Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
Y. BOT
представено на 23 септември 2015 година [1]

Дело C-362/14

Maximillian Schrems
срещу
Data Protection Commissioner
(Преюдициално запитване,

отправено от High Court (Ирландия)

„Преюдициално запитване — Лични данни — Защита на физическите лица при обработването на тези данни — Харта на основните права на Европейския съюз — Членове 7, 8 и 47 — Директива 95/46/ЕО — Член 25 — Решение 2000/520/ЕО — Прехвърляне на лични данни към САЩ — Оценка на достатъчната или недостатъчната степен на защита — Жалба от физическо лице, чиито данни са прехвърлени към трета страна — Национален надзорен орган — Правомощия“

I – **Въведение**

1. В съобщението си от 27 ноември 2013 г. [2] Европейската комисия констатира, че „[п]редаването на лични данни е важен и необходим елемент на трансатлантическите отношения. То представлява неразделна част от търговския обмен между Европа и САЩ, включително в новите бързоразвиващи се сектори в областта на цифровите технологии, като например социалните медии или изчисленията в облак, които предполагат преминаването на големи количества данни от ЕС към САЩ“ [3].

2. Търговският обмен е предмет на уредба в Решение 2000/520/ЕО на Комисията от 26 юли 2000 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ [4]. Това решение предоставя правно основание за прехвърляне на лични данни от Съюза към установени в САЩ предприятия, които се придържат към принципите за сфера на неприкосновеност.

3. Пред посоченото решение днес стои предизвикателството да послужи за допускане на потоците от данни между Съюза и САЩ, като същевременно се гарантира висока степен на защита на тези данни съгласно изискванията на правото на Съюза.

1 — Език на оригиналния текст: френски.

2 — Съобщение на Комисията до Европейския парламент и Съвета, озаглавено „Възстановяване на доверието в обмена на данни между ЕС и САЩ“ (COM(2013) 846 окончателен).

3 — Стр. 2.

4 — ОВ L 215, стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64.

4. Всъщност след поредица от разкрития наскоро се установи наличието на широкомащабни американски програми за събиране на информация. Тези разкрития внесоха смущения във връзка със спазването на нормите на правото на Съюза при прехвърлянето на лични данни към установени в САЩ предприятия и със слабостите на схемата за сфера на неприкосновеност.

5. С настоящото преюдициално запитване Съдът е приканен да уточни какво поведение трябва да възприемат националните надзорни органи и Комисията, когато се сблъскват с нередности при прилагането на Решение 2000/520.

6. В глава IV от Директива 95/46/ЕО 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[5] се предвиждат правила за прехвърляне на лични данни към трети страни.

7. В член 25, параграф 1 от същата глава от Директивата се въвежда принципът, че прехвърлянето на лични данни, които са подложени на обработка или са предназначени за обработка след прехвърлянето им към трета страна, може да се извършва само ако въпросната трета страна гарантира достатъчна степен на защита на тези данни.

8. От друга страна обаче, както законодателят на Съюза посочва в съображение 57 от посочената директива, прехвърлянето на лични данни към трета страна, която не гарантира достатъчно висока степен на защита, трябва да бъде забранено.

9. Съгласно член 25, параграф 2 от Директива 95/46 „[д]остатъчният характер на степента на защита, предоставяна от трета страна, се преценява в светлината на всички обстоятелства, свързани с операцията по предаването на данни или набор от операции по предаване на данни; специално внимание се обръща на характера на данните, целта и продължителността на предлаганата операция или операции по обработката им, на страната по произхода и страната по крайното местоназначение, на законовите правила, както общи, така и секторни, които са в сила във въпросната трета страна, както и на професионалните правила и мерките за сигурност, които се спазват в тази страна“.

10. По силата на член 25, параграф 6 от тази директива Комисията може да констатира, че трета страна гарантира достатъчна степен на защита на личните данни по силата на вътрешното си законодателство или на международните си споразумения. Щом Комисията приеме решение в този смисъл, прехвърлянето на лични данни към съответната трета страна може да бъде извършено.

11. Въз основа на тази разпоредба Комисията приема Решение 2000/520. Съгласно член 1, параграф 1 от това решение „принципите за „сфера на неприкосновеност на личния живот“, прилагани съгласно предоставените в „често задаваните въпроси“[6] насоки, се считат за гарантиращи достатъчна степен на защита на личните данни, прехвърляни от Съюза към установени в САЩ предприятия.

12. Следователно Решение 2000/520 разрешава прехвърлянето на лични данни от държавите членки към установени в САЩ предприятия, които са се задължили да спазват принципите за сфера на неприкосновеност.

5 — ОВ L 281, стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10; изменена с Регламент (ЕО) № 1882/2003 на Европейския парламент и на Съвета от 29 септември 2003 г. (ОВ L 284, стр. 1; Специално издание на български език, 2007 г., глава 1, том 4, стр. 213, наричана по-нататък „Директива 95/46“).

6 — Често задавани въпроси, наричани по-нататък „ЧЗВ“.

13. В приложение I към Решение 2000/520 се посочват определен брой принципи, към които предприятията могат доброволно да се придържат, и са предвидени ограничения и специална система за контрол. През 2013 г. броят на предприятията, които се придържат към това, което може да се квалифицира като „кодекс за поведение“, надхвърля 3 200.

14. В основата на схемата за сфера на неприкосновеност стои разрешение, което обединява самосертифициране и самооценка от страна на частните предприятия и намеса от страна на публичната власт.

15. Принципите за сфера на неприкосновеност са изготвени „след съгласуване с предприятията и широката общественост с цел насърчаване на търговията между Съединените щати и [Съюза]. Те са предназначени единствено за американските организации, които получават лични данни, произхождащи от [Съюза], с цел тези организации да изпълнят условията за сфера на неприкосновеност[, за да се ползват от] презумпцията за „ниво на адекватна защита“, произтичаща от нея“ [7].

16. Принципите за сфера на неприкосновеност, съдържащи се в приложение I към Решение 2000/520, по-специално предвиждат:

— изискване за уведомяване, по силата на което „[в]сяка организация трябва да информира физическите лица за причините за събирането и използването на лична информация, за начините да се свържат с нея за запитвания или оплаквания, за видовете трети лица, на които тази информация ще бъде разкрита, за възможностите за избор и средствата, които предлага организацията на физическите лица с оглед ограничаване използването и разкриването на тези данни. Известието трябва да бъде предоставено […], когато заинтересованите лица бъдат поканени за първи път да предоставят личната информация на организацията или веднага след като стане възможно, но във всеки случай, преди тези данни да бъдат използвани от организацията за цел, различна от тази, за която са били първоначално събрани или обработени от организацията, която извършва предаването или разкриването им за първи път на трето лице“ [8];

— задължение за организациите да предоставят на физическите лица възможността да изберат дали данните им могат да бъдат разкрити на трето лице или да бъдат използвани за несъвместими цели с предназначението или предназначенията, за които тези данни са били първоначално събрани или за които по-късно са получили разрешение от физическото лице. Що се отнася до чувствителната информация, „всяко лице трябва да има възможността да направи своя утвърждаващ или изричен избор („opt in“), при условие че информацията трябва да бъде разкрита на трето лице или използвана за цел, различна от първоначалната, когато е била първоначално събрана или за която по-късно е получено разрешение от физическото лице посредством упражняването от него на правото му на избор“ [9];

— правила относно последващото прехвърляне на данни. Така, „[з]а да разкрият информация на трето лице, организациите трябва да прилагат принципите на [нотификация] и на избор“ [10];

— по отношение на сигурността на данните, задължение за „[о]рганизациите, които създават, поддържат, използват или разпространяват лична информация, […] да вземат необходимите предпазни мерки, за да предотвратят загубата, злоупотребата, непозволения достъп, разкриването, изменението и унищожаването на тези данни“ [11];

7 — Приложение I, втора алинея към Решение 2000/520.

8 — Вж. приложение I, точка „Нотификация“.

9 — Вж. приложение I, точка „Избор“.

10 — Вж. приложение I, точка „Последващо предаване“.

11 — Вж. приложение I, точка „Сигурност“.

— по отношение на пълнотата на данните, задължение за организациите „да взем[ат] подходящите мерки[…], за да гарантира[т] надеждност на данните по отношение на предвиденото им използване, както и тяхната коректност, пълнота и актуалност“ [12];

— че съответното лице, с чиито данни разполага организация, по принцип трябва „да има достъп до тези данни и трябва да има възможността да ги коригира, променя или заличава, когато са неточни“ [13];

— задължение да се предвидят „механизми, които да гарантират спазването на принципите на личната неприкосновеност, да се предвиди право за подаване на жалби за заинтересованите физически лица, засегнати от неспазването на принципите, както и да се санкционират организациите, които не са приложили принципите“ [14].

17. Американска организация, която иска да се придържа към принципите за сфера на неприкосновеност, е длъжна да предвиди в политиката си за защита на личния живот, че оповестява публично придържането си към тези принципи и действително ги съблюдава, както и да се самосертифицира, декларирайки в Департамента по търговия на САЩ, че спазва посочените принципи [15].

18. Организациите разполагат с редица начини за съобразяване с принципите за сфера на неприкосновеност. Така например те могат да „участва[т] в саморегулаторна програма за защита на личните данни, която се основава на тези принципи [или] да отговор[ят] на условията за сфера на неприкосновеност, като разработ[ят] свои саморегулаторни политики по отношение на защитата на личния живот, при условие че тези правила съответстват на принципите.[…] Освен това, когато дадени организации са предмет на регулиране от законови, подзаконови, административни или други правни разпоредби (или съвкупност от правила), които дават ефективна защита на личните данни, те могат също да се ползват от предимствата на сферата на неприкосновеност“ [16].

19. Съществуват редица механизми, обединяващи частния арбитраж и контрола на публичните органи, за проверка на спазването на принципите за сфера на неприкосновеност. Така контролът може да се осигурява посредством система за алтернативно разрешаване на спорове от независима трета страна. Освен това предприятията могат да се задължат да сътрудничат с Групата на Европейския съюз за защита на данните. Накрая, компетентни по разглеждането на жалбите са Федералната търговска комисия (Federal Trade Commission, наричана по-нататък „FTC“) въз основа на правомощията, които са ѝ предоставени в раздел 5 от Закона за Федералната търговска комисия (Federal Trade Commission Act), както и Департаментът по транспорт (Department of Transportation) въз основа на правомощията, които са му предоставени по силата на глава 49 от Кодекса на САЩ (United States Code), раздел 41 712.

20. Съгласно четвърта алинея от приложение I към Решение 2000/520 придържането към принципите за сфера на неприкосновеност може да бъде ограничено по-специално „до необходимата степен, с оглед спазване изискванията за националната сигурност, обществения интерес или изискванията на правоприлагането [в САЩ]“ и „със закон, правителствено регулиране или съдебна практика, които пораждат взаимнопротиворечиви задължения или

12 — Вж. приложение I, точка „Пълнота на данните“.

13 — Вж. приложение I, точка „Достъп“.

14 — Вж. приложение I, точка „Прилагане“.

15 — Член 1, параграфи 2 и 3 от Решение 2000/520. Вж. също приложение II, ЧЗВ 6.

16 — Приложение I, трета алинея.

предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на принципите е ограничено до необходимата степен за гарантиране на първостепенните законово предвидени интереси, за които е поискано разрешителното“ [17].

21. Освен това възможността на компетентните органи на държавите членки да спрат потока от данни е подчинена на редица условия, които са предвидени в член 3, параграф 1 от Решение 2000/520.

22. В настоящото преюдициално запитване възниква въпросът за обхвата на Решение 2000/520 с оглед на членове 7, 8 и 47 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“), както и на член 25, параграф 6 и член 28 от Директива 95/46. Запитването е отправено в рамките на спор между г-н Schrems и Data Protection Commissioner (Комисар за защита на личните данни, наричан по-нататък „Комисарят“) относно отказа на последния да проведе разследване по жалба, подадена от г-н Schrems, поради това че Facebook Ireland Ltd. (наричано по-нататък „Facebook Ireland“) съхранява личните данни на абонатите си на намиращи се в САЩ сървъри.

23. Г-н Schrems е пребиваващ в Австрия гражданин на тази държава. Абонат е на социалната мрежа Facebook от 2008 г.

24. От всички пребиваващи на територията на Съюза абонати на Facebook се изисква да подпишат договор с Facebook Ireland, което е дъщерно дружество на дружеството майка Facebook Inc. със седалище в САЩ (наричано по-нататък „Facebook USA“). Данните на пребиваващите на територията на Съюза абонати на Facebook Ireland изцяло или частично се прехвърлят на разположени на територията на САЩ сървъри на Facebook USA, където се съхраняват.

25. На 25 юни 2013 г. г-н Schrems подава жалба до Комисаря, като по същество твърди, че в правната уредба и практиката на САЩ липсва ефективна защита на съхраняваните на територията на САЩ данни срещу наблюдението, извършвано от държавата. Това било видно от разкритията, които г-н Сноудън започнал да прави през май 2013 г. относно дейността на американските разузнавателни служби и по-специално на National Security Agency (Агенция за национална сигурност, наричана по-нататък „NSA“).

26. От тези разкрития ставало ясно по-специално, че NSA е създала програма, наречена „PRISM“, чрез която агенцията получила свободен достъп до информационните масиви, съхранявани на сървъри в САЩ, притежавани или контролирани от редица дружества, опериращи в областта на интернет и технологиите, като например Facebook USA.

27. Комисарят смята, че не е бил длъжен да проведе разследване по жалбата, тъй като е лишена от правно основание. Той приема, че не съществуват доказателства NSA да е получила достъп до данните на г-н Schrems. Освен това според него жалбата трябвало да бъде отхвърлена въз основа на Решение 2000/520, с което Комисията констатира, че в рамките на схемата за сфера на неприкосновеност САЩ гарантират достатъчна степен на защита на прехвърлените лични данни. Всеки въпрос относно достатъчния характер на защитата на тези данни в САЩ трябвало да се разрешава в съответствие с това решение, което не позволявало на Комисаря да разгледа повдигнатия в жалбата проблем.

28. Националното законодателство, въз основа на което Комисаря отхвърля жалбата, е следното.

17 — Вж. също приложение IV, Б.

29. Член 10, параграф 1 от Закона за защита на данните от 1988 г. (Data Protection Act 1988), изменен със Закона за защита на данните от 2003 г. (Data Protection (Amendment) Act 2003, наричан по-нататък „Законът за защита на данните“), му предоставя правото да разглежда жалбите и гласи:

„а) Комисарят може да проведе или да възложи провеждането на разследване на това дали разпоредбите на настоящия закон са били нарушени, се нарушават или могат да бъдат нарушени по отношение на определено лице, ако това лице подаде жалба до него във връзка с нарушение на някоя от тези разпоредби или ако Комисарят счете, че подобно нарушение може да е извършено.

б) Когато съответното лице подаде жалба до Комисаря въз основа на буква а) от настоящия параграф, той:

i) провежда или възлага провеждане на разследване по жалбата, освен ако не приеме, че е несъстоятелна или със злонамерен характер; и

ii) ако в разумен срок не постигне взаимното съгласие на страните за уреждане на спора, който е предмет на жалбата, Комисарят уведомява писмено жалбоподателя за решението си по нея, като отбелязва, че ако решението е неблагоприятно за жалбоподателя, той може да го обжалва по съдебен ред по силата на член 26 от настоящия закон в срок от 21 дни, считано от момента на получаване на уведомлението“.

30. В настоящия случай Комисарят приема, че жалбата на г-н Schrems е „несъстоятелна или със злонамерен характер“ в смисъл, че е обречена на неуспех, тъй като е лишена от правно основание. Ето защо той отказва да проведе разследване по нея.

31. В член 11 от Закона за защита на данните се регламентира прехвърлянето на лични данни извън територията на страната. В член 11, параграф 2, буква а) от него се предвижда:

„Когато в рамките на уредено в настоящия закон производство възникне въпрос:

i) с цел да се определи дали достатъчната степен на защита, посочена в член 1 от настоящия член, е гарантирана от страна или територия извън Европейското икономическо пространство [(ЕИП)], към която ще бъдат прехвърлени лични данни; и

ii) е направена констатация от Съюза относно въпросния вид прехвърляне,

въпросът се решава в съответствие с тази констатация“.

32. В член 11, параграф 2, буква б) от Закона за защита на данните се дава следното определение на понятието за констатация на Съюза:

„В буква а) от настоящия параграф „констатация на Съюза“ означава констатация, направена от [Комисията] по смисъла на член 25, параграфи 4 или 6 от Директива [95/46] в рамките на предвидената в член 31, параграф 2 от [нея] процедура, за да се определи дали достатъчната степен на защита, посочена в параграф 1 от настоящия член, е гарантирана от страна или територия извън [ЕИП]“.

33. Комисарят отбелязва, че Решение 2000/520 е „констатация на Съюза“ по смисъла на член 11, параграф 2, буква а) от Закона за защита на данните, така че по силата на този закон всеки въпрос относно достатъчния характер на защитата на данните в третата страна, в която те са прехвърлени, трябва да се решава в съответствие с тази констатация. Тъй като става въпрос за същността на подадената от г-н Schrems жалба, а именно че личните данни се прехвърлят към трета страна, която на практика не гарантира достатъчна степен на защита, Комисарят приема, че естеството и самото наличие на Решение 2000/520 не му позволяват да разгледа този въпрос.

34. Г-н Schrems подава жалба до High Court [Върховен съд] срещу решението на Комисаря да отхвърли жалбата му. След като разглежда представените по главното производство доказателства, тази юрисдикция установява, че електронното наблюдение и прихващането на лични данни обслужва необходими и наложителни цели в обществен интерес, а именно опазването на националната сигурност и предотвратяването на тежки престъпления. В това отношение High Court посочва, че наблюдението и прихващането на личните данни, прехвърляни от Съюза към САЩ, обслужва законосъобразни цели, свързани с борбата с тероризма.

35. Според същата юрисдикция направените от г-н Сноудън разкрития обаче доказват значителна степен на прекомерност в действията на NSA и други подобни органи. Макар съдът, разглеждащ исканията за наблюдение на чуждите разузнавателни служби (Foreign Intelligence Surveillance Court, наричан по-нататък „FISC“), който действа в рамките на Закона от 1978 г. за наблюдение на чуждите разузнавателни служби (Foreign Intelligence Surveillance Act of 1978)[18], да упражнявал надзор, производството пред него било поверително и нямало състезателен характер. В допълнение, освен че решенията относно достъпа до лични данни се вземали въз основата на американското право, гражданите на Съюза нямали ефективно право на изслушване по въпроса за наблюдението и прихващането на техните данни.

36. От обширните писмени доказателства, съдържащи се в приложените по главното производство клетвени декларации, ясно следвало, че точността на значителна част от разкритията на г-н Сноудън е безспорна. При това положение High Court приема, че след прехвърлянето на личните данни към САЩ, NSA и други американски агенции за сигурност, като например Федералното бюро за разследвания (Federal Bureau of Investigation, FBI), могат да имат достъп до такива данни в рамките на масово и несистематизирано наблюдение и прихващане.

37. High Court посочва, че в ирландското право значението на конституционните права на личен живот и неприкосновеност на жилището изисква всяка намеса, засягаща тези права, да се осъществява в съответствие със закона и да бъде пропорционална. Масовият и несистематизиран достъп до лични данни изобщо не отговарял на изискването за пропорционалност и следователно трябвало да се счита за противоречащ на ирландската конституция[19].

38. High Court отбелязва, че за да може прихващането на електронни съобщения да се счита за конституционносъбразно, трябва да се докаже, че прихващането на конкретни съобщения и наблюдението на определени лица или групи е било обективно обосновано в интерес на национална сигурност или справянето с престъпността, както и че са налице подходящи и проверими гаранции.

18 — Вж. раздел 702 от този закон, изменен със Закона от 2008 г. (Foreign Intelligence Surveillance Act of 2008). Именно въз основа на този раздел NSA притежава база данни, известна под наименованието „PRISM“ (вж. Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection от 27 ноември 2013 г.).

19 — High Court се позовава по-специално на зачитането на човешкото достойнство и свободата на индивида (преамбюл), личната независимост (член 40, параграф 3, точки 1 и 2), неприкосновеността на жилището (член 40, параграф 5) и закрилата на семейния живот (член 41).

39. Ето защо High Court посочва, че ако настоящото дело трябва да се разглежда единствено въз основа на ирландското право, би възникнал един важен въпрос, а именно дали САЩ „гарантират достатъчна степен на защита на личния живот и на основните права и свободи“ по смисъла на член 11, параграф 1 от Закона за защита на данните. От това следвало, че въз основа на ирландското право и по-специално предвид изискванията на конституцията Комисарят не можел да отхвърли жалбата на г-н Schrems, а трябвало да разгледа този въпрос.

40. Същевременно High Court установява, че разглежданото от него дело засяга прилагането на правото на Съюза по смисъла на член 51, параграф 1 от Хартата, така че законосъобразността на решението на Комисаря трябвало да се прецени с оглед на правото на Съюза.

41. High Court излага проблема, пред който Комисарят се оказва изправен, по следния начин. По силата на член 11, параграф 2, буква а) от Закона за защита на данните Комисарят трябва да се произнесе относно достатъчния характер на защитата в третата страна „в съответствие“ с констатацията на Съюза, направена от Комисията по реда на член 25, параграф 6 от Директива 95/46. Следователно Комисарят не можел да не се съобрази с тази констатация. Тъй като в своето Решение 2000/520 Комисията констатира, че САЩ гарантират достатъчна степен на защита при обработването на данни от дружества, придържащи се към принципите за сфера на неприкосновеност, то жалба, в която се твърди, че защитата е недостатъчна, непременно трябвало да се отхвърли от Комисаря.

42. Като констатира, че по този начин Комисарят стриктно се придържа към буквата на Директива 95/46 и Решение 2000/520, High Court същевременно посочва, че г-н Schrems всъщност възразява срещу условията на самата схема за сфера на неприкосновеност, а не срещу начина, по който Комисарят го е приложил на практика, като подчертава, че той не оспорва пряко валидността на Директива 95/46, нито тази на Решение 2000/520.

43. Според High Court основният въпрос е дали предвид правото на Съюза и с оглед по-специално на последващото влизане в сила на членове 7 и 8 от Хартата Комисарят е абсолютно обвързан от посочената в Решение 2000/520 констатация на Комисията, що се отнася до адекватния характер на правото и практиката в областта на защитата на личните данни в САЩ.

44. Освен това High Court уточнява, че жалбата, с която е сезиран, не съдържа каквото и да било твърдение за нарушение по отношение на действията на самите Facebook Ireland и Facebook USA. Според тази юрисдикция член 3, параграф 1, буква б) от Решение 2000/520, който позволява на компетентните национални органи да разпоредят на предприятие да спре потока от данни към трета страна, обаче се прилага само в хипотези, при които жалбата е насочена против поведението на съответното предприятие, а в разглежданията случай това не е така.

45. Съответно High Court подчертава, че на практика се оспорва не поведението на самото дружество Facebook USA, а по-скоро обстоятелството, че Комисията е решила, че правото и практиката в областта на защитата на данни в САЩ гарантират достатъчна защита, докато от разкритията на г-н Сноудън става ясно, че американските власти могат да имат масов и несистематизиран достъп до личните данни на населението, живеещо на територията на Съюза[20].

20 — В това отношение High Court посочва, че главното основание, изтъкнато пред него от г-н Schrems, е изведено от твърдението, че предвид скорошните разкрития на г-н Сноудън и извършеното широкомащабно предоставяне на лични данни на разположение на разузнавателните служби на САЩ, Комисарят няма основание да приеме, че в тази трета страна съществува достатъчна степен на защита на тези данни.

46. По този въпрос High Court смята, че е трудно да се разбере как Решение 2000/520 на практика може да отговори на изискванията на членове 7 и 8 от Хартата, a fortiori, ако се вземат предвид формулираните от Съда принципи в решение Digital Rights Ireland и др[21]. По-специално, гаранцията, предвидена в член 7 от Хартата и свързана с общите за традициите на държавите членки основни ценности, щяла да бъде изложена на риск, ако на публичните власти бъде позволено да разполагат с произволен и всеобхватен достъп до електронните съобщения, без да трябва да излагат обективни основания, произтичащи от съображения, свързани с националната сигурност или с предотвратяването на престъпността във връзка конкретно със съответни лица, и без никакви подходящи и проверими гаранции. Тъй като жалбата на г-н Schrems водела към извода, че Решение 2000/520 in abstracto може да се окаже несъвместимо с членове 7 и 8 от Хартата, Съдът можел да приеме, че е възможно Директива 95/46, и по-специално член 25, параграф 6 от нея, както и Решение 2000/520 да се тълкуват в смисъл, че позволяват на националните органи да водят собствени разследвания, за да установят дали прехвърлянето на лични данни към трета страна и съхраняването им там отговаря на изискванията, произтичащи от членове 7 и 8 от Хартата.

47. При това положение High Court решава да спре производството и да постави на Съда следните преюдициални въпроси:

„Когато Комисарят разглежда жалба относно прехвърлянето на лични данни към трета страна (в случая Съединените щати), за законодателството и практиката на която се твърди, че не предоставят адекватна защита на съответното физическо лице, абсолютно обвързан ли е Комисарят от констатацията на Съюза в противоположен смисъл, съдържаща се в Решение 2000/520, като се имат предвид членове 7, 8 и 47 от Хартата и независимо от разпоредбите на член 25, параграф 6 от Директива 95/46?

В противен случай Комисарят може и/или трябва ли да проведе самостоятелно разследване по въпроса с оглед на фактическите промени, настъпили след първоначалното публикуване на Решение 2000/520 на Комисията?“.

II – **Моят анализ**

48. С двата отправени от High Court въпроса Съдът е приканен да уточни какви са правомощията, с които разполагат националните надзорни органи, когато са сезирани с жалба относно прехвърляне на лични данни към установено в трета страна предприятие и когато в подкрепа на жалбата се твърди, че тази трета страна не гарантира достатъчна степен на защита на прехвърлените данни, при положение че въз основа на член 25, параграф 6 от Директива 95/46 Комисията е приела решение, с което признава, че тази трета страна гарантира достатъчна степен на защита.

49. Ще отбележа, че подадената от г-н Schrems до Комисаря жалба има две страни. Целта ѝ е да се противопостави на прехвърлянето на лични данни от Facebook Ireland към Facebook USA. Г-н Schrems иска това прехвърляне да се прекрати, тъй като според него САЩ не гарантират достатъчна степен на защита на прехвърляните лични данни в рамките на схемата за сфера на неприкосновеност. Той по-точно упреква въпросната трета страна, че е създала програмата PRISM, която осигурява на NSA свободен достъп до информационните масиви, съхранявани на разположени в САЩ сървъри. Следователно жалбата засяга конкретно прехвърлянето на лични данни от Facebook Ireland към Facebook USA, като същевременно в по-общ план се оспорва гарантираната степен на защита на такива данни в рамките на схемата за сфера на неприкосновеност.

21 — C-293/12 и C-594/12, EU:C:2014:238, т. 65—69.

50. Комисарят смята, че самото наличие на решение на Комисията, с което се признава, че в рамките на схемата за сфера на неприкосновеност САЩ гарантират достатъчна степен на защита, не му позволява да проведе разследване по жалбата.

51. Следователно двата въпроса — с които по същество се цели да се установи дали член 28 от Директива 95/46, разглеждан във връзка с членове 7 и 8 от Хартата, трябва да се тълкува в смисъл, че наличието на решение, прието от Комисията въз основа на член 25, параграф 6 от тази директива, е пречка национален надзорен орган да проведе разследване по жалба, в която се твърди, че трета страна не гарантира достатъчна степен на защита на прехвърляните лични данни, и при необходимост да спре прехвърлянето на тези данни — трябва да се разгледат заедно.

52. В член 7 от Хартата се гарантира правото на зачитане на личния живот, докато в член 8 от нея изрично се прогласява правото на защита на личните данни. В параграфи 2 и 3 от последния член се уточнява, че тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание; че всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им, и че спазването на тези правила подлежи на контрол от независим орган.

А – *По правомощията на националните надзорни органи при наличие на решение на Комисията относно достатъчния характер на защитата*

53. Както посочва г-н Schrems в становището си, за целите на разглежданата в главното производство жалба основният въпрос засяга прехвърлянето на лични данни от Facebook Ireland на Facebook USA предвид повсеместния достъп на NSA и други американски агенции за сигурност до съхраняваните във Facebook USA данни в съответствие с правомощията, които се им предоставени по силата на американското законодателство.

54. В случай че националният надзорен орган е сезиран с жалба, с която се цели да се оспори констатацията, че дадена трета страна гарантира достатъчна степен на защита на прехвърляните данни, според г-н Schrems, ако този орган разполага с доказателства за основателността на съдържащите се в тази жалба твърдения, той има правомощия да разпореди спиране на прехвърлянето на данни, извършвано от посоченото в жалбата предприятие.

55. Предвид задълженията на Комисаря да защитава основните права на г-н Schrems, последният твърди, че Комисарят е длъжен не само да разследва, но — ако жалбата бъде уважена — и да използва правомощията си, за да спре потока от данни между Facebook Ireland и Facebook USA.

56. Комисарят обаче отхвърля жалбата въз основа на разпоредбите от Закона за защита на данните, където са изброени правомощията му. В основата на този извод стои становището на Комисаря, че е обвързан от Решение 2000/520.

57. Оттук следва, че основният проблем в настоящото дело е дали преценката на Комисията относно достатъчния характер на степента на защита, съдържаща се в Решение 2000/520, обвързва по абсолютен начин националния орган за защита на данните и не му позволява да проведе разследване по твърденията, с които се цели да се оспори тази констатация. Следователно преюдициалните въпроси засягат обхвата на правомощията за провеждане на разследване на националните органи за защита на данните при наличие на решение на Комисията относно достатъчния характер на защитата.

58. Според Комисията е важно да се има предвид взаимовръзката между нейните правомощия и тези на националните органи за защита на данни. Компетентността на последните се съсредоточавала основно върху приложението на законодателството в тази област в индивидуални случаи, докато общото преразглеждане на приложението на Решение 2000/520, включително всички решения, съдържащи спиране на изпълнението или отмяната му, било от компетентността на Комисията.

59. Комисията изтъква, че г-н Schrems не е посочил конкретни доводи, позволяващи да се приеме, че е изложен на непосредствена опасност от сериозно увреждане поради прехвърлянето на данни между Facebook Ireland и Facebook USA. От друга страна обаче, заради абстрактното си и общо естество, изразените от г-н Schrems опасения относно програмите за наблюдение, въведени от американските агенции за сигурност, били идентични с тези, накарали Комисията да започне преразглеждането на Решение 2000/520.

60. Според Комисията, ако националните надзорни органи предприемат действия въз основа на жалби, в които се посочват единствено структурни и абстрактни опасения, те щели да навлязат в обхвата на правомощията ѝ да предоговори условията на това решение със САЩ или, при необходимост, да спре изпълнението му.

61. Не споделям мнението на Комисията. Според мен наличието на решение, прието от Комисията въз основа на член 25, параграф 6 от Директива 95/46, не може нито да отнеме, нито дори да намали правомощията, с които разполагат националните надзорни органи по силата на член 28 от тази директива. Противно на твърдението на Комисията, ако националните надзорни органи са сезирани в рамките на индивидуални жалби, това според мен не им пречи, по силата на правомощията им за разследване и независимостта им, да формулират собствено становище относно осигуряваната от трета страна обща степен на защита и да определят последиците от това, когато се произнасят по конкретни случаи.

62. От постоянната практика на Съда следва, че при тълкуването на разпоредбите на правото на Съюза трябва да се взема предвид не само тяхното съдържание, но и техният контекст и целите на правната уредба, от която те са част [22].

63. От съображение 62 от Директива 95/46 е видно, че „създаването в държавите членки на надзорни органи, които изпълняват функциите при пълна независимост, е съществен елемент от защитата на лицата по отношение на обработването на личните им данни“.

64. Съгласно член 28, параграф 1, първа алинея от тази директива „[в]сяка държава членка предвижда, че на нейната територия един или повече държавни органи отговарят за контрола на прилагането на разпоредбите, приети от държавите членки, съгласно настоящата директива“. Член 28, параграф 1, втора алинея от посочената директива гласи, че „[т]ези органи се ползват с пълна независимост при упражняване на функциите, които са им възложени“.

65. В член 28, параграф 3 от Директива 95/46 се изброяват правомощията, с които разполага всеки надзорен орган, а именно правомощия по разследване, ефективни правомощия за намеса, които позволяват по-специално временна или окончателна забрана на обработване на данни, както и правомощие да води съдебни дела, когато са нарушени националните разпоредби, приети в приложение на тази директива, или правомощие да свежда тези нарушения до знанието на съдебните власти.

22 — Вж. по-специално решение Koushkaki (C-84/12, EU:C:2013:862, т. 34 и цитираната съдебна практика).

66. Освен това, съгласно член 28, параграф 4, първа алинея от Директива 95/46 „[в]секи надзорен орган разглежда искове, подадени от което и да е лице […], отнасящи се до защита на неговите права и свободи при обработването на лични данни“. В член 28, параграф 4, втора алинея се уточнява, че „[в]секи надзорен орган, в частност, разглежда искове за проверка на законосъобразността на обработването на данни, подадени от което и да е лице, когато се прилагат националните разпоредби, приети съгласно член 13 [от посочената] директива“. Ще уточня, че последната разпоредба позволява на държавите членки да приемат законодателни мерки за ограничаване на обхвата на определени права и задължения, предвидени в Директива 95/46, ако подобно ограничаване представлява необходима мярка за гарантиране по-специално на националната сигурност, отбраната, обществената сигурност и предотвратяването, разследването, разкриването и преследването на углавни престъпления.

67. Както Съдът вече е посочвал, изискването независим орган да контролира спазването на правилата на правото на Съюза относно защитата на физическите лица при обработването на лични данни, произтича и от първичното право на Съюза, и по-точно от член 8, параграф 3 от Хартата и член 16, параграф 2 ДФЕС[23]. Съдът също така припомня, че „[в] този смисъл учредяването на независими надзорни органи в държавите членки е съществен елемент от осигуряването на защита на лицата при обработването на лични данни“[24].

68. Съдът посочва също, че „член 28, параграф 1, втора алинея от Директива 95/46 трябва да се тълкува в смисъл, че надзорните органи, компетентни да наблюдават обработването на лични данни, трябва да се ползват с независимост, която да им дава възможност да изпълняват функциите си без външно влияние. Тази независимост изключва по-специално всяко предписание и всяко друго външно влияние под каквато и да е форма, независимо дали последното е пряко или косвено, които биха могли да насочат решенията им и по този начин биха могли да застрашат изпълнението на задачата на посочените органи, състояща се в постигането на справедлив баланс между защитата на правото на личен живот и свободното движение на личните данни“[25].

69. Съдът също така уточнява, че „[г]аранцията за независимост на националните надзорни органи цели да осигури ефективността и надеждността на надзора за спазване на разпоредбите в областта на защитата на физическите лица при обработване на лични данни“[26]. Тази гаранция за независимост е установена „с цел да засили защитата на засегнатите от [решенията на тези национални надзорни органи] лица и организации“[27].

70. Както по-специално следва от съображение 10 и от член 1 от Директива 95/46, целта ѝ е „да гарантира висока степен на защита в [Съюза] на основните права и свободи при обработването на лични данни“[28]. Според Съда „[с]ледователно предвидените в член 28 от Директива 95/46 надзорни органи са пазители на споменатите основни права и свободи“[29].

71. Предвид важността на функцията, която изпълняват националните надзорни органи в областта на защитата на физическите лица при обработването на личните данни, правомощията им за намеса трябва да останат непокътнати дори ако Комисията е приела решение въз основа на член 25, параграф 6 от Директива 95/46.

23 — Вж. решения Комисия/Австрия (C-614/10, EU:C:2012:631, т. 36) и Комисия/Унгария (C-288/12, EU:C:2014:237, т. 47).

24 — Вж. по-специално решения Комисия/Унгария (C-288/12, EU:C:2014:237, т. 48 и цитираната съдебна практика). В този смисъл вж. също Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238, т. 68 и цитираната съдебна практика).

25 — Вж. по-специално решение Комисия/Унгария (C-288/12, EU:C:2014:237, т. 51 и цитираната съдебна практика).

26 — Решение Комисия/Германия (C-518/07, EU:C:2010:125, т. 25).

27 — Пак там.

28 — Пак там (т. 22 и цитираната съдебна практика).

29 — Пак там (т. 23). Вж. също в този смисъл решения Комисия/Австрия (C-614/10, EU:C:2012:631, т. 52) и Комисия/Унгария (C-288/12, EU:C:2014:237, т. 53).

72. В това отношение ще отбележа, че отникъде не следва, че схемите за прехвърляне на лични данни към трети страни са изключени от материалното приложно поле на член 8, параграф 3 от Хартата, в който на най-високо равнище в йерархията на нормите в правото на Съюза е утвърдено значението на контрола, упражняван от независим орган, що се отнася до спазването на правилата относно защитата на личните данни.

73. Ако националните надзорни органи бяха абсолютно обвързани от приетите от Комисията решения, това неизбежно би ограничило тяхната пълна независимост. В съответствие с ролята им на пазители на основните права националните надзорни органи трябва да могат да провеждат разследвания напълно независимо по подадените до тях жалби във висшия интерес на защитата на физическите лица при обработването на личните данни.

74. Освен това, както белгийското правителство и Европейският парламент правилно отбелязват в съдебното заседание, не съществува никаква йерархична обвързаност между глава IV от Директива 95/46 относно прехвърлянето на лични данни към трети страни и глава VI от нея, посветена по-специално на ролята на националните надзорни органи. Нищо в глава VI не подсказва, че разпоредбите относно националните надзорни органи са подчинени по някакъв начин на отделните разпоредби относно прехвърлянето на данни, съдържащи се в глава IV от Директива 95/46.

75. Напротив, от член 25, параграф 1 от Директивата, който е включен в глава IV от нея, изрично следва, че разрешаването на прехвърлянето на лични данни към трета страна, гарантираща достатъчна степен на защита, може да се извършва само без да се засяга спазването на националните разпоредби, приети в съответствие с другите разпоредби от посочената директива.

76. В това отношение ще припомня, че по силата на тази разпоредба държавите членки трябва да предвидят в националното си законодателство, че прехвърлянето на лични данни, които са подложени на обработка или са предназначени за обработка след прехвърлянето им към трета страна, може да се извършва само ако без да се засяга спазването на националните разпоредби, приети в съответствие с другите разпоредби на Директива 95/46, въпросната трета страна гарантира достатъчна степен на защита.

77. В съответствие с член 28, параграф 1 от тази директива националните надзорни органи отговарят за контрола по прилагането на територията на всяка държава членка на разпоредбите, приети от държавите членки съгласно Директивата.

78. Тясната връзка между тези две разпоредби позволява да се приеме, че посоченото в член 25, параграф 1 от Директива 95/46 правило, според което прехвърлянето на лични данни може да се извършва само ако третата страна получател гарантира достатъчна степен на защита, е част от правилата, за чийто контрол по прилагане отговарят националните надзорни органи.

79. Правомощията на националните надзорни органи за провеждане на напълно независимо разследване по жалбите, с които са сезирани по силата на член 28 от Директива 95/46, следва да се тълкуват разширително в съответствие с член 8, параграф 3 от Хартата. Следователно тези правомощия не могат да се ограничават от предоставените на Комисията от законодателя на Съюза правомощия по силата на член 25, параграф 6 от посочената директива, за да се констатира, че предложената от трета страна степен на защита е достатъчна.

80. Предвид съществената им роля в областта на защитата на личните данни националните надзорни органи трябва да могат да провеждат разследване, когато са сезирани с жалба, съдържаща доказателства, с които може да се оспори гарантираната от трета страна степен на защита, включително когато Комисията е констатирала в решение, прието въз основа на член 25, параграф 6 от Директива 95/46, че съответната трета страна гарантира достатъчна степен на защита.

81. Ако след проведеното от национален надзорен орган разследване той счете, че спорното прехвърляне на данни накърнява защитата, с която гражданите на Съюза трябва да се ползват при обработването на техните данни, този орган разполага с правомощието да спре прехвърлянето на въпросните данни независимо от извършената в решението на Комисията обща оценка.

82. Всъщност от член 25, параграф 2 от Директива 95/46 безспорно е видно, че достатъчният характер на предоставяната от трета страна степен на защита се преценява въз основа на съвкупност от фактически и правни обстоятелства. Ако едно от тези обстоятелства се промени, така че да постави под въпрос достатъчния характер на степента на защитата, предоставена от трета страна, сезираният с жалба национален надзорен орган трябва да може да определи последиците по отношение на оспореното прехвърляне на данни.

83. Действително, както посочва Ирландия, Комисарят, както и другите държавни органи, е обвързан от Решение 2000/520. Всъщност от член 288, четвърта алинея ДФЕС следва, че прието от институция на Съюза решение е задължително в своята цялост. Следователно Решение 2000/520 е задължително за държавите членки, които са негови адресати.

84. В това отношение ще отбележа, че член 5 от самото Решение 2000/520 гласи, че „[д]ържавите членки вземат всички необходими мерки, за да се съобразят с [това] решение, най-късно деветдесет дни след датата на нотификацията му до държавите членки“. Освен това член 6 от него потвърждава, че „[негови адресати] са държавите членки“.

85. Смятам обаче, че предвид горепосочените разпоредби от Директива 95/46 и Хартата задължителното действие на Решение 2000/520 не може да изключи възможността за провеждането на каквото и да е разследване от страна на Комисаря по жалби, в които се твърди, че прехвърлянето на лични данни към САЩ в рамките на това решение не е придружено с необходимите гаранции за защита, изисквани от правото на Съюза. С други думи, подобно обвързващо действие не може да доведе до цялостно отхвърляне на всички жалби от този вид, тоест незабавно и без проверка на тяхната основателност.

86. Освен това ще добавя, че от структурата на член 25 от Директива 95/46 е видно, че констатацията относно това дали дадена трета страна гарантира достатъчна степен на защита, може да се извърши или от държавите членки, или от Комисията. Следователно става въпрос за споделена компетентност.

87. От член 25, параграф 6 от тази директива следва, че щом Комисията констатира, че дадена трета страна гарантира достатъчна степен на защита по смисъла на член 25, параграф 2 от Директивата, държавите членки трябва да вземат необходимите мерки, за да се съобразят с решението на Комисията.

88. Тъй като подобно решение води до разрешаване на прехвърлянето на лични данни към трета страна, чиято степен на защита се счита за достатъчна от Комисията, то по принцип държавите членки трябва да разрешат прехвърлянето на данни да бъде извършвано от установените на тяхна територия предприятия.

89. Член 25 от Директива 95/46 обаче не предоставя изключителни права на Комисията по отношение на констатацията за достатъчната или недостатъчната степен на защита на прехвърляните лични данни. Структурата на този член свидетелства за това, че държавите членки също играят роля в тази област. Действително решенията на Комисията изпълняват важна роля за уеднаквяването на условията за прехвърляне на данни, които са в сила в държавите членки. Това уеднаквяване обаче може да продължи само докато съответната констатация не бъде оспорена.

90. Според мен доводът за необходимостта от уеднаквяване на условията за прехвърляне на лични данни към трета страна е ограничен в положение като разглежданото в главното производство, в което Комисията не само е уведомена, че констатацията ѝ е подложена на критики, а и самата тя формулира подобни критики и води преговори за поправяне на положението.

91. Преценката за наличието или липсата на предоставена от трета страна достатъчна степен на защита също може да доведе до сътрудничество между държавите членки и Комисията. Член 25, параграф 3 от Директива 95/46 предвижда в това отношение, че „[д]ържавите членки и Комисията се информират взаимно за случаите, в които считат, че трета страна не гарантира достатъчна степен на защита по смисъла на параграф 2“. Както отбелязва Парламентът, това ясно показва, че държавите членки и Комисията имат равностойна роля за разкриване на случаите, в които трета страна не гарантира достатъчна степен на защита.

92. С решението относно достатъчния характер на защитата се цели да се разреши прехвърлянето на лични данни към съответната трета страна. Това не означава, че надзорните органи не могат повече да бъдат сезирани от гражданите на Съюза с искане за защита на личните им данни. В това отношение ще отбележа, че в член 28, параграф 4, първа алинея от Директива 95/46, съгласно който „[в]секи надзорен орган разглежда искове, подадени от което и да е лице, […] отнасящи се до защита на неговите права и свободи при обработването на лични данни“, не се предвижда изключение от този принцип при наличие на решение, прието от Комисията въз основа на член 25, параграф 6 от посочената директива.

93. Така, макар прието от Комисията решение по силата на предоставените ѝ от последната разпоредба изпълнителни правомощия да води до разрешаване на прехвърлянето на лични данни към трета страна, подобно решение не може да доведе до отнемане на правомощията на държавите членки, и по-специално на националните им надзорни органи, или дори само до ограничаването им, щом са изправени пред твърдения за нарушаване на основни права.

94. Съответният национален надзорен орган трябва да бъде в състояние да упражнява предвидените в член 28, параграф 3 от Директива 95/46 правомощия, сред които правомощието за временно или окончателно забраняване на обработването на лични данни. Макар при изброяването на предвидените в тази разпоредба правомощия да не се предвиждат изрично такива относно прехвърляне на данни от една страна членка към трета страна, според мен подобно прехвърляне трябва да се счита за обработване на данни[30]. Както е видно от формулировката на посочената разпоредба, изброяването освен това не е изчерпателно. При всички случаи, предвид съществената роля на националните надзорни органи в системата, въведена с Директива 95/46, те трябва да разполагат с правомощие да прекратяват прехвърляне на данни при установяване на случай на доказано накърняване или при опасност от накърняване на основните права.

30 — Вж. заключението на генералния адвокат Léger по дело Парламент/Съвет и Комисия (C-317/04, EU:C:2005:710, т. 92—95). Вж. също решение Парламент/Съвет и Комисия (C-317/04 и C-318/04, EU:C:2006:346, т. 56).

95. Ще добавя, че лишаването на националния надзорен орган от правомощията му по разследване при обстоятелства като разглежданите по настоящото дело би противоречало не само на принципа за независимост, а и на целта на Директива 95/46, установена в член 1, параграф 1 от нея.

96. Както Съдът вече е приемал, „[о]т съображения 3, 8 и 10 от Директива 95/46 следва, че целта на законодателя на Съюза е била да улесни свободното движение на личните данни чрез сближаване на законодателствата на държавите членки, като същевременно защити основните права на лицата, и по-специално правото на защита на личния живот, и гарантира висока степен на защита в рамките на Съюза. Така член 1 от същата директива предвижда, че държавите членки са длъжни да осигурят защитата на основните права и свободи на физическите лица, и в частност на правото им на личен живот, при обработването на лични данни“ [31].

97. Следователно разпоредбите на Директива 95/46 трябва да бъдат тълкувани в съответствие с нейната цел за гарантиране на висока степен на защита на основните права и свободи на физическите лица, по-специално на личния им живот, при обработването на лични данни в рамките на Съюза.

98. От значението на тези цел и ролята, която държавите членки трябва да играят за постигането ѝ, следва, че когато особени обстоятелства будят сериозни съмнения относно спазването на гарантираните от Хартата основни права при прехвърлянето на лични данни към трета страна, държавите членки и съответно техните национални надзорни органи не могат да бъдат обвързани изцяло от решение на Комисията относно достатъчния характер на защитата.

99. Съдът вече е постановявал, че „разпоредбите на Директива 95/46, доколкото уреждат обработката на личните данни, които могат да засегнат основните свободи, и по-специално правото на личен живот, по необходимост трябва да се тълкуват с оглед на основните права, които съгласно постоянната съдебна практика са неразделна част от общите принципи на правото, съблюдаването на които Съдът осигурява и които понастоящем са закрепени в Хартата“ [32].

100. Освен това ще отбележа съдебната практика, съгласно която „държавите членки са длъжни не само да тълкуват националното си право по начин, който да съответства на правото на Съюза, но и да не допускат да се основават на тълкуване на текст от вторичното право, което би влязло в конфликт с основните права, защитавани от правния ред на Съюза, или с останалите общи принципи на правото на Съюза“ [33].

101. В решението си N. S. и др.[34] Съдът постановява, че „прилагането на Регламент [(ЕО)] № 343/2003[35] въз основа на необорима презумпция, че основните права на търсещия убежище ще бъдат спазени в държавата членка, която по принцип е компетентна да разгледа молбата му, е несъвместимо със задължението на държавите членки да тълкуват и прилагат Регламент № 343/2003 в съответствие с основните права“ [36].

31 — Вж. по-специално решение IPI (C-473/12, EU:C:2013:715, т. 28 и цитираната съдебна практика).

32 — Вж. по-специално решение Google Spain и Google (C-131/12, EU:C:2014:317, т. 68 и цитираната съдебна практика).

33 — Вж. по-специално решение N. S. и др. (C-411/10 и C-493/10, EU:C:2011:865, т. 77 и цитираната съдебна практика).

34 — C-411/10 и C-493/10, EU:C:2011:865.

35 — Регламент на Съвета от 18 февруари 2003 година за установяване на критерии и механизми за определяне на държава членка, компетентна за разглеждането на молба за убежище, която е подадена в една от държавите членки от гражданин на трета страна (ОВ L 50, стр. 1; Специално издание на български език, 2007 г., глава 19, том 6, стр. 56).

36 — Точка 99 от това решение.

102. В това отношение, в контекста на статута на държавите членки, представляващи една спрямо друга безопасни страни на произход, що се отнася до всички правни и практически въпроси, свързани с проблемите на правото на убежище, според Съда трябва да се презюмира, че отношението към търсещите убежище лица във всяка държава членка отговаря на изискванията на Хартата, както и на Конвенцията за статута на бежанците, подписана в Женева на 28 юли 1951 г.[37], и на Европейската конвенция за защита на правата на човека и основните свободи, подписана в Рим на 4 ноември 1950 г[38]. Съдът въпреки това постановява, че „не е изключено в определена държава членка на практика да има значителни затруднения за функционирането на тази система и съответно да е налице голям риск при прехвърляне на търсещи убежище лица в тази държава членка отношението към тях да е несъвместимо с основните им права“[39].

103. Ето защо Съдът приема, че „държавите членки, включително националните юрисдикции, са длъжни да не прехвърлят търсещото убежище лице в „компетентната държава членка“ по смисъла на Регламент № 343/2003, когато не може да не им е известно, че системните недостатъци на процедурата за предоставяне на убежище и на условията за приемане на търсещи убежище лица в тази държава членка съставляват сериозни и потвърдени основания да се смята, че [търсещото убежище лице] би бил[о] изложен[о] на реална опасност от нечовешко или унизително отношение по смисъла на член 4 от Хартата“[40].

104. Струва ми се, че приносът на съдебната практика в решение N. S. и др.[41] може да бъде разширен и да обхване положение като разглежданото в главното производство. Така тълкуване на вторичното право на Съюза, почиващо на необорима презумпция, че основните права ще бъдат зачетени — независимо дали от държава членка, Комисията, или от трета страна — трябва да се приеме за несъвместимо със задължението на държавите членки да тълкуват и прилагат вторичното право на Съюза в съответствие с основните права. Следователно член 25, параграф 6 от Директива 95/46 не налага подобна необорима презумпция за спазване на основните права по отношение на преценката на Комисията на достатъчната степен на защита, предоставена от трета страна. Напротив, презумпцията, залегнала в основата на тази разпоредба, а именно че прехвърлянето на данни към трета страна става в съответствие с основните права, трябва да се приеме за оборима[42]. Ето защо тази разпоредба не трябва да се разглежда като застрашаваща гаранциите, съдържащи се по-специално в член 28, параграф 3 от Директива 95/46 и в член 8, параграф 3 от Хартата, целящи защита и зачитане на правото на защита на личните данни.

105. Следователно от посоченото съдебно решение се налага изводът, че при констатирани системни недостатъци в третата страна, към която се прехвърлят лични данни, държавите членки трябва да имат възможност да вземат необходимите мерки за закрилата на основните права, защитени с членове 7 и 8 от Хартата.

106. Както впрочем посочва италианското правителство в становището си, приемането от Комисията на решение относно достатъчния характер на защитата не може да доведе до намаляване на защитата на гражданите на Съюза при обработката на техните данни, когато те са прехвърляни към трета страна, в сравнение със степента на защита, с която тези лица биха се ползвали, ако данните им бяха обработвани в рамките на Съюза. Ето защо националните

37 — Recueil des traités des Nations unies, том 89, стр. 150, № 2545 (1954).

38 — Вж. решение N. S. и др. (C-411/10 и C-493/10, EU:C:2011:865, т. 80).

39 — Пак там (т. 81).

40 — Пак там (т. 94).

41 — C-411/10 и C-493/10, EU:C:2011:865.

42 — Точка 104 от това решение.

надзорни органи трябва да имат възможност да се намесват и да упражняват правомощията си по отношение на прехвърлянето на данни към трети страни, за които има решение относно достатъчния характер на защитата. В противен случай гражданите на Съюза биха били защитени в по-малка степен, отколкото при обработка на данните им в рамките на Съюза.

107. Следователно единствената последица от приемането на решение от Комисията на основание член 25, параграф 6 от Директива 95/46 е вдигането на общата забрана за изнасяне на лични данни към трети страни, гарантиращи степен на защита, сравнима с предоставяната в тази директива. С други думи, не става въпрос за създаване на специален режим на изключение, който да предоставя по-малка степен на защита на гражданите на Съюза в сравнение с предвидения в посочената директива общ режим за обработка на данни, извършвана в рамките на Съюза.

108. Действително в точка 63 от своето решение Lindqvist [43] Съдът посочва, че „[г]лава IV от Директива 95/46, в която е включен член 25, въвежда специален режим“. Според мен обаче това не означава, че подобен режим непременно предоставя по-малка степен на защита. Напротив, за постигане на определената в член 1, параграф 1 от Директива 95/46 цел за защита на данните член 25 от нея налага редица задължения на държавите членки и Комисията [44] и въвежда принципа, че когато трета страна не предоставя достатъчна степен на защита, прехвърлянето на лични данни към тази страна трябва да бъде забранено [45].

109. Що се отнася по-специално до схемата за сфера на неприкосновеност, Комисията предвижда намеса на националните надзорни органи и спиране от тяхна страна на потоците от данни само в рамките, очертани от член 3, параграф 1, буква б) от Решение 2000/520.

110. Според съображение 8 от това решение „[с] цел да се гарантира прозрачността и да се запази възможността на компетентните органи в държавите членки да осигурят защитата на физическите лица по отношение на обработването на личните данни, в настоящото решение трябва да се указва при какви изключителни обстоятелства спирането на някои конкретни потоци с данни може да бъде оправдано, дори ако е било установено достатъчно ниво на защита“.

111. В настоящото дело предмет на обсъждане по-специално е прилагането на член 3, параграф 1, буква б) от посоченото решение. По силата на тази разпоредба решение за спиране на потока от данни може да се вземе от националните надзорни органи в случаите, „когато е много вероятно принципите да са нарушени; когато всичко сочи, че съответната инстанция за прилагане не взима или няма да вземе в необходимите срокове мерките, които се налагат с цел решаване на въпросното дело; когато продължаването на предаване на данни представлява неминуем риск от сериозни вреди за съответните лица; и когато компетентните органи на държавите членки са направили достатъчно последователни усилия, в зависимост от обстоятелствата, за да предупредят организацията и да ѝ дадат възможност да отговори“.

43 — C-101/01, EU:C:2003:596.

44 — Точка 65.

45 — Точка 64.

112. Посочената разпоредба поставя редица условия, които са предмет на различни тълкувания от страните в хода на настоящото производство [46]. Без навлизане в подробности по тълкуванията е видно, че тези условия строго определят рамките на правомощията на националните надзорни органи за спиране на потоците от данни.

113. Така, противно на твърдението на Комисията, член 3, параграф 1, буква б) от Решение 2000/520 трябва да се тълкува в съответствие с целта за защита на личните данни, преследвана от Директива 95/46, както и в светлината на член 8 от Хартата. Задължителното изискване за тълкуване в съответствие с основните права подкрепя разширителното тълкуване на тази разпоредба.

114. От това следва, че предвидените в член 3, параграф 1, буква б) от Решение 2000/520 условия според мен не могат да попречат на национален надзорен орган напълно независимо да упражнява правомощията, възложени му съгласно член 28, параграф 3 от тази Директива 95/46.

115. Както по същество посочват белгийското и австрийското правителство в съдебното заседание, „аварийният изход“, какъвто е член 3, параграф 1, буква б) от Решение 2000/520, е толкова тесен, че е трудно да се използва на практика. Той изисква изпълнението на кумулативни критерии и поставя летвата твърде високо. Така в светлината на член 8, параграф 3 от Хартата е невъзможно свободата на действие на националните надзорни органи относно прерогативите, които произтичат от член 28, параграф 3 от Директива 95/46, да бъде ограничена така, че тези прерогативи да не могат повече да бъдат упражнявани.

116. В това отношение Парламентът правилно отбелязва, че законодателят на Съюза е решил какви правомощия трябва да притежават националните надзорни органи. Изпълнителното правомощие, предоставено на Комисията от законодателя на Съюза в член 25, параграф 6 от Директива 95/46, обаче не засяга правомощията, предоставени от същия законодател на националните надзорни органи в член 28, параграф 3 от Директивата. С други думи, Комисията не е оправомощена да ограничава правомощията на националните надзорни органи.

117. Ето защо, за да се гарантира подходяща степен на защита на основните права на физическите лица при обработката на личните данни, националните надзорни органи трябва да бъдат оправомощени да провеждат разследвания при твърдения за нарушение на тези права. Ако след провеждането на такива разследвания въпросните органи установят, че в третата страна, за която е прието решение относно достатъчния характер на защитата, са налице сериозни признаци за накърняване на правото на гражданите на Съюза на защита на личните им данни, те трябва да могат да спрат прехвърлянето на данни към установения в тази трета страна получател.

118. С други думи, националните надзорни органи трябва да имат възможност да проведат собствено разследване и при необходимост да спират прехвърлянето на данни независимо от ограничителните условия, определени в член 3, параграф 1, буква б) от Решение 2000/520.

46 — Според г-н Schrems първото условие, според което „е много вероятно принципите да са нарушени“, не е изпълнено. На практика не се твърди, че самото Facebook USA, в качеството си на самосертифициран орган, на който са прехвърлени данни, е нарушило принципите за сфера на неприкосновеност поради масовия и несистематизиран достъп до притежаваните от него данни от страна на американските органи. Всъщност принципите за сфера на неприкосновеност са ограничени изрично от американското право, което приложение I, четвърта алинея към Решение 2000/520 определя чрез препратка към законите, правителственото регулиране и съдебната практика.

119. Освен това съгласно предвидените в член 28, параграф 3 от Директива 95/46 правомощия да водят съдебни дела, когато са нарушени националните разпоредби, приети в съответствие с тази директива, или да свеждат тези нарушения до знанието на съдебните власти, националните надзорни органи трябва да имат възможността — когато са запознати с факти, от които е видно, че трета страна не гарантира достатъчна степен на защита — да сезират национален съд, който от своя страна при необходимост може да отправи преюдициално запитване пред Съда, с цел да се прецени валидността на решение на Комисията относно достатъчния характер на защитата.

120. От всички изложени съображения следва, че член 28 от Директива 95/46, разглеждан във връзка с членове 7 и 8 от Хартата, трябва да се тълкува в смисъл, че наличието на решение, прието от Комисията въз основа на член 25, параграф 6 от тази директива, не е пречка национален надзорен орган да проведе разследване по жалба, в която се твърди, че трета страна не гарантира достатъчна степен на защита на прехвърляните лични данни, и при необходимост да спре прехвърлянето на тези данни.

121. Макар в акта за преюдициално запитване High Court да подчертава, че в главното производство г-н Schrems формално не оспорва нито валидността на Директива 95/46, нито тази на Решение 2000/520, от този акт е видно, че с основната си критика г-н Schrems цели да оспори констатацията, според която в рамките на схемата за сфера на неприкосновеност САЩ гарантират достатъчна степен на защита на прехвърлените лични данни.

122. От становището на Комисаря е видно също така, че с жалбата си г-н Schrems цели пряко да оспори Решение 2000/520. С подаването на тази жалба той е искал да оспори условията и функционирането на самата схема за сфера на неприкосновеност, тъй като масовото наблюдение на прехвърляните към САЩ лични данни разкривало липсата на истинска защита на тези данни в действащото право и практики в посочената трета страна.

123. Освен това самата запитваща юрисдикция отбелязва, че гаранцията, предоставена от член 7 от Хартата и свързана с общите за конституционните традиции на държавите членки основни ценности, щяла да бъде изложена на риск, ако на публичните власти бъде позволено да разполагат с произволен и всеобхватен достъп до електронните съобщения, без да трябва да излагат обективни основания, произтичащи от съображения, свързани с националната сигурност или с предотвратяването на престъпността във връзка конкретно със съответни лица, и без никакви подходящи и проверими гаранции[47]. По този начин запитващата юрисдикция косвено изразява съмнения относно валидността на Решение 2000/520.

124. Следователно преценката на това дали в рамките на схемата за сфера на неприкосновеност САЩ гарантират достатъчна степен на защита на прехвърляните лични данни, неизбежно налага да се разгледа валидността на това решение.

125. В това отношение следва да се посочи, че в рамките на инструмента за сътрудничество между Съда и националните юрисдикции, установен с член 267 ДФЕС, дори ако в рамките на преюдициално производство е сезиран единствено с въпрос относно тълкуването на правото на Съюза, при определени специфични обстоятелства може да се наложи Съдът да разгледа валидността на разпоредби от вторичното право.

47 — Точка 24 от акта за преюдициално запитване.

126. Ето защо Съдът нееднократно служебно е прогласявал невалидността на акт, за който му е било поискано само тълкуване [48]. Съдът постановява също, че „когато става ясно, че същинската цел на поставените от национална юрисдикция въпроси се отнася повече до разглеждането на валидността, отколкото до тълкуването на актове [на Съюза], Съдът трябва незабавно да даде повече яснота на посочената юрисдикция, без да я задължава да се съобразява с напълно дилаторен формализъм, несъвместим с характера на установените с член [267 ДФЕС] механизми“ [49]. Впрочем Съдът вече е приел, че изразените от запитваща юрисдикция съмнения по отношение на съвместимостта на акт на вторичното право с нормите за защитата на основните права трябва да бъдат разбирани като поставяне под въпрос на валидността на този акт с оглед на правото на Съюза [50].

127. Ще припомня също произтичащото от практиката на Съда, а именно че актовете на институциите, органите и организациите на Съюза се ползват от презумпция за валидност, което означава, че произвеждат правно действие, докато не бъдат оттеглени, отменени в производство по жалба за отмяна или обявени за невалидни вследствие на преюдициално запитване или възражение за незаконосъобразност. Единствено Съдът е компетентен да установи невалидността на акт на Съюза и тази компетентност е предоставена, за да се обезпечи правната сигурност, като се осигури еднакво прилагане на правото на Съюза. Ако не е обявено за невалидно и не е изменено или отменено от Комисията, решението продължава да бъде задължително в своята цялост и пряко приложимо във всяка държава членка [51].

128. За да предостави изчерпателен отговор на запитващата юрисдикция и да премахне съмненията, изразени в хода на настоящото производство относно валидността на Решение 2000/520, смятам, че Съдът трябва да прецени валидността на това решение.

129. При това положение е важно също така да се уточни, че разглеждането на въпроса дали Решение 2000/520 е валидно, трябва да се причисли към твърденията за нарушение, предмет на обсъждане в рамките на настоящото производство. Всъщност не всички аспекти относно функционирането на схемата за сфера на неприкосновеност са обсъдени в тези рамки и затова според мен не е възможно тук да се направи изчерпателен анализ на недостатъците на тази схема.

130. За сметка на това въпросът дали всеобхватният и нецеленасочен достъп на американските разузнавателни служби до прехвърляните данни може да засегне законосъобразността на Решение 2000/520, бе предмет на обсъждане пред Съда в рамките на настоящото производство. Следователно валидността на това решение може да се прецени от тази гледна точка.

48 — Вж. по-специално решения Strehl (62/76, EU:C:1977:18, т. 10—17), Roquette Frères (145/79, EU:C:1980:234, т. 6) и Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, т. 32—39).

49 — Решение Schwarze (16/65, EU:C:1965:117, стр. 1094).

50 — Вж. решение Hauer (44/79, EU:C:1979:290, т. 16).

51 — Вж. по-специално решение CIVAD (C-533/10, EU:C:2012:347, т. 39—41 и цитираната съдебна практика).

Б – *Относно валидността на Решение 2000/520*

1. По обстоятелствата, които трябва да се вземат предвид при преценката на валидността на Решение 2000/520

131. Следва да се припомни съдебната практика, съгласно която „в рамките на жалба за отмяна законосъобразността на даден акт трябва да се преценява в зависимост от фактическите и правните обстоятелства, към датата, на която е приет актът, като преценката на Комисията може да бъде отхвърлена само ако е явно неправилна с оглед на данните, с които е разполагала към момента на приемане на въпросния акт“ [52].

132. В своето решение Gaz de France — Berliner Investissement [53] Съдът припомня принципа, че „преценката за валидността на даден акт, която Съдът следва да направи в рамките на преюдициалното запитване, по правило трябва да се основава на положението, което съществува към момента на приемането на акта“ [54]. Съдът изглежда обаче допуска, че „в определени случаи валидността на даден акт може да се прецени в зависимост от нови обстоятелства, настъпили след приемането му“ [55].

133. Така очертаният от Съда подход според мен е особено релевантен в рамките на настоящото дело.

134. Всъщност приеманите от Комисията решения въз основа на член 25, параграф 6 от Директива 95/46 имат особени характеристики. С тях трябва да се прецени дали предоставяната от трета страна степен на защита на личните данни е достатъчна. В случая става въпрос за преценка, която може да се променя в зависимост от фактическия и правния контекст, който преобладава в съответната трета страна.

135. Предвид това, че решението относно достатъчния характер на защитата представлява особен вид решение, на правилото, съгласно което преценката на валидността му може да се извърши само в зависимост от обстоятелствата, които съществуват към момента на неговото приемане, трябва да се придаде нюанс в конкретния случай. Подобно правило иначе би довело до това години след приемането на решение относно достатъчния характер на защитата, в преценката на валидността, която Съдът трябва да извърши, да не може да се вземат предвид настъпилите по-късно събития, макар такова преюдициално запитване за преценка на валидността да не е ограничено във времето и да се отправя именно в резултат на настъпили впоследствие обстоятелства, разкриващи недостатъците на разглеждания акт.

136. В конкретния случай оставянето в сила на Решение 2000/520 в продължение на около петнадесет години свидетелства за имплицитното потвърждаване от страна на Комисията на извършената през 2000 г. от нея оценка. Когато в рамките на преюдициално запитване Съдът трябва да се произнесе по валидността на оценка, която е оставена в сила от Комисията във времето, то не е само е възможно, но и е уместно той да съпостави посочената оценка с новите обстоятелства, настъпили след приемането на решението относно достатъчния характер на защитата.

52 — Вж. по-специално решение BVGD/Комисия (T-104/07 и T-339/08, EU:T:2013:366, т. 291), в което се прави позоваване на решение IECC/Комисия (C-449/98 P, EU:C:2001:275, т. 87).

53 — C-247/08, EU:C:2009:600.

54 — Точка 49 и цитираната съдебна практика.

55 — Точка 50 и цитираната съдебна практика. В този смисъл вж. *Lenaerts*, K., *Maselis*, I., et *Gutman*, K., EU Procedural Law. Oxford University Press, 2014, където се посочва, че „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court“ (точка 10.16, стр. 471).

137. Предвид особеното естество на решението относно достатъчния характер на защитата то трябва редовно да бъде преразглеждано от страна на Комисията. Ако след междувременното настъпване на нови събития Комисията не изменя решението си, това означава, че тя имплицитно, но непременно, потвърждава първоначално извършената преценка. Така тя потвърждава и констатацията си, че съответната трета страна гарантира достатъчна степен на защита на прехвърляните лични данни. Тогава Съдът следва да разгледа дали тази констатация все още е валидна въпреки настъпилите впоследствие обстоятелства.

138. Според мен, за да се гарантира ефективният съдебен контрол на този вид решения, преценката на валидността на това решение трябва да се извърши, като се вземе предвид настоящият правен и фактически контекст.

2. По понятието за достатъчна степен на защита

139. Член 25 от Директива 95/46 изцяло почива на принципа, че прехвърляне на лични данни към трета страна не може да се извършва, освен ако посочената трета страна не гарантира достатъчна степен на защита на такива данни. Следователно целта на този член е да се гарантира непрекъснатостта на предоставената с тази директива защита при прехвърляне на лични данни към трета страна. В това отношение следва да се припомни, че Директивата предоставя висока степен на защита на гражданите на Съюза по отношение на обработката на техните лични данни.

140. Предвид важната роля, която защитата на личните данни играе с оглед на основното право за зачитане на личния живот, подобна висока степен на защита съответно трябва да бъде гарантирана и при прехвърляне на лични данни към трета страна.

141. Ето защо смятам, че въз основа на член 25, параграф 6 от Директива 95/46 Комисията може да установи, че трета страна гарантира достатъчна степен на защита само когато, след извършена цялостна преценка на правото и практиката във въпросната трета страна, тя е в състояние да докаже, че тази трета страна предоставя степен на защита, която по същество е равностойна на предоставяната с Директивата, макар условията на защитата да могат да се различават от обичайно срещаните в рамките на Съюза.

142. Макар английският термин „adequate“ от езикова гледна точка да може да се разбира като обозначаващ едва „задоволителна“ или „достатъчна“ степен на защита и съответно да има различен смислов обхват спрямо френския термин „adéquat“, следва да се отбележи, че единственият критерий, който трябва да ръководи тълкуването на този термин, е целта за постигане на висока степен на защита на основните права, както се изисква от Директива 95/46.

143. Анализът на предоставената от трета страна степен на защита трябва да отчита два основни елемента, а именно съдържанието на приложимите правила и средствата за гарантиране на спазването на тези правила [56].

144. Според мен, за да се постигне степен на защита — равностойна по същество на тази, която действа в рамките на Съюза — схемата за сфера на неприкосновеност, която в голяма степен се основава на самосертифициране и самооценка от страна на доброволно участващите в тази схема предприятия, следва да се допълва от задоволителни гаранции и годен механизъм за контрол. Така прехвърлянето на лични данни към трети страни не следва да се ползва с по-ниска степен на защита спрямо извършваната в рамките на Съюза обработка на данни.

56 — Вж. стр. 5 от работния документ РГ 12 на Комисията, озаглавен „Предаване на лични данни към трети страни: прилагане на членове 25 и 26 от Директивата на ЕС за защита на данните“, приет на 24 юли 1998 г. от работната група за защита на физическите лица по отношение на обработването на личните данни.

145. В това отношение най-напред ще отбележа, че в Съюза преобладава виждането, че наличието на механизъм за външен надзор под формата на независим орган представлява необходим за всяка система елемент за гарантиране на спазването на правилата относно защитата на личните данни.

146. Освен това, за да се гарантира полезното действие на член 25, параграфи 1—3 от Директива 95/46, следва да се вземе предвид обстоятелството, че достатъчният характер на защитата, предоставяна от трета страна, е положение, което може да се промени във времето в зависимост от редица фактори. Следователно държавите членки и Комисията трябва непрекъснато да следят за всяка промяна в обстоятелствата, която може да породи необходимост от преоценка на достатъчния характер на степента на защита, предоставяна от трета страна. Преценката на достатъчния характер на степента на тази защита в никакъв случай не може да се определи в даден момент и след това да се остави в сила неограничено, независимо от наличието на всякакви промени в обстоятелствата, показващи в действителност, че предоставяната степен на защита вече не е достатъчна.

147. Следователно задължението на третата страна да гарантира достатъчна степен на защита представлява непрекъснато задължение. Ако оценката е извършена в определен момент, оставянето в сила на решението относно достатъчния характер на защитата предполага, че междувременно не е настъпила промяна в обстоятелствата, която да постави под въпрос извършената от Комисията първоначална оценка.

148. Всъщност не трябва да се забравя, че целта на член 25 от Директива 95/46 е да не се допусне прехвърляне на данните към трета страна, която не гарантира достатъчна степен на защита, в нарушение на основното право на защита на личните данни, гарантирано от член 8 от Хартата.

149. Важно е да се подчертае, че правомощието, предоставено на Комисията от законодателя на Съюза в член 25, параграф 6 от Директива 95/46, да констатира дали дадена трета страна гарантира достатъчна степен на защита, изрично е поставено в зависимост от изискването въпросната трета страна да гарантира достатъчна степен на защита по смисъла на параграф 2 от този член. Ако нови обстоятелства могат да поставят под въпрос първоначалната оценка на Комисията, тя трябва да адаптира решението си в съответствие с тях.

3. Моята преценка

150. Ще припомня, че съгласно член 25, параграф 6 от Директива 95/46 „Комисията може да констатира, в съответствие с процедурата, посочена в член 31, параграф 2, че трета страна гарантира достатъчна степен на защита по смисъла на параграф 2 на настоящия член, по силата на вътрешното си законодателство или на международните споразумения, сключени от нея, и по-конкретно след приключване на преговорите, упоменати в параграф 5, за защитата на личния живот и на основните свободи и права на лицата“. При тълкуване във връзка с член 25, параграф 2 от тази директива, от член 25, параграф 6 от нея следва, че за да установи дали трета страна гарантира достатъчна степен на защита, Комисията трябва да извърши преценка на всички действащи правни норми в тази трета страна и на тяхното приложение.

151. Както вече бе посочено, оставянето в сила на Решение 2000/520 от Комисията, въпреки настъпването на нови правни и фактически обстоятелства, трябва да се разбира като желание от нейна страна на потвърди първоначалната си оценка.

152. В рамките на преюдициално запитване Съдът не следва да се произнася по обстоятелствата, които са в основата на спора, накарали националната юрисдикция да отправи това запитване [57].

153. Ето защо ще се позова на обстоятелствата, посочени от запитващата юрисдикция в преюдициалното ѝ запитване — обстоятелства, които освен това в голяма степен са приети за установени от самата Комисия [58].

154. Обстоятелствата, посочени пред Съда с цел се оспори оценката на Комисията, съгласно която схемата за сфера на неприкосновеност гарантира достатъчна степен на защита на прехвърляните от Съюза към САЩ данни, могат да бъдат описани по следния начин.

155. В преюдициалното си запитване запитващата юрисдикция използва като отправна точка две фактически констатации. От една страна, личните данни, прехвърляни от предприятия като Facebook Ireland към установеното в САЩ тяхно дружество майка, впоследствие могат да бъдат достъпни за NSA, както и за други американски агенции за сигурност, в хода на дейности по масово и нецеленасочено наблюдение и прихващане. Всъщност вследствие на разкритията на г-н Сноудън от наличните доказателства понастоящем не можело да се направи друго правдоподобно заключение [59]. От друга страна, гражданите на Съюза не разполагали с никакво ефективно право да бъдат изслушвани по въпроса за наблюдението и прихващането на техните данни от NSA и други американски агенции за сигурност [60].

156. Така направените от High Court фактически констатации са подкрепени от извършените от самата Комисия констатации.

157. В съобщението ѝ относно функционирането на сферата на неприкосновеност на личния живот от гледна точка на гражданите на ЕС и дружествата, установени в ЕС, посочено по-горе, отправна точка за Комисията е констатацията, че през 2013 г. информацията за мащаба и обхвата на американските програми за наблюдение е породила опасения за това дали личните данни, прехвърляни законно към САЩ в рамките на схемата за неприкосновеност, продължават да са защитени. Тя посочва, че всички предприятия, участващи в програмата PRISM, които предоставят достъп на американските власти до данни, съхранявани и обработвани в САЩ, изглежда са сертифицирани по схемата за сфера на неприкосновеност. Според Комисията това е превърнало схемата в един от каналите, посредством които се предоставя достъп на американските разузнавателни служби за събиране на лични данни, първоначално обработени в ЕС [61].

158. От гореизложеното следва, че правото и практиката на САЩ позволяват широкомащабно събиране на лични данни на граждани на Съюза, които се прехвърлят в рамките на схемата за сфера на неприкосновеност, без последните да разполагат с ефективна съдебна защита.

159. Според мен тези фактически констатации показват, че Решение 2000/520 не съдържа достатъчно гаранции. Поради липсата на гаранции то е приложено по начин, който не отговаря на нужните изисквания на Хартата и на Директива 95/46.

57 — Вж. по-специално решение Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, т. 22 и цитираната съдебна практика).

58 — Вж. съобщението на Комисията, посочено в бележка под линия 2, и Съобщение на Комисията до Европейския парламент и Съвета относно функционирането на „сферата на неприкосновеност на личния живот“ („Safe Harbour“) от гледна точка на гражданите на ЕС и дружествата, установени в ЕС (COM(2013) 847 окончателен).

59 — Точка 7, буква в) от акта за преюдициално запитване.

60 — Точка 7, буква б) от акта за преюдициално запитване.

61 — Стр. 20 от съобщението.

160. Комисията приема решения въз основа на член 25, параграф 6 от Директива 95/46, за да констатира, че дадена трета страна „гарантира“ достатъчна степен на защита. Терминът „гарантира“, спрегнат в сегашно време, означава, че за да бъде оставено в сила подобно решение, то трябва да се отнася за трета страна, която след приемането му продължава да гарантира достатъчна степен на защита.

161. Всъщност направените разкрития относно действията на NSA, която използвала прехвърлени в рамките на схемата за сфера на неприкосновеност данни, ясно показват слабостите на правното основание, каквото е Решение 2000/520.

162. Недостатъците, разкрити в хода на настоящото производство, са посочени по-специално в приложение I, четвърта алинея към това решение.

163. Ще припомня, че съгласно тази разпоредба „[п]ридържането към принципите [за сфера на неприкосновеност] може да бъде ограничено: а) до необходимата степен, с оглед спазване изискванията за националната сигурност, обществения интерес или изискванията на правоприлагането [в САЩ]; б) със закон, правителствено регулиране или съдебна практика, които пораждат взаимнопротиворечиви задължения или предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на принципите е ограничено до необходимата степен за гарантиране на първостепенните законово предвидени интереси, за които е поискано разрешителното“.

164. Проблемът се дължи най-вече на използването от страна на американските власти на предвидените в посочената разпоредба дерогации. Поради твърде общата им формулировка прилагането на тези дерогации от посочените власти не се ограничава до строго необходимото.

165. Към тази твърде обща формулировка се добавя обстоятелството, че гражданите на Съюза не разполагат с подходящи правни средства за защита срещу обработката на личните им данни за цели, различни от тези, за които са събрани първоначално и след това са прехвърлени към САЩ.

166. Предвидените в Решение 2000/520 дерогации от прилагането на принципите за сфера на неприкосновеност, по-специално относно изискванията, свързани с националната сигурност, е трябвало да бъдат съпътствани от въвеждането на годен механизъм за независим надзор за предотвратяване на установените нарушения на правото на личен живот.

167. Така разкритията относно практиките на американските разузнавателни служби във връзка с всеобхватното наблюдение на данните, прехвърляни в рамките на схемата за сфера на неприкосновеност, разкриват някои недостатъци на Решение 2000/520.

168. Твърдените в разглеждания случай деяния не съставляват нарушение от страна на Facebook на принципите за сфера на неприкосновеност. Ако сертифицирано предприятие като Facebook USA предоставя достъп на американските власти до данните, прехвърлени му от държава членка, може да се приеме, че то прави това, за да се съобрази с американското законодателство. Предвид обстоятелството, че подобна хипотеза се допуска изрично в Решение 2000/520 поради широката формулировка на съдържащите се в него дерогации, на практика в настоящото дело въпросът е дали такива дерогации са съвместими с първичното право на Съюза.

169. В това отношение следва да се подчертае, че съгласно постоянната практика на Съда спазването на правата на човека е условие за законосъобразност на актовете на Съюза и че Съюзът не може да допуска мерки, които са несъвместими със спазването на тези права[62].

170. Освен това от практиката на Съда е видно, че предоставянето на събрани лични данни на трети лица — публични органи или частноправни субекти, представлява намеса, засягаща правото на зачитане на личния живот, „независимо от последващото използване на така предоставените данни“[63]. В решение Digital Rights Ireland и др.[64] Съдът също така потвърждава, че разрешаването на достъп до такива данни на компетентните национални органи представлява отделно нарушение на това основно право[65]. В допълнение, всякакъв вид обработване на лични данни попада в обхвата на член 8 от Хартата и представлява намеса, засягаща правото на защита на личните данни[66]. Следователно достъпът, с който разполагат американските разузнавателни служби, до прехвърляните данни също представлява намеса, засягаща основното право на защита на личните данни, гарантирано от член 8 от Хартата, тъй като подобен достъп представлява обработване на тези данни.

171. Както Съдът констатира в това решение, така идентифицираната намеса се оказва широкомащабна и трябва да се счита за особено тежка предвид големия брой засегнати потребители и количеството прехвърлени данни. Тези обстоятелства и тайният характер на достъпа на американските власти до личните данни, прехвърлени към установените в САЩ предприятия, правят намесата изключително сериозна.

172. Към това се прибавя и фактът, че гражданите на Съюза — потребители на Facebook, не са уведомени, че личните им данни ще бъдат общодостъпни за американските агенции за сигурност.

173. Следва също така да се подчертае, че запитващата юрисдикция е установила, че в САЩ гражданите на Съюза не разполагат с никакво ефективно право да бъдат изслушани по въпроса за наблюдението и прихващането на техните данни. FISC упражнява надзор, но производството пред него е поверително и няма състезателен характер[67]. Смятам, че в случая става въпрос за намеса, засягаща закрилното с член 47 от Хартата право на гражданите на Съюза на ефективни правни средства за защита.

174. Следователно налице е намеса, която е разрешена с посочените в приложение I, четвърта алинея към Решение 2000/520 дерогации от принципите за сфера на неприкосновеност и която засяга основните права, защитени в членове 7, 8 и 47 от Хартата.

175. По-нататък следва да се провери дали тази намеса е обоснована или не.

176. Съгласно член 52, параграф 1 от Хартата всяко ограничаване на упражняването на признатите от Хартата права и свободи трябва да бъде предвидено в закон и да зачита основното съдържание на същите права и свободи. При спазване на принципа на пропорционалност ограниченията на тези права и свободи могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

62 — Вж. по-специално решение Kadi и Al Barakaat International Foundation/Съвет и Комисия (C-402/05 P и C-415/05 P, EU:C:2008:461, т. 284 и цитираната съдебна практика).

63 — Решение Österreichischer Rundfunk и др. (C-465/00, C-138/01 и C-139/01, EU:C:2003:294, т. 74).

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

65 — Точка 35.

66 — Точка 36.

67 — Точка 7, буква б) от акта за преюдициално запитване.

177. Предвид така определените условия за допускане на ограничения в упражняването на защитаваните от Хартата права и свободи силно се съмнявам, че разглежданите в настоящото дело ограничения могат да се смятат за съответстващи на основното съдържание на членове 7 и8 от Хартата. Всъщност достъпът на американските разузнавателни служби до прехвърляните данни изглежда обхваща съдържанието на електронните съобщения, което би засегнало същественото съдържание на основното право на зачитане на личния живот и останалите права, признати от член 7 от Хартата. Освен това, доколкото широката формулировка на ограниченията, предвидени в приложение I, четвърта алинея към Решение 2000/520, потенциално позволява да не се прилагат всички принципи за сфера на неприкосновеност, може да се приеме, че тези ограничения засягат същественото съдържание на основното право на защита на личните данни[68].

178. Колкото до въпроса дали установената намеса отговаря на цел от общ интерес, на първо място ще припомня, че съгласно приложение I, четвърта алинея, буква б) към Решение 2000/520 придържането към принципите за сфера на неприкосновеност може да бъде ограничено „със закон, правителствено регулиране или съдебна практика, които пораждат взаимнопротиворечиви задължения или предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на принципите е ограничено до необходимата степен за гарантиране на първостепенните законово предвидени интереси, за които е поискано разрешителното“.

179. Трябва да се констатира, че „законово предвидените интереси“, споменати в посочената разпоредба, не са уточнени. Това води до несигурност по отношение на възможното твърде широко приложно поле на тази дерогация от прилагането на принципите за сфера на неприкосновеност от страна на придържащите се към принципите предприятия.

180. Текстът на разясненията, съдържащи се в буква Б от приложение IV към Решение 2000/520, озаглавено „Изрични законови разрешения“, потвърждава това впечатление и по-специално твърдението, според което „[е ясно], че когато американското законодателство предвижда конфликтно задължение, американските организации, били те спазващи принципите „сфера на неприкосновеност на личния живот“ или не, са длъжни да спазват това законодателство“. Що се отнася до изричните разрешения, посочва се, че „ако принципите „сфера на неприкосновеност на личния живот“ трябва да запълнят пропастта между американския и европейския режими за защита на личния живот, ние трябва да спазваме законодателните прерогативи на избраните от нас законодатели“.

181. Според мен от това следва, че тази дерогация противоречи на членове 7 и 8 и член 52, параграф 1 от Хартата, доколкото не преследва цел от общ интерес, определена по достатъчно точен начин.

182. При всички случаи лесният и общ начин, по който в приложение I, четвърта алинея, буква б) към Решение 2000/520 и в приложение IV, буква Б към него се предвижда, че принципите за сфера на неприкосновеност могат да бъдат отхвърлени при прилагане на нормите от американското право, е несъвместим с условието, че дерогациите от правилата относно защитата на личните данни трябва да се ограничат до строго необходимото. Действително условието за необходимост е посочено, но макар доказването на това условие да е в тежест на съответното предприятие, не виждам как подобно предприятие може да не изпълни задължение за отклоняване от принципите за сфера на неприкосновеност, произтичащо от правни норми, които е длъжно да прилага.

68 — В това отношение решение вж. Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238, т. 39 и 40).

183. Поради това смятам, че Решение 2000/520 трябва да се обяви за невалидно, тъй като наличието на дерогация, която позволява по толкова общ и неточен начин отклоняване от принципите на схемата за сфера на неприкосновеност, самò по себе си не позволява да се приеме, че тази схема гарантира достатъчна степен на защита на личните данни, прехвърляни към САЩ от Съюза.

184. Колкото до първата категория ограничения, предвидени в приложение I, четвърта алинея, буква а) към Решение 2000/520 поради изискванията, свързани с националната сигурност, обществения интерес и спазването на американското право, единствено първата цел ми се струва, че е достатъчно точна, за да може да се определи като цел от общ интерес, призната от Съюза по смисъла на член 52, параграф 1 от Хартата.

185. По-нататък следва да се провери пропорционалността на установената намеса.

186. В това отношение следва да се припомни, че „съгласно постоянната практика на Съда принципът на пропорционалност изисква актовете на институциите на Съюза да са годни да постигнат легитимните цели, следвани от разглежданата правна уредба, и да не надхвърлят границите на подходящото и необходимото за постигането на тези цели“ [69].

187. Що се отнася до съдебния контрол за спазването на тези условия, „доколкото става въпрос за намеса в основни права, обхватът на правото на преценка на законодателя на Съюза може да се окаже ограничен в зависимост от някои фактори, сред които по-специално са съответният сектор, естеството на разглежданото право, гарантирано от Хартата, естеството и степента на намеса, както и нейната цел“ [70].

188. Смятам, че решенията, които Комисията приема въз основа на член 25, параграф 6 от Директива 95/46, подлежат на пълен контрол от страна на Съда, що се отнася до пропорционалността на извършената от тази институция оценка на достатъчния характер на степента на защита, предоставена от трета страна „по силата на вътрешното [ѝ] законодателство или на международните [ѝ] споразумения“.

189. В това отношение следва да се отбележи виждането на Съда в решение Digital Rights Ireland и др. [71], че „като се имат предвид, от една страна, важната роля на защитата на личните данни с оглед на основното право на зачитане на личния живот, и от друга страна, широтата и тежестта на уредена съгласно [оспорваната директива] намеса в него, правото на преценка на законодателя на Съюза се оказва ограничено, поради което следва да бъде упражнен стриктен контрол“ [72].

190. Подобна намеса трябва да може да постигне целта на разглеждания акт на Съюза и да бъде необходима за постигането на тази цел.

191. В това отношение „[щ]о се отнася до зачитането на личния живот, съгласно постоянната практика на Съда защитата на това основно право изисква [...] дерогациите и ограниченията на защитата на личните данни да се въвеждат в границите на строго необходимото“ [73].

69 — Решение Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238, т. 46 и цитираната съдебна практика).

70 — Пак там (т. 47 и цитираната съдебна практика).

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

72 — Точка 48.

73 — Решение Digital Rights Ireland и др. (C-293/12 и C 594/12, EU:C:2014:238, т. 52 и цитираната съдебна практика).

192. При упражняване на контрола си Съдът взема предвид и обстоятелството, че „във връзка с правото на зачитане на личния живот, провъзгласено в член 7 от Хартата, защитата на личните данни, произтичаща от изричното задължение, предвидено в член 8, параграф 1 от нея, придобива особено значение“ [74].

193. Според Съда, който в това отношение се позовава на практиката на Европейския съд по правата на човека, „разглежданата правна уредба на Съюза трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито данни са били запазени, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби, както и срещу всякакъв незаконен достъп или използване на тези данни“ [75]. Съдът посочва, че „[н]еобходимостта от такива гаранции е още по-голяма, когато [...] личните данни са подложени на автоматична обработка и съществува значителен риск от незаконен достъп до тях“ [76].

194. Според мен съществува аналогия между приложение I, четвърта алинея, буква а) към Решение 2000/520 и член 13, параграф 1 от Директива 95/46. В първата разпоредба е посочено, че придържането към принципите за сфера на неприкосновеност на личния живот може да бъде ограничено от „изискванията за националната сигурност, обществения интерес или изискванията на правоприлагането [в САЩ]“. Във втората разпоредба е предвидено, че държавите членки могат да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, предвидени в член 6, параграф 1, член 10, член 11, параграф 1, член 12 и член 21 от посочената директива, ако подобно ограничаване представлява необходима мярка за гарантиране по-специално на националната сигурност, отбраната, обществената сигурност, както и предотвратяването, разследването, разкриването и преследването на углавни престъпления.

195. Както Съдът посочва в своето решение IPI [77], от текста на член 13, параграф 1 от Директива 95/46 следва, че държавите членки могат да предвидят такива мерки единствено ако те са необходими. Следователно „необходимостта“ от мерките обуславя възможността на държавите членки, предоставена с посочената разпоредба [78]. За обработването на лични данни в рамките на Съюза предвидените в член 13 от тази директива ограничения трябва да се разбират като сведени до строго необходимото за постигане на преследваната цел. Според мен това трябва да се отнася и за предвидените в приложение I, четвърта алинея към Решение 2000/520 ограничения на принципите за сфера на неприкосновеност.

196. Следва обаче да се констатира, че не всички текстове на различните езици на приложение I, четвърта алинея, буква а) към Решение 2000/520 съдържат критерия за необходимост. Такъв е случаят по-специално с текста на френски език, в който се посочва, че „[l]'adhésion aux principes peut être limitée par [...] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis“, докато например в текстовете на испански, немски и английски език се отбелязва, че въведените ограничения трябва да бъдат необходими за постигане на горепосочените цели.

197. Във всеки случай фактическите елементи, изтъкнати от запитващата юрисдикция, както и от Комисията в горепосочените ѝ съобщения, ясно показват, че на практика прилагането на тези ограничения не е сведено до строго необходимото за постигане на поставените цели.

74 — Пак там (т. 53).

75 — Пак там (т. 54 и цитираната съдебна практика).

76 — Пак там (т. 55 и цитираната съдебна практика).

77 — C-473/12, EU:C:2013:715.

78 — Точка 32.

198. В това отношение ще отбележа, че достъпът до прехвърлените лични данни, с който разполагат американските разузнавателни служби, в общ план включва всички лица и всички средства за електронна комуникация, както и всички прехвърлени данни, включително съдържанието на съобщенията, без да се прави никакво разграничение, ограничение или изключение в зависимост от преследваната цел от общ интерес [79].

199. Всъщност достъпът на американските разузнавателни служби до прехвърляните данни засяга общо всички лица, които използват електронни съобщителни услуги, без да е необходимо съответните лица да представляват заплаха за националната сигурност [80].

200. Подобно масово и нецеленасочено наблюдение е непропорционално по своето естество и представлява неоправдана намеса, засягаща гарантираните в членове 7 и 8 от Хартата права.

201. Както с основание посочва Парламентът в становището си, тъй като за законодателя на Съюза или за държавите членки е невъзможно да приемат законови разпоредби, които в нарушение на Хартата да предвиждат масово и нецеленасочено наблюдение, оттук, a fortiori, непременно следва, че в никакъв случай не може да се смята, че трети страни могат да гарантират достатъчна степен на защита на личните данни на гражданите на Съюза, ако тяхната правна уредба действително разрешава масово и нецеленасочено наблюдение и прихващане на този вид данни.

202. Освен това е важно да се подчертае, че схемата за сфера на неприкосновеност, както е определена в Решение 2000/520, не съдържа гаранции, които могат да предотвратят масов и всеобхватен достъп до прехвърлените данни.

203. В това отношение ще отбележа, че в Решение Digital Rights Ireland и др. [81] Съдът подчертава значението на това да се предвидят „ясни и точни правила, определящи обхвата на намеса в основните права, закрепени в членове 7 и 8 от Хартата“ [82]. Подобна намеса според Съда трябва да е „точно уредена с разпоредби, които да могат да гарантират, че тя действително се свежда до строго необходимото“ [83]. В същото решение Съдът изтъква и необходимостта да се предвидят „достатъчни гаранции, каквито се изискват от член 8 от Хартата, позволяващи да се осигури ефикасна защита на [личните] данни срещу рискове от злоупотреба, както и срещу всякакъв незаконен достъп и незаконно използване на тези данни“ [84].

204. Налага се изводът, че механизмите на частния арбитраж и FTC, поради своята ограничена до търговските спорове роля, не са средства за оспорване на достъпа на американските разузнавателни служби до прехвърлените от Съюза лични данни.

205. Компетентността на FTC обхваща нелоялните и измамните действия и практики в областта на търговията и съответно не се отнася до събирането и използването на личните данни за нетърговски цели [85]. Ограничената област на компетентност на FTC ограничава правото на частноправните субекти на защита на личните им данни. FTC е създадена не за гарантиране на защитата на индивидуалното право на личен живот, за което са създадени националните

79 — Вж. по аналогия решение Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238, т. 57 и цитираната съдебна практика).

80 — Пак там (т. 58 и 59).

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

82 — Точка 65

83 — Пак там.

84 — Пак там (т. 66).

85 — В това отношение вж. приложение II, ЧЗВ 11 към Решение 2000/520, „Действие на Федералната търговска комисия“, и приложения III, V и VII към него.

надзорни органи в Съюза, а за гарантиране на лоялна и надеждна търговия на потребителите, което de facto ограничава възможностите ѝ за намеса в сферата на защитата на личните данни. Следователно FTC не изпълнява роля, сравнима с тази на националните надзорни органи, предвидени в член 28 от Директива 95/46.

206. Гражданите на Съюза, чиито данни са прехвърлени, могат да се обръщат към установени в САЩ специализирани арбитражни органи като TRUSTe и BBBOnline за получаване на уточнения по въпроса дали предприятието, което притежава личните им данни, нарушава условията на режима за самосертифициране. Осигуряваният от организации като TRUSTe частен арбитраж не може да разглежда нарушения на правото на защита на личните данни, извършени от организации или органи, различни от самосертифицираните предприятия. Тези арбитражни организации не разполагат с никаква компетентност да се произнасят по законосъобразността на дейностите на американските агенции за сигурност.

207. Следователно нито FTC, нито частните арбитражни организации не разполагат с компетентност за проверка на възможните нарушения на принципите на защита на личните данни, извършени от публичноправни субекти като американските служби за сигурност. Подобна компетентност обаче е съществена за пълното гарантиране на ефективната защита на тези данни. Следователно при приемането на Решение 2000/520 и оставянето му в сила Комисията не е можела да констатира, че за всички прехвърляни към САЩ лични данни се гарантира достатъчна защита на правото, предоставено в член 8, параграф 3 от Хартата, тоест че независим орган упражнява ефективен контрол за спазването на изискванията за защита и неприкосновеност на тези данни.

208. Ето защо трябва да се констатира, че в рамките на предвидената в Решение 2000/520 схема за сфера на неприкосновеност липсва независим орган, който може да контролира това дали прилагането на дерогациите от принципите за сфера на неприкосновеност се ограничава до строго необходимото. Както вече стана ясно, от гледна точка на правото на Съюза такъв контрол от независим орган представлява съществен елемент от осигуряването на защита на лицата при обработването на лични данни [86].

209. В това отношение следва да се подчертае ролята, която националните надзорни органи изпълняват в действащата в Съюза система на защита на личните данни при контрола на ограниченията, предвидени в член 13 от Директива 95/46. Съгласно член 28, параграф 4, втора алинея от тази директива „[в]секи надзорен орган, в частност, разглежда искове за проверка на законосъобразността на обработването на данни, подадени от което и да е лице, когато се прилагат националните разпоредби, приети съгласно член 13 на настоящата директива“. По аналогия, смятам, че споменаването на ограничения при прилагането на принципите за сфера на неприкосновеност в приложение I, четвърта алинея към Решение 2000/520 би трябвало да бъде съпроводено с въвеждането на контролен механизъм, чието действие се осигурява от независим орган, специализиран в областта на защитата на личните данни.

210. Всъщност намесата от страна на независими надзорни органи е в основата на европейската система за защита на личните данни. Ето защо, съвсем естествено, наличието на такива органи изначално се счита за едно от необходимите условия, за да се направи констатацията, че предоставяната от третите страни степен на защита е достатъчна. В случая става въпрос за условие, което е необходимо, за да не бъдат забранени потоците от данни от територията на държавите членки към тази на трети страни в съответствие с член 25 от Директива 95/46 [87].

86 — Вж. решение Digital Rights Ireland и др. (C-293/12 и C-594/12, EU:C:2014:238, т. 68 и цитираната съдебна практика).

87 — Вж. *Poullet*, Y. L'autorité de contrôle: „vues“ de Bruxelles. — Revue française d'administration publique, № 89, janvier—mars 1999, p. 69, p. 71.

Както се посочва в документа за обсъждане, приет от създадената с член 29 от Директивата работна група, в Европа съществува широк консенсус за това, че „механизмът за „външен контрол“ под формата на независим орган е необходим за всяка система елемент, с който се цели да се гарантира спазването на правилата относно защитата на данни“ [88].

211. Освен това ще отбележа, че FISC не предлага ефективно средство за съдебна защита на гражданите на Съюза, чиито лични данни се прехвърлят към САЩ. Всъщност защитата срещу наблюдението от правителствените служби по раздел 702 от Закона от 1978 г. за наблюдение на чуждите разузнавателни служби се прилага единствено за американските граждани, както и за чуждестранните граждани, пребиваващи законно и постоянно в САЩ. Както самата Комисия посочва, контролът на американските програми за събиране на сведения може да бъде подобрен, като се засили ролята на FISC и се въвеждат правни средства за защита на физическите лица. Тези механизми биха могли да намалят обработката на лични данни на граждани на Съюза, които не са от значение за целите на националната сигурност [89].

212. Впрочем самата Комисия посочва, че гражданите на Съюза нямат никаква възможност да получат достъп, поправка или заличаване на данни или административна или съдебна защита по отношение на събирането и по-нататъшното обработване на личните им данни, които се провеждат в рамките на американските програми за наблюдение [90].

213. Накрая следва да се посочи, че американските норми относно закрилата на личния живот могат да се прилагат различно за американските и за чуждестранните граждани [91].

214. От гореизложеното следва, че Решение 2000/520 не предвижда ясни и точни правила, определящи обхвата на намесата, засягаща основните права, закрепени в членове 7 и 8 от Хартата. Налага се изводът, че от това решение и неговото приложение произтича широкомащабна и особено тежка намеса, засягаща тези основни права, без намесата да е точно уредена с разпоредби, които могат да гарантират, че тя действително се свежда до строго необходимото.

215. Така с приемането на Решение 2000/520 и оставянето му в сила Комисията е надхвърлила границите, които спазването на принципа на пропорционалност налага с оглед на членове 7 и 8 и член 52, параграф 1 от Хартата. Към това се прибавя констатацията за наличие на необоснована намеса, засягаща закриляното с член 47 от Хартата право на гражданите на Съюза на ефективна защита.

216. Следователно това решение трябва да се обяви за невалидно, тъй като поради описаните по-горе нарушения на основните права не може да се приеме, че схемата за сфера на неприкосновеност, въведена с него, гарантира достатъчна степен на защита на личните данни, прехвърляни от Съюза към САЩ в рамките на същата схема.

217. С оглед на констатираните нарушения на основните права на гражданите на Съюза смятам, че Комисията е трябвало да спре прилагането на Решение 2000/520.

218. Действието на това решение е неограничено във времето. Настоящото дело показва обаче, че достатъчният характер на степента на защита, предоставяна от трета страна, може да се променя във времето в зависимост от промените на правните и фактическите обстоятелства, въз основа на които е прието посоченото решение.

88 — Вж. стр. 7 от работния документ РГ 12 на Комисията, посочен в бележка под линия 56.

89 — Стр. 10 и 11 от Съобщението на Комисията, посочено в бележка под линия 2.

90 — Вж. точка 7.2 на стр. 21 от Съобщението на Комисията, посочено в бележка под линия 58.

91 — По този въпрос вж. *Kuner*, C. Foreign Nationals and Data Protection Law: A Transatlantic Analysis. — Data Protection Anno 2014: How To Restore Trust? Intersentia, Cambridge, 2014, p. 213, p. 216 et sq.

219. Ще отбележа, че самото Решение 2000/520 съдържа разпоредби, предвиждащи възможност Комисията да го адаптира в зависимост от обстоятелствата.

220. Както е видно от съображение 9 от това решение „[в]ъзможно е да се наложи „личната неприкосновеност“, създадена според принципите и ЧЗВ, да бъде преразгледана в светлината на опита и на тенденциите в областта на защитата на личния живот при условията, където технологията позволява все по-лесно да се предават и обработват лични данни, както и в светлината на докладите относно изпълнението от компетентните правоприлагащи органи“.

221. По същия начин съгласно член 3, параграф 4 от посоченото решение, „[а]ко информациите, събрани съгласно параграфи 1, 2 и 3, представят доказателства, че някоя институция, натоварена със задачата да контролира спазването на принципите, приети по силата на ЧЗВ в Съединените щати, не изпълнява ефикасно задачата си, Комисията информира Департамента по търговия на САЩ и ако е необходимо, предлага проектомерки за приемане […] с цел заличаването или преустановяването на действието на настоящото решение или за да се ограничи обхватът му“.

222. Освен това съгласно член 4, параграф 1 от Решение 2000/520 то „може да бъде адаптирано във всеки един момент в светлината на натрупания опит по време на неговото прилагане и/или ако нивото на защита, осигурено от принципите и ЧЗВ, се окаже недостатъчно спрямо изискванията на законодателството на САЩ. Независимо от всичко това Комисията преценява прилагането на настоящото решение въз основа на информацията, с която разполага, три години след нотификацията му до държавите членки и съобщава на комитета, създаден по силата на член 31 от Директива 95/46[…], всички документи, които биха повлияли върху оценката, според която разпоредбите на член 1 от настоящото решение гарантират достатъчно ниво на защита по смисъла на член 25 от Директива 95/46“. Съгласно член 4, параграф 2 от Решение 2000/520 „Комисията представя, ако е необходимо, проектомерки в съответствие с процедурата, предвидена в член 31 от Директива 95/46“.

223. В писменото си становище Комисията констатира, че „има голяма вероятност […] придържането към принципите за сфера на неприкосновеност на личния живот да е било ограничено така, че вече да не отговаря на строго установените условия за изключението, предвидено в областта на националната сигурност“ [92]. В това отношение тя отбелязва, че „[в]ъпросните разкрития показват широкомащабна и несистематизирана по своето естество степен на наблюдение, която е несъвместима с предвидения в това изключение критерий за необходимост, нито, в по-общ план, с правото на защита на личните данни, установено в член 8 от Хартата“ [93]. Самата Комисия констатира също, че „[о]бхватът на [програмите] за наблюдение, заедно с неравностойното третиране на гражданите на [Съюза], поставя под съмнение нивото на защита, предоставяно от споразумението за сфера на неприкосновеност“ [94].

224. Освен това в съдебното заседание Комисията изрично признава, че в рамките на Решение 2000/520, както то се прилага понастоящем, няма гаранции, че правото на гражданите на Съюза на защита на техните данни ще бъде закриляно. Според нея обаче тази констатация не може да доведе до невалидност на решението. Макар Комисията да е съгласна с твърдението, че трябва да действа с оглед на нови обстоятелства, тя смята, че е взела подходящи и пропорционални мерки, започвайки преговори със САЩ за преразглеждане на схемата за сфера на неприкосновеност.

225. Не споделям това становище. Всъщност прехвърлянето на лични данни към САЩ междувременно трябва да може се спре по инициатива на националните надзорни органи или вследствие на подадени до тях жалби.

92 — Точка 44

93 — Пак там.

94 — Вж. стр. 5 от Съобщението на Комисията, посочено в бележка под линия 2.

226. Освен това смятам, че с оглед на тези констатации, Комисията е трябвало да спре прилагането на Решение 2000/520. Всъщност целта за защита на личните данни, преследвана от Директива 95/46 и от член 8 от Хартата, налага задължения не само за държавите членки, но и за институциите на Съюза, както е видно от член 51, параграф 1 от Хартата.

227. В оценката си на степента на защита, предоставяна от трета страна, Комисията трябва да разгледа не само вътрешното законодателство и международните споразумения на тази трета страна, но и начина, по който защитата на личните данни се гарантира на практика. Ако прегледът на практиката разкрива недостатъци във функционирането, Комисията трябва да реагира и при необходимост да спре прилагането на решението си и/или да го адаптира незабавно.

228. Както вече посочих в изложението си по-горе, задължението, с което са натоварени държавите членки, се състои основно в гарантиране на спазването на предвидените в Директива 95/46 правила чрез дейността на националните им надзорни органи.

229. Задължението на Комисията в случай на установено неизпълнение на задължения от съответната трета страна е да спре прилагането на решение, което е приела въз основа на член 25, параграф 6 от тази директива, докато води преговори с нея с цел преустановяване на неизпълнението.

230. Ще припомня, че с приетото от Комисията решение въз основа на тази разпоредба се цели да се констатира, че дадена трета страна „гарантира“ достатъчна степен на защита на личните данни, които се прехвърлят към тази трета страна. Терминът „гарантира“, спрегнат в сегашно време, означава, че за да бъде оставено в сила подобно решение, то трябва да се отнася за трета страна, която след приемането му продължава да гарантира достатъчна степен на защита.

231. Съгласно съображение 57 от Директива 95/46 „предаването на лични данни в трета страна, която не гарантира достатъчно висока степен на защита, трябва да бъде забранено“.

232. Съгласно член 25, параграф 4 от тази директива „[а]ко Комисията констатира, съгласно процедурата, предвидена в член 31, параграф 2, че дадена трета страна не осигурява достатъчна степен на защита по смисъла на параграф 2 на настоящия член, държавите членки взимат необходимите мерки за предотвратяване на всякакво предаване на данни от същия вид на въпросната трета страна“. Освен това в член 25, параграф 5 от Директива се посочва, че „[в] подходящия момент Комисията започва преговори с цел да поправи състоянието на нещата, произтичащо от заключенията, направени съгласно параграф 4“.

233. От последната разпоредба е видно, че в установената с член 25 от Директива 95/46 система преговорите, започнати с трета страна, имат за цел да се отстрани липсата на достатъчна степен на защита, констатирана съгласно процедурата, предвидена в член 31, параграф 2 от посочената директива. В разглеждания случай Комисията не е констатирала формално съгласно тази процедура, че схемата за сфера на неприкосновеност вече не гарантира достатъчна степен на защита. При това положение Комисията обаче решава да започне преговори със САЩ именно защото преди това е приела, че гарантираната в тази трета страна степен на защита вече не е достатъчна.

234. Въпреки че е знаела за недостатъците във функционирането при прилагането на Решение 2000/520, Комисията нито е спряла прилагането на последното, нито го е адаптирала, поради което извършването на нарушението на основните права на лицата, чиито лични данни са били прехвърлени и продължават да бъдат прехвърляни в рамките на схемата за сфера на неприкосновеност, е продължило.

235. Съдът обаче постановява — наистина в друг контекст — че Комисията трябва да се грижи за адаптиране на правната уредба с оглед на новите данни [95].

236. Подобно бездействие на Комисията, което пряко накърнява основните права, защитени с членове 7, 8 и 47 от Хартата, според мен представлява допълнително съображение за обявяване на Решение 2000/520 за невалидно в рамките на настоящото преюдициално запитване [96].

III – **Заключение**

237. С оглед на гореизложените съображения предлагам на Съда да отговори на поставените от High Court въпроси по следния начин:

Член 28 от Директива 95/46/ЕО 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, разглеждан във връзка с членове 7 и 8 от Хартата на основните права на Европейския съюз, трябва да се тълкува в смисъл, че наличието на решение, прието от Комисията въз основа на член 25, параграф 6 от Директива 95/46, не е пречка национален надзорен орган да проведе разследване по жалба, в която се твърди, че трета страна не гарантира достатъчна степен на защита на прехвърляните лични данни, и при необходимост да спре прехвърлянето на тези данни.

Решение 2000/520/ЕО на Комисията от 26 юли 2000 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ, е невалидно.

95 — Вж. в този смисъл решение Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, т. 40).

96 — Макар в свое решение T. Port (C-68/95, EU:C:1996:452) Съдът да приема, че „в договора не се предвижда възможност за отправяне на преюдициално запитване, с което национална юрисдикция да поиска от Съда да установи в рамките на производството по запитването, че е налице неправомерно бездействие от страна на институция“ (т. 53), изглежда в решение Ten Kate Holding Musselkanaal и др. (C-511/03, EU:C:2005:625, т. 29) Съдът възприема по-благоприятна позиция по отношение на тази възможност.