР[…], в член 2, буква а) от което се прави разграничение между правоприлагащи органи в широк смисъл — които обхващат „национален полицейски, митнически или друг орган, който е оправомощен по националното право да открива, предотвратява и разследва престъпления или престъпна дейност, както и да упражнява власт и да предприема принудителни мерки в контекста на такива дейности“ — от една страна, и „[а]генциите или звената, занимаващи се изключително с въпроси на националната сигурност“, от друга страна[…].

[…]

84. […] налице [е] приемственост между Директива 95/46 и Директива 2002/58, що се отнася до правомощията на държавите членки във връзка с националната сигурност. Никоя от двете няма за предмет защитата на основните права в тази специфична област, в която дейностите на държавите членки не се „управляват от законодателството на [Съюза]“.

85. Посоченият [в] съображение [11 от Директива 2002/58] „баланс“ следва от необходимостта да се зачитат правомощията на държавите членки в областта на националната сигурност, когато ги упражняват *пряко и със собствени средства*. Обратно, когато — включително по същите съображения за национална сигурност — е необходимо съдействие от страна на частноправни субекти, на които се налагат определени задължения, това обстоятелство определя попадането в сфера (защитата на неприкосновеността на личния живот, изисквана от тези частноправни субекти), която се урежда от правото на Съюза.

86. Както Директива 95/46, така и Директива 2002/58 се опитват да постигнат този баланс, допускайки правата на частноправните субекти да могат да бъдат ограничавани по силата на законодателни мерки, приети от държавите в съответствие с член 13, параграф 1 и член 15, параграф 1 от съответните директиви. В това отношение няма никаква разлика между двете.

[…]

89. Определянето на тези дейности на публичната власт трябва по необходимост да бъде ограничително, като в противен случай би се лишила от полезно действие правната уредба на Съюза в областта на защитата на неприкосновеността на личния живот. В член 23 от Регламент № 2016/679 се предвижда — в съответствие с член 15, параграф 1 от Директива 2002/58 — ограничаването *чрез законодателна мярка* на предвидените в него права и задължения, когато това е необходимо с цел да се гарантира в частност националната сигурност, отбраната или обществената сигурност. Отново, ако преследването на тези цели беше достатъчно за изключване от приложното поле на Регламент № 2016/679, би било излишно националната сигурност да се посочва като основание за ограничаване чрез законодателни мерки на правата, гарантирани с този регламент“.

3. Последиците от прилагането в настоящия случай на решение Tele2 Sverige и Watson

35. Запитващата юрисдикция се концентрира върху тълкуването, дадено от Съда в решение Tele2 Sverige и Watson, като излага трудностите, които според нея са свързани с неговото прилагане в настоящия случай.

36. Всъщност в решение Tele2 Sverige и Watson се посочват условията, на които трябва да отговаря национална правна уредба, която въвежда задължението за запазване на данни за трафик и за местонахождение с цел последващ достъп до тях от страна на публичните органи.

37. Както по дела C-511/18 и C-512/18 (и по аналогични съображения) считам, че националните разпоредби, до които се отнася настоящото преюдициално запитване, не отговарят на условията, предвидени в решение Tele2 Sverige и Watson, тъй като предвиждат общо и неизбирателно запазване на лични данни, позволяващо да се изгради детайлна картина на живота на засегнатите лица през дълъг период от време.

38. В заключението по посочените дела поставям въпроса дали е възможно нюансиране или допълване на практиката, установена с въпросното съдебно решение, предвид последиците от нея за борбата с тероризма или за защитата на държавата от други аналогични заплахи за националната сигурност.

39. Позволявам си по-долу да възпроизведа още няколко точки от въпросното заключение, в което основно поддържам, че след като е възможно нюансиране на посочената съдебна практика, тя трябва да бъде потвърдена по същество:

„135. Макар да е трудно, не е невъзможно да се определят точно и съгласно обективни критерии както категориите данни, чието запазване се счита за необходимо, така и кръгът на засегнатите лица. Вярно е, че най-*практично и ефективно* би било общото и неизбирателно запазване на толкова данни, колкото могат да получат доставчиците на електронни съобщителни услуги, но […] въпросът не може да се решава с оглед на *практическата ефективност*, а трябва да се разглежда с оглед на *правната ефективност* и в контекста на правовата държава.

136. Тази дейност по определяне е типично законодателна дейност, ограничена от рамките на практиката на Съда. […]

137. Изхождайки от предпоставката, че операторите са събрали данните по начин, съответстващ на разпоредбите на Директива 2002/58, и че запазването им се е извършило на основание член 15, параграф 1[…], достъпът на компетентните органи до тази информация трябва да се осъществява при условията, които са определени от Съда и които анализирам в заключението си по дело C-520/18, към което препращам.

138. Затова също и в този случай националната правна уредба трябва да определи материалните и процесуалните условия за достъп на компетентните органи до запазените данни[…]. В контекста на разглежданите преюдициални запитвания тези условия биха позволили достъпа до данните на лицата, които са заподозрени, че подготвят, ще извършат или са извършили терористичен акт или че може да са замесени в такова престъпление […].

139. От съществено значение е обаче — освен в надлежно обосновани неотложни случаи — достъп до въпросните данни да се предоставя след предварителен контрол, осъществен от юрисдикция или от независим административен орган, чието решение се приема след мотивирана молба на компетентните органи[…]. По този начин там, където абстрактната уредба в закона не е достатъчна, се осигурява *конкретната* преценка на този независим орган, който също е задължен да гарантира държавната сигурност и защитата на основните права на гражданите“.

Б. По втория преюдициален въпрос

40. Запитващата юрисдикция поставя втория си въпрос, в случай че отговорът на първия е утвърдителен. В този случай тя иска да установи какви „други изисквания, освен предвидените в ЕКПЧ“ или произтичащите от решение Tele2 Sverige и Watson, би трябвало да се прилагат.

41. В това отношение тя посочва, че прилагането на условията съгласно решение Tele2 Sverige и Watson „би осуетило вземаните от ССР мерки за гарантиране на националната сигурност“.

42. Тъй като предлагам на първия въпрос да се даде отрицателен отговор, не е необходимо да се разглежда вторият. Както подчертава самата запитваща юрисдикция, вторият въпрос зависи от това да се приемат за съвместими с правото на Съюза „масово[то] събиране и техники[те] за автоматизирана обработка“ на лични данни на всички потребители в Обединеното кралство, които операторите на електронни съобщителни услуги ще трябва да предават на ССР.

43. Ако Съдът счете за необходимо да даде отговор на втория въпрос, смятам, че би трябвало да потвърди условията съгласно решение Tele2 Sverige и Watson във връзка със:

– забраната на общия достъп до данните,

– необходимостта от предварително разрешение от съд или независим орган, за да се оправдае този достъп,

– задължението за информиране на засегнатите лица, освен ако по този начин се засяга ефективността на мярката,

– запазването на данните в рамките на Европейския съюз.

44. Повтарям, че е достатъчно тези задължително приложими условия да се потвърдят по причините, изложени в заключенията ми по дела C-511/18 и C-512/18 и C-520/18, без да е необходимо да се въвеждат „други“ допълнителни изисквания в смисъла, посочен от запитващата юрисдикция.

V. Заключение

45. С оглед на всичко изложено по-горе предлагам на Съда да отговори на Investigatory Powers Tribunal (Съд за контрол върху правомощията по разследване, Обединено кралство) по следния начин:

„Член 4 ДЕС и член 1, параграф 3 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) трябва да се тълкуват в смисъл, че не допускат национална правна уредба, задължаваща доставчик на електронна съобщителна мрежа да предоставя на службите за сигурност и разузнаване на държава членка „масиви с данни за съобщения“, които масиви предполагат предварителното общо и неизбирателно събиране на въпросните данни“.

При условията на евентуалност:

„Достъпът от страна на службите за сигурност и разузнаване на държава членка до данните, предавани от доставчиците на електронни съобщителни мрежи, трябва да отговаря на условията, предвидени в решение от 21 декември 2016 г., Tele2 Sverige и Watson (C-203/15 и C-698/15, EU:C:2016:970)“.