Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
M. CAMPOS SÁNCHEZ-BORDONA
представено на 12 май 2016 година [1]

Дело C-582/14

Patrick Breyer
срещу
Bundesrepublik Deutschland(Преюдициално запитване,

отправено от Bundesgerichtshof (Федерален върховен съд, Германия)

„Обработване на лични данни — Директива 95/46/ЕО — Член 2, буква а) и член 7, буква е) — Понятие за лични данни — IP адреси — Съхраняване от доставчик на услуги за електронни медии — Национално законодателство, което не допуска отчитане на законния интерес, преследван от администратора на лични данни“

1. Адрес по интернет протокол (наричан по-нататък „IP адрес“) е поредица от двоични числа, обозначаваща дадено устройство (компютър, таблет, смартфон), която го идентифицира и позволява достъпа до електронната съобщителна мрежа. За да се свърже с интернет, устройството трябва да използва числовата поредица, предоставена от доставчиците на услугата за достъп до мрежата. IP адресът се изпраща до сървъра, където се намира ползвания интернет сайт.

2. По-конкретно, доставчиците на услуги за достъп до мрежата (обикновено телефонните компании) предоставят на своите клиенти временно, при всяко свързване с интернет, така наречените „динамични IP адреси“, които биват променяни при последващи свързвания. Същите тези компании поддържат регистър за това какви IP адреси са били предоставени във всеки един момент на конкретно устройство [2].

3. Обикновено притежателите на уебсайтове, достъпни чрез динамичните IP адреси, също поддържат регистри, в които се съхранява информацията кои сайтове са посетени, кога и от кой динамичен IP адрес. От техническа гледна точка тези регистри могат да бъдат съхранявани без ограничения във времето след преустановяване на интернет връзката на съответния ползвател.

4. Сам по себе си динамичният IP адрес не е достатъчен, за да може доставчикът на услуги да идентифицира ползвателя на неговия интернет сайт. Това обаче е възможно, ако динамичният IP адрес се свърже с други допълнителни данни, с които разполага доставчикът на услуга за достъп до мрежата.

1 — Език на оригиналния текст: испански.

2 — Член 5 от Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51), наред с други задължения, изисква запазването за целите на разследване, разкриване и преследване на престъпления „датата и времето на влизането и излизането от услугата за интернет достъп […] заедно с IP адреса, бил той динамичен или статичен, присвоен на дадено съобщение от доставчика на услугата за интернет достъп, и идентификатора на ползвател на абоната или регистрирания ползвател“.

5. Спорът в настоящото производство е за това дали динамичните IP адреси представляват лични данни по смисъла на член 2, буква а) от Директива 95/46/ЕО[3]. За неговото разрешаване е необходимо, на първо място, да се прецени какво е значението във връзка с това на обстоятелството, че с необходимите за идентифициране на ползвателя допълнителни данни не разполага притежателят на интернет сайта, а трето лице (по-конкретно доставчикът на услуги за достъп до мрежата).

6. Това е нов за Съда въпрос, доколкото, макар в точка 51 от решение Scarlet Extended[4] същият да постановява, че IP адресите са „защитени лични данни, тъй като позволяват точното идентифициране на ползвателите“, този извод е направен във връзка със събирането и идентифицирането на IP адреси от страна на осигуряващия достъп до мрежата[5], а не от доставчик на съдържание, какъвто е разглежданият случай.

7. Ако бъде прието, че динамичните IP адреси са лични данни за доставчика на интернет услуги, на следващо място, трябва да се прецени дали тяхното обработване попада в обхвата на приложение на Директива 95/46.

8. Възможно е тези IP адреси, макар и да са лични данни, да не се ползват с произтичащата от Директива 95/46 закрила, ако например целта на тяхното обработване е наказателно преследване срещу евентуални атаки спрямо съответния интернет сайт. В такъв случай Директива 95/46 е неприложима съгласно предвиденото в член 3, параграф 2, първо тире от нея.

9. Освен това следва да се прецени дали доставчикът на услуги, който регистрира динамичните IP адреси при осъществяване на достъп до интернет сайтовете му от ползвател (в случая Федерална република Германия), действа като публичноправен орган или по-скоро като частноправен субект.

10. Ако се прилага Директива 95/46, трябва, на последно място, да се уточни доколко член 7, буква е) от същата директива допуска национално законодателство, което ограничава обхвата на едно от установените в посочената разпоредба условия, при които се допуска обработването на лични данни.

I – **Правна уредба**

A– *Право на Съюза*

11. Съображение 26 от Директива 95/46 гласи следното:

„(26) като имат предвид, че принципите на защита трябва да се прилагат за всяка информация, отнасяща се до идентифицирано лице или подлежащо на идентификация лице; като имат предвид, че за да се определи дали едно лице подлежи на идентификация, следва да се разглежда съвкупността от всички средства, които биха могли да бъдат използвани разумно от администратора или от друго лице с цел идентифицирането на даденото лице; като имат предвид, че принципите на защита не се отнасят до данни, които са направени анонимни по начин, който прави невъзможно идентифицирането на съответното физическо лице; като имат предвид, че кодексите за поведение по смисъла на член 27

3 — Директива на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10).

4 — Решение от 24 ноември 2011 г. (C-70/10, EU:C:2011:771, т. 51).

5 — Същото се отнася и за решение от 19 април 2012 г., Bonnier Audio и др. (C-461/10, EU:C:2012:219, т. 51 и 52).

могат да бъдат полезно средство за предоставяне на указания относно начините, по които данните могат да бъдат направени анонимни и да бъдат съхранени във форма, която прави невъзможно идентифицирането на съответното физическо лице“.

12. Съгласно член 1 от Директива 95/46:

„1. В съответствие с настоящата директива държавите членки защищават основните права и свободи на физическите лица и в частност правото им на личен живот при обработването на лични данни.

2. Държавите членки не могат нито да ограничават, нито да забраняват свободното движение на лични данни между държавите членки по съображения, свързани със защитата, предоставяна съгласно параграф 1“.

13. Съгласно член 2 от Директива 95/46:

„По смисъла на настоящата директива:

а) „лични данни“ означава всяка информация, свързана с идентифицирано или подлежащо на идентификация лице („съответно физическо лице“); за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност;

б) „обработване на лични данни“ („обработване“) означава всяка операция или набор от операции, извършвани или не с автоматични средства, прилагани към личните данни, като събиране, запис, организиране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на предоставяне на данните, актуализиране или комбиниране, блокиране, изтриване или унищожаване;

[…]

г) „администратор“ означава физическо или юридическо лице, държавен орган, агенция или друг орган, който сам или съвместно с други определя целите и средствата на обработка на лични данни; когато целите и средствата на обработката се определят от национални или общностни законови или подзаконови разпоредби, администраторът или специфичните критерии за неговото назначаване могат да бъдат определени в националното право или в правото на Общността;

[…]

е) „трето лице“ означава всяко физическо или юридическо лице, държавен орган, агенция или друг орган, различни от съответното физическо лице, администратора, обработващия данните и лицата, които под прякото ръководство на администратора или обработващия данните, имат право да обработват данните;

[…]“.

14. Член 3 от Директива 95/46, озаглавен „Приложно поле“, предвижда:

„1. Настоящата директива се прилага към пълната или частична обработка на лични данни с автоматизирани средства, както и към обработката със средства, които не са автоматизирани, на лични данни, съставляващи част от файлова система или които са предназначени да съставляват част от файлова система.

2. Настоящата директива не се прилага за обработването на лични данни:

— при извършване на дейности, извън приложното поле на правото на Общността, например дейностите, предвидени в дял V и дял VI от Договора за Европейския съюз, и във всички случаи при дейности по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност (включително икономическото благосъстояние на държавата, когато процесът на обработка е свързан с държавната сигурност) и при дейности на държавата в областта на наказателното право;

[…]“

15. Глава II от Директива 95/46, която се отнася до „[о]бщи[те] правила относно законността на обработването на лични данни“, започва с член 5, съгласно който „държавите членки в границите на разпоредбите на настоящата глава определят по-точно условията, при които обработването на данни е законно“.

16. Съгласно член 6 от Директива 95/46:

„1. Държавите членки предвиждат, че личните данни трябва:

а) да се обработват справедливо и законно;

б) да се събират за конкретни, ясно формулирани и законни цели и да не бъдат допълнително обработени по начин, който е несъвместим с тези цели. Допълнителната обработка на данните за исторически, статистически или научни цели няма да се разглежда като несъвместима, при условие че държавите членки предоставят необходимите гаранции за това;

в) да бъдат адекватни, релевантни, и да не са прекомерни по отношение на целите, за които се събират и/или обработват допълнително;

г) да бъдат точни и при необходимост да се актуализират; трябва да се предприемат всички възможни разумни стъпки, за да се гарантира, че данни, които са неточни или непълни по отношение на целите, за които са събрани, или за които се обработват допълнително, се изтриват или поправят;

д) да се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително. Държавите членки предвиждат подходящи гаранции за личните данни, съхранявани за по-дълъг срок за исторически, статистически или научни цели.

2. Администраторът осигурява спазването на параграф 1“.

17. Съгласно член 7 от Директива 95/46:

„Държавите членки предвиждат, че обработването на лични данни може да се извършва, само ако:

а) съответното физическо лице е дало недвусмислено своето съгласие за това; или

б) обработването е необходимо за изпълнението на договор, по който съответното физическо лице е страна, или за да се предприемат стъпки по искане на съответното физическо лице преди сключването на договора; или

в) обработването е необходимо за спазването на правно задължение, чийто субект е администраторът; или

г) обработването е необходимо, за да бъдат защитени жизнено важни интереси на съответното физическо лице; или

д) обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес или при упражняване на официалните правомощия, които са предоставени на администратора или трето лице, на което се разкриват данните; или

е) обработването е необходимо за целите на законните интереси, преследвани от администратора или от трето лице или лица, на които се разкриват данните, с изключение на случаите, когато пред тези интереси имат преимущество интереси, свързани с основните права и свободи на съответното физическо лице, които изискват защита по силата на член 1, параграф 1“.

18. Член 13 от Директива 95/46 предвижда:

„1. 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, ако подобно ограничаване представлява необходима мярка за гарантиране на:

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

г) предотвратяването, разследването, разкриването и преследването на углавни престъпления или за нарушения на етичните кодекси при регламентираните професии;

д) важни икономически и финансови интереси на държавата членка или на Европейския съюз, включително валутни, бюджетни и данъчни въпроси;

е) функции по наблюдение, проверка или регламентиране, свързани, дори случайно, с упражняването на официални правомощия в случаите, посочени в букви в), г) и д);

ж) защита на съответното физическо лице или на правата и свободите на други лица.

[…]“.

Б – *Национално законодателство*

19. Член 12 от Telemediengesetz (Закон за електронните медии, наричан по-нататък „TMG“)[6] предвижда:

„1. Доставчикът на услуги може да събира и използва лични данни с цел предоставяне на достъп до електронни медии само доколкото този закон или друг нормативен акт, който изрично се отнася до електронните медии, разрешава това или ако ползвателят е дал своето съгласие.

2. Доставчикът на услуги може да използва за други цели събраните за предоставяне на достъп до електронни медии лични данни само доколкото този закон или друг нормативен акт, който изрично се отнася до електронните медии, допуска това или ако ползвателят е дал своето съгласие.

3. Съответните действащи разпоредби за защита на личните данни се прилагат и когато данните не се обработват автоматизирано, освен ако не е предвидено друго“.

20. Съгласно член 15 от TMG:

„(1) Доставчикът на услуги може да събира и използва лични данни на ползвател само доколкото е необходимо, за да се даде възможност за и за да се отчете ползването на електронни медии („данни за ползването“). „Данни за ползването“ са по-специално:

1. признаците за идентифициране на ползвателя,

2. данните за началото и края на съответното ползване, както и за неговия обхват и

3. данните за ползваните от ползвателя електронни медии.

(2) Доставчикът на услуги може да обедини данните за ползването на различни електронни медии от същия потребител, доколкото е необходимо за отчитането на сметките на ползвателя.

[…]

(4) Доставчикът на услуги може да използва данни за ползването след края на действието на ползване, доколкото данните са необходими за целите на отчитането на сметките на ползвателя („данни за отчитането“). Данните могат да бъдат блокирани от доставчика на услуги с цел изпълнение на съществуващи срокове за съхранение по силата на закон, устав или договор. […]“.

21. Съгласно член 3 от Bundesdatenschutzgesetz (Федерален закон за защита на данните, наричан по-нататък „BDSG“)[7] „лични данни са конкретни сведения за личното или фактическо положение на идентифицирано или на подлежащо на идентификация физическо лице („съответно физическо лице“). […]“.

II – **Факти**

22. Г-н Breyer е предявил иск срещу Федерална република Германия за прекратяване на действията по съхраняване на IP адреси.

6 — Закон от 26 февруари 2007 г. (BGBl. I, стр. 179).

7 — Закон от 20 декември 1990 г. (BGBI 1990 I, стр. 2954).

23. Редица федерални учреждения поддържат общодостъпни интернет портали, на които предоставят актуална информация. При повечето от тези портали всички влизания се регистрират в лог-файлове или регистри на протоколи с цел защита от атаки и осигуряване на възможност за наказателно преследване на лицата, извършващи атаките. В тези файлове се съхраняват, включително след края на съответното действие, наименованието на ползваните данни или ползвания сайт, въведените думи в полетата за търсене, времето на ползването, прехвърленото количество данни, съобщението дали ползването е било успешно и IP адресът на компютъра, от който същото е осъществено.

24. Г-н Breyer, който е ползвал различни подобни сайтове, иска Федералната република Германия да бъде осъдена да преустанови съхраняването, лично или чрез трети лица, на IP адреса на хост системата, от която той е осъществявал ползването, доколкото съхраняването не е необходимо за възстановяване на далекосъобщителната услуга в случай на смущения във функционирането.

25. Първоинстанционният съд отхвърля иска на г-н Breyer. Апелативната му жалба обаче е частично уважена, като Федералната република е осъдена да се въздържа от съхраняване след края на съответната операция за достъп. Наложеното въздържане е обусловено от това по време на ползването жалбоподателят да е посочил своите лични данни, включително под формата на имейл адрес, и от незадължителния характер на регистрацията за целите на възстановяване на достъпа до електронната медия.

III – **Преюдициалните въпроси**

26. След като и двете страни подават касационна жалба, шести състав на Bundesgerichtshof (Федерален върховен съд, Германия) отправя постъпилото в Съда на 17 декември 2014 г. преюдициално запитване със следните въпроси:

„1. Трябва ли член 2, буква а) от Директива 95/46/ЕО […] да се тълкува в смисъл, че адрес по интернет протокол (IP адрес), който се запазва от доставчик на услуги при влизане в неговия интернет сайт, представлява за него лични данни и когато трето лице (в случая — доставчикът на услугата за достъп) разполага с допълнителната информация, необходима за идентифицирането на съответното лице?

2. Допуска ли член 7, буква е) от Директивата за защита на данните разпоредба от националното право, съгласно която доставчикът на услуги може да събира и използва лични данни за ползвател без неговото съгласие само доколкото е необходимо, за да се даде възможност и да се отчете конкретното ползване на електронна медия от съответния ползвател, и съгласно която целта за осигуряване на общата функционална способност на електронната медия не може да оправдае използването на данните след края на съответното действие на ползване?“.

27. Запитващата юрисдикция посочва, че в съответствие с германското законодателство жалбоподателят би могъл да изисква въздържане от действията по съхраняване на IP адресите, ако това съхраняване представлява недопустимо посегателство върху неговото общо право на защита на личността съгласно нормативната уредба за защита на данни, по-конкретно на правото му на „информационно самоопределение“ (член 1004, параграф 1 и член 823, параграф 1 от Bürgerliches Gesetzbuch (германския граждански кодекс)] във връзка с членове 1 и 2 от Grundgesetz (германската конституция).

28. Такъв би бил случаят, ако: а) IP адресът (във всеки случай едновременно с датата на получаване на достъп до интернет сайт) може да бъде квалифициран като „лични данни“ по смисъла на член 2, буква а) във връзка със съображение 26, второ изречение от Директива 95/46 или съответно на член 12, параграфи 1 и 3 от TMG във връзка с член 3, параграф 1 от BDSG и б) ако не е налице нито едно от основанията за разрешаване по смисъла на член 7, буква е) от Директива 95/46 или съответно на член 12, параграфи 1 и 3 и член 15, параграфи 1 и 4 от TMG.

29. Според Bundesgerichtshof (Федерален върховен съд) за тълкуването на националното право (член 12, параграф 1 от TMG) от определящо значение е да се установи по какъв начин следва да се разбира личният характер на данните по смисъла на член 2, буква а) от Директива 95/46.

30. Запитващата юрисдикция посочва също, че съгласно член 15, параграф 1 от TMG доставчикът на услуги може да събира и използва лични данни на ползвател само доколкото е необходимо, за да се даде възможност за и за да се отчете ползването на електронни медии („данни за ползването“)[8], тълкуването на която разпоредба е тясно свързано с това на член 7, буква е) от Директива 95/46.

IV – **Производството пред Съда. Становища на страните**

31. Писмени становища са представили правителствата на Германия, Австрия и Португалия, както и Комисията. Само последната институция и г-н Breyer се явяват на проведеното на 25 февруари 2016 г. съдебно заседание, като германското правителство се е отказало да участие в същото.

А– *Становища на страните по първия въпрос*

32. Според г-н Breyer лични данни са включително тези, събирането на които е възможно само на теория, тоест изхождайки от наличието на една абстрактна, потенциална възможност, без значение дали на практика се осъществява това събиране. Според него обстоятелството, че конкретна организация може да е относително неспособна да идентифицира дадено лице чрез IP адрес, не означава, че това лице не е застрашено. Освен това според жалбоподателя от значение е обстоятелството, че Германия съхранява неговите IP данни с цел, при необходимост, да идентифицира евентуални атаки или да предприеме наказателно преследване, както член 113 от Telekommunikationsgesetz (Закон за телекомуникациите) допуска и както нееднократно се е случвало.

33. Германското правителство твърди, че на първия въпрос трябва да се отговори отрицателно. Според него динамичните IP адреси не разкриват „идентифицирано“ лице по смисъла на член 2, буква а) от Директива 95/46. За да се установи дали тези адреси предоставят данни за „подлежащо на идентификация“ лице по смисъла на същата разпоредба, проверката за „*възможност за идентификация*“ трябва да се извършва чрез прилагане на „относителен“ подход. Според германското правителство това следва от съображение 26 от Директива 95/46, според което трябва да се вземат предвид само средствата, които биха могли да бъдат използвани „разумно“ от администратора или от друго лице с цел идентифицирането на даденото лице. Това уточнение означавало, че законодателят на Съюза не е искал да включи в приложното поле на Директива 95/46 хипотезите, при които е обективно възможно идентификацията да бъде извършена от всяко трето лице.

8 — Според Bundesgerichtshof (Федерален върховен съд) данните за ползването са признаците за идентифициране на ползвателя, данните за началото и края на съответното ползване и неговия обхват, както и данните за ползваните от ползвателя електронни медии.

34. Германското правителство освен това счита, че понятието „лични данни“ по член 2, буква а) от Директива 95/46 трябва да се тълкува в съответствие с целта на тази директива, която е да се гарантира спазването на основните права. Необходимостта от защита на физическите лица би могла да се разглежда по различен начин в зависимост от това кой разполага с данните и дали има или не средствата да си послужи с тях, за да бъдат тези лица идентифицирани.

35. Германското правителство твърди, че г-н Breyer не може да бъде идентифициран чрез IP адресите съвместно с останалите данни, които доставчиците на съдържание съхраняват. За това е необходимо да се използва информацията, с която разполагат осигуряващите достъп до интернет, които при отсъствието на законово основание нямат право да я предоставят на доставчиците на съдържание.

36. Австрийското правителство от своя страна счита, че отговорът трябва да бъде утвърдителен. В съответствие със съображение 26 от Директива 95/46, за да бъде дадено лице подлежащо на идентификация, не се изисква всички негови идентификационни данни да се намират в ръцете само на една организация. Така IP адресът би могъл да представлява лични данни, ако трето лице (например осигуряващият достъп до интернет) разполага със средствата за идентифициране на титуляря на този адрес, без да полага прекомерни усилия.

37. Португалското правителство също смята, че следва да се даде утвърдителен отговор, като приема, че IP адресът съвместно с датата на ползване представлява лични данни, доколкото може да доведе до идентифициране на ползвателя от организация, различна от тази, съхранила IP адреса.

38. Комисията също предлага да се даде утвърдителен отговор, като се позовава на решение Scarlet Extended[9]. Комисията счита, че доколкото съхраняването на IP адресите служи именно за идентификация на ползвателите в случай на кибератаки, използването на допълнителните данни, които регистрират осигуряващите достъп до интернет, представлява средство, което може да бъде „разумно“ използвано по смисъла на съображение 26 от Директива 95/46. В крайна сметка според Комисията, както преследваната с посочената директива цел, така и членове 7 и 8 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“) предполагат широко тълкуване на член 2, буква а) от Директива 95/46.

Б– *Становища на страните по втория въпрос*

39. Г-н Breyer счита, че член 7, буква е) от Директива 95/46 представлява общо правило, чието практическо приложение налага уточнение. Според практиката на Съда това означавало да се обсъдят обстоятелствата в конкретния случай и да се прецени дали има лица със законен интерес по смисъла на посочената разпоредба, като за целите на приложението ѝ е не само допустимо, но и абсолютно необходимо да бъдат предвидени особени правила по отношение на тези лица. В конкретния случай, според г-н Breyer, националните разпоредби са съвместими с член 7, буква е) от Директива 95/46, доколкото обществеият портал няма интерес от съхраняването на лични данни или защото интересът от закрила на анонимността има по-голяма тежест. Според него системното съхраняване на лични данни е несъвместимо с демократичното общество, нито е необходимо и пропорционално с оглед гарантиране на функционалната способност на електронните медии, което е напълно възможно без регистрирането на тези лични данни, както се установявало от интернет сайтовете на някои федерални министерства.

9 — Решение от 24 ноември 2011 г. (C-70/10, EU:C:2011:771, т. 51).

40. Германското правителство твърди, че вторият въпрос не следва да се обсъжда, доколкото същият е отправен единствено в случай че на първия бъде даден утвърдителен отговор, какъвто според него, поради изложените по-горе съображения, той не следва да получи.

41. Австрийското правителство предлага да се отговори в смисъл, че Директива 95/46 по принцип допуска съхраняването на данни като разглежданите в главното производство, когато това е крайно необходимо, за да се гарантира функционалната способност на електронните медии. Според посоченото правителство ограничено съхраняване на IP адреса отвъд времето, през което се ползва даден интернет сайт, може да бъде законно с оглед задължението на администратора на лични данни да прилага мерките за защита на тези данни, установено в член 17, параграф 1 от Директива 95/46. Борбата срещу кибератаки би могла да оправдае проверката на данните за предходни атаки и ограничаването на достъпа до интернет сайта на някои IP адреси. Пропорционалността на съхраняването на данни като разглежданите в главното производство от гледна точка на целта за гарантиране на функционалната способност на електронните медии би трябвало да се преценява във всеки отделен случай, при отчитане на принципите, залегнали в член 6, параграф 1 от Директива 95/46.

42. Според португалското правителство член 7, буква е) от Директива 95/46 допуска национално законодателство като разглежданото в главното производство, тъй като германският законодател вече е извършил предвиденото в посочената разпоредба претегляне на законните интереси на администратора на лични данни, от една страна, и на правата и свободите на лицата, за които тези данни се отнасят, от друга страна.

43. Комисията счита, че националното законодателство, което транспонира член 7, буква е) от Директива 95/46, трябва да определи целите на обработването на лични данни по начин, че същите да могат да бъдат предвидими за съответното засегнато лице. Според нея германското законодателство не спазва това изискване, предвиждайки в член 15, параграф 1 от TMG, че съхраняването на IP адресите се допуска, „доколкото е необходимо, за да се даде възможност за […] ползването на електронни медии“.

44. Ето защо Комисията предлага на втория въпрос да бъде отговорено в смисъл, че разглежданата разпоредба не допуска тълкуване на национална норма, според която публичен орган, който действа като доставчик на услуги, може да презаписва и използва личните данни на ползвател без неговото съгласие, включително когато преследваната цел е да се гарантира общата функционална способност на електронната медия, ако въпросната национална норма не установява посочената цел по достатъчно ясен и точен начин.

V – **Анализ**

A– *По първия въпрос*

1. Уточняване на отправения въпрос

45. Съгласно формулировката на Bundesgerichtshof (Федерален върховен съд) с първия от въпросите си запитващата юрисдикция иска да установи дали IP адрес, с който се осъществява достъп до даден интернет сайт, представлява за публичния орган, който е притежател на тази интернет сайт, лични данни (по смисъла на член 2, буква а) от Директива 95/46) в случаите, когато осигуряващият достъп до мрежата разполага с допълнителни данни, позволяващи идентификацията на заинтересованото лице.

46. Така формулиран въпросът е достатъчно конкретен, за да не допусне изначално възникването на други, абстрактни въпроси относно правната природа на IP адресите в контекста на защитата на личните данни.

47. На първо място, Bundesgerichtshof (Федерален върховен съд) се позовава изключително на „динамичните IP адреси“ или на тези, които се предоставят временно за всяко свързване с мрежата и се променят при последващи свързвания. Следователно въпросът не се отнася до „фиксираните или статичните IP адреси“, които не се променят и позволяват свързаното с мрежата устройство винаги да бъде идентифицирано.

48. На второ място, запитващата юрисдикция изхожда от презумпцията, че осигуряващият достъп до интернет сайта в главното производство не е в състояние да идентифицира посредством динамичния IP адрес лицата, които го посещават, нито разполага с допълнителни данни, които съвместно с този IP адрес позволяват тяхната идентификация. Изглежда, че в този контекст според Bundesgerichtshof (Федерален върховен съд) динамичният IP адрес не представлява лични данни по смисъла на член 2, буква а) от Директива 95/46 *за осигуряващия достъп до интернет сайта*.

49. Съмнението на запитващата юрисдикция е свързано с възможността динамичният IP адрес да бъде квалифициран като лични данни за осигуряващия достъп до интернет сайта, *ако трето лице има на разположение допълнителни данни*, които съвместно с този адрес позволяват идентификацията на посетителите на интернет сайтовете му. Bundesgerichtshof (Федерален върховен съд) обаче — и това е съществено уточнение — няма предвид всяко трето лице, което разполага с допълнителните данни, а единствено осигуряващият достъп до мрежата (следователно изключва други лица, които евентуално имат на разположение такива данни).

50. Така извън предмета на спора остават, наред с други, и следните въпроси: а) дали статичните IP адреси са лични данни по смисъла на Директива 95/46[10]; б) дали динамичните IP адреси винаги и при всякакви обстоятелства представляват лични данни по смисъла на посочената директива и на последно място, в дали квалифицирането на динамичните IP адреси като лични данни е неизбежно, ако съществува трето лице, независимо кое е то, което може да ги използва за идентификацията на ползвателите на мрежата.

51. Следователно става въпрос само за това да се прецени дали динамичният IP адрес представлява лични данни за доставчика на интернет услуга, когато съобщителната компания, която предлага достъпа до мрежата (осигуряващият достъп), разполага с допълнителни данни, които съвместно с този адрес позволяват идентифицирането на лицето, което посещава интернет сайта, администриран от първия доставчик.

10 — Въпрос, по който Съдът се е произнесъл в решение от 24 ноември 2011 г., Scarlet Extended (C-70/10, EU:C:2011:771, т. 51) и в решение от 19 април 2012 г., Bonnier Audio и др. (C-461/10, EU:C:2012:219). В точки 51 и 52 от последното решение Съдът постановява, че съобщаването на „името и адрес[а] на […] интернет потребителя, използвал IP адреса, от който е бил извършен твърдяният незаконосъобразен обмен на файлове, съдържащи защитени произведения, с оглед на идентифицирането му […] представлява обработване на лични данни по смисъла на член 2, първа алинея от Директива 2002/58 във връзка с член 2, буква б) от Директива 95/46“.

2. По същество

52. Повдигнатият с настоящото преюдициално запитване въпрос е предмет на засилен дебат в германската доктрина и германската съдебна практика, вижданията по който са разделени на две [11]. Съгласно едното от тях (което се основава на „обективен“ или „абсолютен“ подход) даден ползвател подлежи на идентифициране и следователно IP адресът представлява лични данни, които са обект на защита, когато, независимо от способностите и средствата на доставчика на интернет услуга, неговото идентифициране е възможно с простото свързване на този динамичен IP адрес с данните, предоставени от трето лице (например осигуряващият достъп до мрежата).

53. Според последователите на другото виждане (защитаващи „относителен“ подход) възможността ползвателят да бъде напълно идентифициран с помощта на трето лице не е достатъчна, за да се придаде на динамичния IP адрес качеството на лични данни. От значение е способността на лицето със собствени средства да си послужи с данните, до които има достъп, и по този начин да идентифицира дадено лице.

54. В каквото и да се състои този спор в националното право, отговорът на Съда трябва да се ограничи до тълкуването на двете разпоредби от Директива 95/46, посочени както от запитващата юрисдикция, така и от страните в производството, тоест на член 2, буква а) [12] и съображение 26 [13] от същата директива.

55. Само поради факта, че предоставят информация за датата и часа на осъществяване на достъп до даден интернет сайт от компютър (или друго устройство), динамичните IP адреси разкриват някои особености от поведението на интернет потребителите и следователно предполагат евентуално нарушение на правото им на личен живот [14], прогласено в член 8 от Европейската конвенция за защита на правата на човека и основните свободи и в член 7 от Хартата, в светлината на която, както и на член 8 от същата, трябва да се тълкува Директива 95/46 [15]. Всъщност страните по делото не оспорват това обстоятелство, което само по себе си не е предмет и на преюдициалния въпрос.

56. Лицето, за което се отнасят посочените детайли, не е „подлежащо на идентификация физическо лице“. Датата и часът на свързването, както и неговият цифров източник, не разкриват нито пряко, нито непряко, кое е физическото лице, притежаващо устройството, от което е посетен интернет сайтът, както и идентичността на ползвателя, който го използва (това може да бъде всяко физическо лице).

11 — Относно двете доктринални становища вж. например *Schreibauer*, M. — In: Kommentar zum Bundesdatenschutzgesetz. Nebengesetze, Esser, M., Kramer, P. et Von Lewinski, K. (eds.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. ed., § 11 Telemediengesetz (4—10). *Nink*, J. et *Pohle*, J. Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze. — Multimedia und Recht, 9/2015, p. 563—567. *Heidrich*, J. et *Wegener*, C. Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging. — Multimedia und Recht, 8/2015, p. 487—492. *Leisterer*, H. Die neuen Pflichten zur Netz — und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr. — Computer und Recht, 10/2015, p. 665—670.

12 — Възпроизведен в точка 13 по-горе.

13 — Възпроизведено в точка 11 по-горе.

14 — Това припомня генералният адвокат Cruz Villalón в заключението си по дело Scarlet Extended (C-70/10, EU:C:2011:255, т. 76), като в същия смисъл е и разбирането на Европейския надзорен орган по защита на данните, изложено в становище от 22 февруари 2010 г. относно текущите преговори, водени от Европейския съюз за Търговско споразумение за борба с фалшифицирането (ACTA) (ОВ C 147, 2010 г., стр. 1, точка 24), както и в становище от 10 май 2010 г. относно предложението за Директива на Европейския парламент и на Съвета относно борбата със сексуалното малтретиране, сексуалната експлоатация на деца и детската порнография и за отмяна на Рамково решение 2004/68/ПВР (ОВ C 323, 2010 г., стр. 6, точка 11).

15 — Вж. в този смисъл решение от 23 май 2003 г., Österreichischer Rundfunk (C-465/00, C-138/01 и C-139/01, EU:C:2003:294, т. 68), както и заключението на генералния адвокат Kokott по дело Promusicae (C-275/06, EU:C:2007:454, т. 51 и сл.).

57. Въпреки това, доколкото даден динамичен IP адрес спомага да се определи — било сам по себе си, било чрез свързването му с други данни — кой е притежателят на устройството, използвано за достъп до интернет сайта, този адрес може да се квалифицира като информация относно „подлежащо на идентификация лице“ [16].

58. Според изложеното от Bundesgerichtshof (Федерален върховен съд) динамичният IP адрес сам по себе си не е достатъчен, за да се идентифицира ползвателят, който чрез него е имал достъп до определен интернет сайт. Обратно, ако доставчикът на интернет услуга би могъл посредством динамичния IP адрес да идентифицира ползвателя, в такъв случай адресът несъмнено ще представлява лични данни по смисъла на Директива 95/46. Не изглежда обаче това да е смисълът на преюдициалния въпрос, в който се подчертава, че доставчиците на интернет услуги, които са страни по главното производство, не могат да идентифицират ползвателя само посредством динамичния IP адрес.

59. Съвместно с други данни динамичният IP адрес позволява ползвателят да бъде идентифициран „непряко“ — обстоятелство, с което всички са съгласни. Допуска ли възможността от съществуването на допълнителни данни, които могат да бъдат свързани с динамичния IP адрес, последният да бъде определен като лични данни по смисъла на Директивата? Следва да се прецени дали за целта е достатъчна само абстрактната възможност тези данни да бъдат узнати, или напротив — същите трябва да са на разположение на лицето, което вече познава динамичния IP адрес, или на трето лице.

60. Страните са съсредоточили становищата си върху тълкуването на съображение 26 от Директива 95/46, като извеждат от съдържанието му израза „средства, които биха могли да бъдат използвани разумно от администратора или от друго лице с цел идентифицирането на даденото лице“. Въпросът на запитващата юрисдикция не се отнася до допълнителни данни на разположение на доставчиците на услуги, участващи в главното производство. Не става въпрос и за всяко трето лице, което разполага с тези допълнителни данни (чието свързване с динамичния IP адрес позволява идентифициране на ползвателя), а за осигуряващия достъп до мрежата.

61. Следователно в настоящия случай не е нужно Съдът да преценява всички средства, които ответникът в главното производство би могъл „разумно“ да използва, за да могат динамичните IP адреси, с които същият разполага, да бъдат квалифицирани като лични данни. Доколкото Bundesgerichtshof (Федерален върховен съд) се позовава само на допълнителни данни, които са на разположение на трети лица, би могло да се направи изводът: а) или че ответникът не разполага с допълнителни данни, позволяващи идентификацията на ползвателя, б) или че дори да има достъп до такива данни като администратор, не може да ги използва разумно за тази цел по смисъла на съображение 26 от Директива 95/46.

62. И двете хипотези зависят от преценка на фактите, която е в правомощията само на запитващата юрисдикция. Съдът би могъл да предостави на последната единствено критерии от общ характер, посредством които да се даде тълкуване на израза „средства, които биха могли да бъдат използвани разумно от администратора“, само ако Bundesgerichtshof (Федерален

16 — Може да се предположи, освен при наличие на доказателства за противното, че това е лицето, което е използвало интернет и е посетило съответния интернет сайт. Въпреки това, дори да се игнорира тази презумпция, информацията относно датата, часа и цифровия източник на достъпа до даден интернет сайт позволява този достъп да бъде свързан с притежателя на устройството и същият да бъде индиректно асоцииран с модела на поведението му в мрежата. Възможното изключение биха били IP адресите, предоставяни на компютри в заведения от типа *интернет кафе*, чиито анонимни ползватели представляват неподлежащи на идентификация лица, а осъщественият трафик не предоставя никаква съществена информация, имаща характера на лични данни, за собствениците на тези заведения. Това обаче е единственото изключение от правилото, че IP адресите представляват лични данни, прието от работната група за защита на лицата при обработването на лични данни, създадена с Директива 95/46 (така наречената „работна група по член 29“). Вж. нейно Становище 4/2007 от 20 юни 2007 г. относно понятието „лични данни“, WP136, достъпно на адрес http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

върховен съд) имаше някакви съмнения относно способността на ответника разумно да си служи със съответните допълнителни данни. Доколкото това не е така, според мен в случая Съдът не следва да определя тълкувателни критерии, които не са от съществено значение за запитващата юрисдикция, нито са поискани от нея.

63. Ето защо същността на отправения въпрос се състои в това да се прецени дали за квалифицирането на динамичните IP адреси като лични данни е от значение обстоятелството, че едно конкретно трето лице, а именно осигуряващият достъп до интернет, разполага с допълнителни данни, които съвместно с тези адреси могат да послужат за идентифициране на ползвателя, посетил определен интернет сайт.

64. Отново се налага да се разгледа съображение 26 от Директива 95/46. Изразът „средства, които биха могли да бъдат използвани [...] *от друго лице*“ [17], би могъл да доведе до тълкуване, според което е достатъчно трето лице да може да се снабди с допълнителни данни (които съвместно с динамичния IP адрес биха могли да послужат за целите на идентифициране на дадено лице), за да се приеме, че този адрес представлява eo ipso лични данни.

65. Подобно максималистично тълкуване на практика би довело до това всеки вид информация, колкото и недостатъчна да е сама по себе си за идентифицирането на даден ползвател, да се счита за лични данни. Никога не би било възможно да се отхвърли с абсолютна сигурност възможността от съществуването на трето лице, разполагащо с допълнителни данни, които съвместно с подобна информация, да доведат в резултат на това до разкриване на идентичността на дадено лице.

66. Според мен възможността напредъкът на техническите средства в едно по-далечно или по-близко бъдеще да открие пътя за достъп до инструменти за получаване и обработване на информация, които стават все по-сложни, оправдава загрижеността от поставяне на закрилата на правото на личен живот на преден план. Направен е опит при определянето на съответните правни категории в сферата на защита на данните да бъдат включени достатъчно обширни и гъвкави хипотези на поведение, за да се обхване всеки случай, които би могъл да възникне [18].

67. Считам обаче, че тази загриженост — между впрочем напълно легитимна — не може да бъде основание да се игнорира изразената волята на законодателя, както и че систематичното тълкуване на съображение 26 от Директива 95/46 трябва да бъде сведено до „средства, които биха могли да бъдат използвани разумно“ от *определени трети лица*.

68. Така както съображение 26 не се отнася до всякакви средства на разположение на администратора на лични данни (в случая доставчикът на интернет услуги), а само до тези, които същият би могъл да използва „разумно“, по същия начин следва да се приеме, че законодателят има предвид „други лица“, към които, *отново разумно*, може да се обърне администраторът на лични данни, търсещ да му бъдат предоставени допълнителните данни за целите на идентификацията. Не би бил такъв случаят, когато контактът с другите лица на практика е много скъп по отношение на човешки и финансови ресурси или пък е фактически неизпълним или забранен от закона. В противен случай, както предупредих по-горе, би било практически невъзможно да се направи разграничение между едните и другите средства, тъй като винаги би могла да възникне хипотеза за съществуването на трето лице, което, колкото и недостъпно да е за доставчика на интернет услуги, би могло да разполага — в момента или в бъдеще — с допълнителни данни, които да спомогнат за идентифицирането на даден ползвател.

17 — Курсивът е мой.

18 — Тази предпазна и превантивна функция е в основата на становището, защитавано от работната група по член 29, според което, както посочих, следва да се изхожда от принципа, че IP адресите са лични данни, приемайки като единствено изключение случаите, в които доставчикът на услугата е в състояние да определи с абсолютна сигурност, че става въпрос за адреси, съответстващи на лица, неподлежащи на идентифициране, каквито са ползвателите на интернет кафе. Вж. бележка под линия 16 по-горе.

69. Както вече посочих, третото лице, което Bundesgerichtshof (Федерален върховен съд) има предвид, е осигуряващият достъп до мрежата. Това със сигурност е третото лице, към което е най-разумно да се приеме, че ще се обърне доставчикът на услуги, за да се снабди с конкретните допълнителни данни, ако иска да идентифицира по най-ефективен, правилен и непосредствен начин ползвателя, осъществил достъп до неговия интернет сайт благодарение на динамичния IP адрес. По никакъв начин не става въпрос за хипотетично трето лице, което е непознато и недостъпно, а за главно действащо лице в интернет, за който със сигурност е известно, че разполага с търсените от доставчика на услуги данни за идентифициране на даден ползвател. На практика, според изложеното от запитващата юрисдикция, именно към това конкретно трето лице има намерение да се обърне ответникът в главното производство, за да се снабди с допълнителните данни, които са му необходими.

70. Осигуряващият достъп до интернет е типичното друго лице, за което се отнася съображение 26 от Директива 95/46, към което съвсем „разумно“ може да се обърне доставчикът на услуги в главното производство. Остава обаче да се разреши въпросът дали получаването на допълнителните данни, с които това трето лице разполага, може да се квалифицира като „разумно“ изпълнимо или реализуемо.

71. Германското правителство твърди, че тъй като информацията, с която разполага осигуряващият достъп до интернет, представлява лични данни, същият не може да я предоставя просто така, а само в съответствие с нормативната уредба за обработването на тези данни [19].

72. Това несъмнено е вярно, тъй като, за да може тази информация да бъде използвана, трябва да се спазва приложимото законодателство относно личните данни. Дадена информация може да бъде „разумно“ получена само ако се спазват условията, регламентиращи достъпа до този вид данни, първото от които е предвидената от закона възможност за тяхното съхраняване и предоставяне на други лица. Действително осигуряващият достъп до интернет има право да откаже предоставянето на поисканите данни, но е възможно и обратното. Възможността за предоставяне на данни, която е напълно „разумна“, превръща сама по себе си динамичния IP адрес в лични данни за доставчика на интернет услуги съгласно съображение 26 от Директива 95/46.

73. Става въпрос за осъществима *в рамките на закона* и следователно „разумна“ възможност. Разумните средства за достъп, които се имат предвид в Директива 95/46, по правило трябва да бъдат законни средства [20]. Както припомня германското правителство [21], запитващата юрисдикция изхожда, разбира се, от тази предпоставка. Така способите за достъп от правна гледна точка значително намаляват, тъй като същите трябва да бъдат изключително законосъобразни. Докато обаче тези способи съществуват, колкото и ограничено да е тяхното приложение на практика, те представляват „разумно средство“ по смисъла на Директива 95/46.

74. Ето защо считам, че както е формулиран, първият от въпросите на Bundesgerichtshof (Федерален върховен съд), следва да получи утвърдителен отговор. Динамичният IP адрес трябва да се квалифицира като лични данни за доставчика на интернет услуги, тъй като съществува трето лице (осигуряващият достъп до мрежата), към което той може да се обърне разумно, за да се снабди с други допълнителни данни, които заедно с този адрес позволяват идентифицирането на даден ползвател.

19 — Точки 40 и 45 от писменото му становище.

20 — В този смисъл е без значение обстоятелството, че достъпът до лични данни на практика може да бъде осъществен чрез нарушаване на законите за защита на данни.

21 — Точки 47 и 48 от писменото му становище.

75. Считам, че резултатът, до който би довело обратно на предлаганото от мен разрешение, е в негова подкрепа. Ако динамичните IP адреси не представляваха лични данни за доставчика на интернет услуги, той би могъл да ги съхранява за неограничен срок, като във всеки един момент би могъл да поиска от осигуряващия достъп до интернет допълнителните данни, за да ги свърже с тези адреси и да идентифицира ползвателя. При това положение, както германското правителство признава[22], в момента, в който допълнителните данни, позволяващи идентификацията на ползвателя, вече са на разположение, динамичният IP адрес ще придобие характера на лични данни, като приложимо в случая ще бъде законодателството за защита на данните.

76. Става въпрос обаче за данни, съхраняването на които ще е възможно, доколкото същите до момента не са приемани като лични данни за доставчика на услуги. По този начин правната квалификация на динамичния IP адрес като лични данни ще зависи от този доставчик и същата ще бъде обусловена от възможността в един бъдещ момент той да реши да използва този адрес, за да идентифицира ползвателя съвместно с допълнителните данни, с които трябва да се снабди от трето лице. Според мен обаче от определящо значение съгласно Директива 95/46 е възможността, която е разумна, да съществува „достъпно“ трето лице, разполагащо с необходимите средства, които да позволят идентифицирането на дадено лице, а не осъществяването на възможността това трето лице да бъде потърсено.

77. Би могло да се приеме, както твърди германското правителство, че динамичният IP адрес се превръща в лични данни в момента, в който бъде получен от осигуряващия достъп до интернет. Тогава обаче би трябвало да се приеме, че квалифицирането му като лични данни се извършва с обратна сила в рамките на срока за съхраняване на IP адреса и следователно да се приеме за отпаднало, ако срокът, през който може да бъде съхранен, при положение че още в самото начало този адрес е бил квалифициран като лични данни, е изтекъл. В такъв случай би се стигнало до резултат, който противоречи на духа на законодателството за защита на личните данни. Причината, обосноваваща съхраняването на тези данни само за определено време, ще бъде опорочена при евентуално забавяне да се отчете присъщият им още от самото начало характер: възможността да служат като средство за идентификация — самостоятелно или заедно с други данни — на дадено физическо лице. По същата причина, от съображения за икономия, е по-разумно това им качество да бъде признато още в началото.

78. Ето защо като първо заключение считам, че член 2, буква а) от Директива 95/46 трябва да се тълкува в смисъл, че IP адрес, съхранен от доставчик на услуги във връзка с достъп до неговия интернет сайт, представлява за този доставчик лични данни, доколкото лице, осигуряващо достъп до мрежата (интернет), разполага с допълнителни данни, позволяващи заинтересованото лице да бъде идентифицирано.

Б– *По втория преюдициален въпрос*

79. С втория преюдициален въпрос Bundesgerichtshof (Федерален върховен съд) иска да установи дали член 7, буква е) от Директива 95/46 допуска национална уредба, която позволява събирането и използването на личните данни на ползвател само доколкото е необходимо, за да се даде възможност и да се отчете конкретното ползване на дадена електронна медия от този ползвател, като целта за осигуряване на общата функционална способност на електронната медия не може да оправдае използването на данните след края на съответното действие на ползване.

22 — Точка 36 от писменото му становище.

80. Отговорът на този въпрос се нуждае от уточняване на предоставената от Bundesgerichtshof (Федерален върховен съд) информация, съгласно която спорните данни се съхраняват с цел да се гарантира функционалната способност на засегнатите в главното производство интернет сайтове, предоставяйки възможност, при необходимост, за наказателно преследване на кибератаките, на които евентуално биха били подложени.

81. Така преди всичко трябва да се прецени дали обработването на IP адресите, за което става въпрос в акта за преюдициално запитване, попада в обхвата на изключението, предвидено в член 3, параграф 2, първо тире от Директива 95/46 [23].

1. Относно приложимостта на Директива 95/46 към обработването на спорните данни

82. По всичко изглежда, че в спора по главното производство Федерална република Германия действа като обикновен доставчик на интернет услуги, тоест като частноправен субект (и следователно sine imperio). От това поначало следва, че обработването на данните, предмет на настоящото производство, не е изключено от обхвата на приложение на Директива 95/46.

83. Както Съдът посочва в решение Lindqvist [24], дейностите по член 3, параграф 2 от Директива 95/46 „във всички случаи са присъщи на държавите или на държавните органи дейности, които са извън областите на дейност на частноправните субекти“ [25]. Директива 95/46 е приложима, доколкото администраторът на спорните данни, независимо от качеството си на публичноправен орган, на практика действа като частноправен субект.

84. При изложението на основната цел, преследвана от германската администрация с регистрирането на динамичните IP адреси, запитващата юрисдикция подчертава, че същото е необходимо за „осигуряване и поддържане на сигурността и достъпа до нейните електронни медии“; по-конкретно то има за цел „откриването и отбиването на често срещаните атаки от вида „Denial-of-Service“, при които телекомуникационната инфраструктура се парализира чрез целенасочено и координирано претоварване на определени сървъри с голям брой запитвания“ [26]. Съхраняването на динамичните IP адреси с тази цел е обичайна практика на всички притежатели на уебсайтове от особена важност, без да включва нито пряко, нито косвено упражняването на властнически правомощия, поради което включването му в обхвата на приложение на Директива 95/46 не разкрива особени затруднения.

85. Bundesgerichtshof (Федерален върховен съд) обаче посочва, че съхраняването на динамичните IP адреси от доставчиците на услуги, участващи в главното производство, има за цел също така предприемането на наказателно преследване, в случай на необходимост, срещу евентуалните извършители на кибератаки. Достатъчна ли е тази цел, за да бъде обработването на посочените данни изключено от приложното поле на Директива 95/46?

86. Според мен, ако под „наказателно преследване“ се разбира упражняването на ius puniendi на държавата от страна на доставчиците на услуги — ответници в главното производство, ще бъдем изправени пред „дейности на държавата в областта на наказателното право“ и следователно — пред едно от изключенията, предвидени в член 3, параграф 2, първо тире от Директива 95/46.

23 — Директива 95/46 не се прилага „при дейности по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност […] и *при дейности на държавата в областта на наказателното право*“ (курсивът е мой).

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

25 — Пак в този смисъл, решение от 16 декември 2008 г., Satakunnan Markkinapörssi и Satamedia (C-73/07, EU:C:2008:727, т. 41).

26 — Точка 36 от акта за преюдициално запитване.

87. В този случай съгласно практиката на Съда, установена с решение Huber[27], обработването на личните данни от доставчиците на услуги с цел да се гарантира сигурността и техническата функционалност на техните електронни медии ще попадне в обхвата на приложение на Директива 95/46, докато обработването на данни, свързано с дейността на държавата в областта на наказателното право, ще бъде извън този обхват.

88. По същия начин, дори когато самото наказателно преследване не е в правомощията на Федерална република Германия в качеството ѝ на обикновен доставчик на услуги без властнически правомощия, а като всеки друг частноправен субект тя се ограничава само до това да предостави спорните IP адреси на съответния държавен орган за предприемане на репресивни мерки, обработването на динамичните IP адреси отново ще представлява дейност, която е изключена от обхвата на приложение на Директива 95/46.

89. Това се установява от съдебната практиката, установена с решение Парламент/Съвет и Комисия[28], в което Съдът постановява, че обстоятелството, че определени лични данни „се събират от частни оператори с търговски цели и тези оператори организират прехвърлянето им към трета държава“, не означава, че това прехвърляне „не попада в обхвата на приложение“ на член 3, параграф 2, първо тире от Директива 95/46, ако неговата цел е осъществяването на дейности на държавата в областта на наказателното право и при положение че същото „попада в рамки, установени от публичните органи и е свързано със защитата на държавната сигурност“[29].

90. Обратно, ако, както смятам, под „наказателно преследване“ следва да се разбира, до какъвто извод може да се достигне от акта за преюдициално запитване, правото на всеки частноправен субект в качеството му на легитимирано лице да поиска упражняването на ius puniendi от страна на държавата посредством съответните действия, не може да се твърди, че обработването на динамичните IP адреси има за предмет дейността на държавата в областта на наказателното право, която е изключена от приложното поле на Директива 95/46.

91. На практика съхраняването и регистрирането на тези данни ще послужат като допълнително доказателствено средство, с което притежателят на интернет сайта може да сезира държавата с искане за наказателно преследване срещу незаконно поведение. В крайна сметка става въпрос за средство за защита по наказателноправен ред на признати от правовия ред права на частноправен субект (в случая на публичен орган, чиито права и задължения се уреждат от частното право). От тази гледна точка става въпрос за същото действие като извършеното от всеки друг доставчик на интернет услуги, който търси закрилата на държавата в съответствие с нормативно установените процедури за упражняване на наказателно преследване.

92. Следователно, доколкото германската администрация действа като доставчик на интернет услуги, лишен от властнически правомощия — обстоятелство, което трябва да бъде преценено от запитващата юрисдикция — извършваното от нея обработване на динамичните IP адреси, имащи характера на лични данни, попада в обхвата на приложение на Директива 95/46.

2. По същество

93. Член 15, параграф 1 от TMG допуска събирането и използването на лични данни на ползвател само доколкото е необходимо, за да се даде възможност за и да се отчете конкретното ползване на електронните медии. По-конкретно, доставчикът на услуги може да събира и използва единствено така наречените „данни за ползването“, тоест личните данни на

27 — Решение от 16 декември 2008 (C-524/06, EU:C:2008:725, т. 45).

28 — Решение от 30 май 2006 г. (C-317/04 и C-318/04, EU:C:2006:346, т. 54—59).

29 — Пак там, т. 59. В случая става въпрос за лични данни, обработването на които не е необходимо за целите на предоставянето на услуги, които съставляват осъществяваната от частноправните оператори (авиокомпании) дейност, които данни обаче последните са били задължени да предоставят на северноамериканските власти за целите на предотвратяване и борба с тероризма.

даден ползвател, необходими, за да „се даде възможност за и да се отчете ползването на електронните медии“. Тези данни трябва да бъдат заличени след края на операцията (тоест когато бъде преустановено конкретното ползване на електронната медия), освен ако тяхното съхраняване не е необходимо „за целите на отчитането“, както предвижда параграф 4 от посочения член 15 от TMG.

94. Изглежда, че член 15 от TMG изключва възможността данните за ползването да бъдат съхранявани след преустановяване на връзката на други основания, включително с цел да се гарантира „ползването на електронните медии“ като цяло. Предвиждайки като основание за съхраняването на данните само целите на отчитане, посочената разпоредба от TMG би могла да се разбира (макар запитващата юрисдикция да е тази, която трябва да даде окончателно тълкуване на същата) в смисъл, че изисква данните за ползването да се използват само за да се осигури конкретно ползване, след което те трябва да бъдат заличени.

95. Член 7, буква е) от Директива 95/46 [30] позволява обработването на личните данни по начин, който бих квалифицирал като по-щедър (за администратора на лични данни), отколкото предвидения в текста на член 15 от TMG. Германската разпоредба може да се приеме в това отношение за по-ограничителна от разпоредбата на Съюза, тъй като поначало не предвижда възможност за удовлетворяване на друг законен интерес, който не е свързан с отчитане на ползването, независимо че, действайки в качеството си на доставчик на интернет услуги, Федерална република Германия може да има също така законен интерес да гарантира функционалната способност на своите интернет сайтове отвъд всяко конкретно тяхно ползване [31].

96. Практиката на Съда, установена с решение ASNEF и FECEMD [32], предоставя критериите, необходими, за да се отговори на втория преюдициален въпрос. В това решение Съдът постановява, че от преследваната от Директива 95/46 цел „следва, че член 7 от Директива 95/46 съдържа изчерпателен списък на случаите, в които обработването на лични данни може да се счита за законно“ [33]. От това може да се направи извод, че „държавите членки не могат нито да добавят нови критерии за законност на обработването на лични данни към член 7 от Директива 95/46, нито да предвиждат допълнителни изисквания, които изменят обхвата на някой от посочените в този член шест критерия“ [34].

97. Член 15 от TMG не предвижда допълнително изискване към предвидените в член 7 от Директива 95/46 относно законността на обработването на данните — какъвто е случаят по делата ASNEF и FECEMD [35]— но при посоченото от запитващата юрисдикция стриктно тълкуване на въпросната разпоредба същата ограничава съдържанието на условието, съдържащо се в буква е) на член 7; докато законодателят на Съюза е предвидил като общо правило „[…] целите на законните интереси, преследвани от администратора или от трето лице или лица, на които се разкриват данните“, член 15 от TMG отчита единствено необходимостта „да се даде възможност за и за да се отчете ползването на електронните медии“.

30 — Възпроизведен в точка 17 по-горе.

31 — Вж. точка 85 по-горе. В действителност притежателите на интернет сайтове имат законен интерес да предотвратяват и отбиват споменатите от запитващата юрисдикция ограничения на услугата („denials of service“), тоест масирани атаки, които понякога се осъществяват целенасочено срещу определени интернет сайтове с цел тяхното претоварване и блокиране.

32 — Решение от 24 ноември 2011 г. (C-468/10 и C-469/10, EU:C:2011:777).

33 — Пак там, т. 30.

34 — Решение ASNEF и FECEMD (C-468/10 и C-469/10, EU:C:2011:777, т. 32).

35 — В този случай националното законодателство добавя към изискванията на член 7, буква е) от Директива 95/46 обработваните данни да се съдържат в общодостъпни източници.

98. Също както по дело ASNEF и FECEMD [36] и в настоящия случай става въпрос за национална мярка — отново, ако бъде възприето посоченото по-горе стриктно тълкуване — която по-скоро променя обхвата на един от критериите по член 7 от Директива 95/46, отколкото да се ограничи до неговото по-точно определяне — единственото, за което органите на държавите членки разполагат с известна свобода на преценка съгласно член 5 от Директива 95/46.

99. Всъщност съгласно тази разпоредба „държавите членки в границите на разпоредбите на настоящата глава [37] определят по-точно условията, при които обработването на данни е законно. Въпреки това, съгласно постановеното в решение ASNEF и FECEMD [38], „държавите членки не могат нито да въвеждат други критерии за законност на обработването на лични данни, различни от прогласените в член 7 от тази директива, нито чрез допълнителни изисквания да изменят обхвата на предвидените в посочения член 7 шест критерия“.

100. Член 15 от TMG би намалил съществено обхвата на законния интерес, обосноваващ обработването на личните данни, спрямо предвиденото в член 7, буква е) от Директива 95/46, като не се ограничава до това да го конкретизира или уточни в рамките на разрешеното от член 5 от същата директива. Това своеобразно намаляване е освен това безусловно и категорично и не допуска защитата и осигуряването на общата функционална способност на електронната медия да бъдат претеглени спрямо „интереси, свързани с основните права и свободи на съответното физическо лице, които изискват защита по силата на член 1, параграф 1“ от Директива 95/46, както предвижда член 7, буква е) от същата директива.

101. В крайна сметка, също както по дела ASNEF и FECEMD [39], германският законодател „спрямо [някои категории лични данни] определя окончателно резултата от претеглянето на противоположните права и интереси, без да допуска различен резултат в зависимост от обстоятелствата на конкретния случай“, поради което „не става въпрос […] за по-точно определяне по смисъла на […] член 5“ от Директива 95/46.

102. При това положение считам, че Bundesgerichtshof (Федерален върховен съд) е задължен да даде тълкуване на националното законодателство в съответствие с Директива 95/46, което означава: а) сред основанията за обработване на така наречените „данни за ползването“ да може да се включи законният интерес на доставчика на електронни медии да защити тяхната обща функционална способност и б) да се допуска този интерес на доставчика на услугата да бъде претеглян спрямо интересите, свързани с основните права и свободи на съответния ползвател, за да се прецени кои от тях изискват защита по силата на член 1, параграф 1 от Директива 95/46 [40].

103. Според мен не е необходимо да се произнасям относно начина, по който това претегляне трябва да бъде извършено в случая по главното производство. Bundesgerichtshof (Федерален върховен съд) не е отправил питане във връзка с това, интересувайки се от разрешаването на предхождащ претеглянето въпрос, а именно дали такава преценка е допустима.

36 — Решение от 24 ноември 2011 г. (C-468/10 и C-469/10, EU:C:2011:777).

37 — Глава II, която е озаглавена „Общи правила относно законността на обработването на лични данни“ и обхваща членове 5—21 от Директива 95/46.

38 — Решение от 24 ноември 2011 г. (C-468/10 и C-469/10, EU:C:2011:777, т. 36).

39 — Пак там, т. 47.

40 — В хода на заседанието представителят на г-н Breyer оспори твърдението, че запазването на динамичните IP адреси е необходимо, за да се гарантира общата функционалност на интернет услугите при евентуални атаки. Не считам, че по този въпрос може да бъде даден категоричен отговор, разрешаването на който обаче трябва във всеки отделен случай да бъде предхождано от претеглянето на интереса на притежателя на интернет сайта спрямо правата и интересите на ползвателите.

104. Накрая, считам за излишно да посочвам, че запитващата юрисдикция може да вземе предвид евентуалните правни мерки, приети от държавата членка в рамките на правомощието, съдържащо се в член 13, параграф 1, буква г) от Директива 95/46, за да очертае обхвата на правата и задълженията, предвидени в член 6 от същата директива, когато това е необходимо, за да се гарантира, наред с друго, „[…] предотвратяването, разследването, разкриването и преследването на углавни престъпления […]“. Този въпрос също не е засегнат от запитващата юрисдикция, която несъмнено е запозната с посочените две разпоредби.

105. Ето защо предлагам на втория преюдициален въпрос да се отговори в смисъл, че член 7, буква е) от Директива 95/46 не допуска национална разпоредба, тълкуването на която не позволява доставчик на услуги да събира и обработва лични данни на даден ползвател без неговото съгласие с цел да се гарантира функционалната способност на електронната медия след приключването на съответното действие на ползване.

VI – **Заключение**

106. С оглед на изложеното по-горе предлагам на Съда да отговори на поставените въпроси, както следва:

„1) Съгласно член 2, буква а) 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 динамичен IP адрес, чрез който даден ползвател е осъществил достъп до интернет сайта на доставчик на електронни медии, представлява за този доставчик „лични данни“, доколкото осигуряващият достъп до мрежата разполага с допълнителни данни, които заедно с динамичния IP адрес позволяват идентифицирането на ползвателя.

2) Член 7, буква е) от Директива 95/46 трябва да се тълкува в смисъл, че целта да се гарантира функционалната способност на електронната медия по начало може да се счита за законен интерес, удовлетворяването на който обосновава обработването на лични данни след преценка за преимуществото на това обработване спрямо интересите или основните права на засегнатото лице. Национална разпоредба, която не допуска отчитането на този законен интерес, е несъвместима с посочения член“.