MANUEL CAMPOS SÁNCHEZ-BORDONA
FŐTANÁCSNOK INDÍTVÁNYA
Az ismertetés napja: 2016. május 12.[1]

C-582/14. sz. ügy

Patrick Breyer
kontra
Bundesrepublik Deutschland

(a Bundesgerichtshof [szövetségi legfelsőbb bíróság, Németország] által benyújtott előzetes döntéshozatal iránti kérelem)

„Személyes adatok feldolgozása — 95/46/EK irányelv — A 2. cikk a) pontja és a 7. cikk f) pontja — A »személyes adatok« fogalma — IP-címek — Elektronikus médiaszolgáltató által végzett tárolás — Nemzeti szabályozás, amely nem engedi meg az adatkezelő által kitűzött jogos érdek figyelembevételét”

1. Az internetprotokoll-cím (a továbbiakban: IP-cím) egy olyan bináris számsor, amelyet valamely eszközhöz (számítógép, tablet, okostelefon) rendelve azt azonosítja, és megengedi az elektronikus kommunikációs hálózathoz való csatlakozását. Az internetre való csatlakozáskor az eszköznek a hálózat-hozzáférést nyújtó szolgáltató által adott számsort kell alkalmaznia. Az IP-cím továbbításra kerül a felkeresett internetes oldalt tároló szerverre.

2. Különösen a hálózat-hozzáférést nyújtó szolgáltatók (általában a telefontársaságok) rendelnek az ügyfeleikhez úgynevezett „dinamikus IP-címeket”, időleges jelleggel, az egyes internet-csatlakozásokhoz kapcsolódóan, és a későbbi csatlakozások alkalmával rendszeresen változtatják azokat. Ugyanezen társaságok nyilvántartást vezetnek, amelyben szerepel, hogy egy meghatározott eszközhöz egy adott pillanatban milyen IP-címet rendeltek hozzá.[2]

3. A dinamikus IP-címekkel felkeresett internetes honlapok tulajdonosai is szoktak nyilvántartást vezetni, amelyekben feltüntetik, hogy milyen oldalakat, mikor és milyen dinamikus IP-címről kerestek fel. E nyilvántartások technikailag időkorlát nélkül tárolhatók az egyes felhasználók internethez való kapcsolódásának befejezését követően.

4. Egy dinamikus IP-cím önmagában nem elegendő ahhoz, hogy a szolgáltató azonosítsa az internetes oldal használóját. Ezt az azonosítást viszont a szolgáltató el tudja végezni, ha a dinamikus IP-címet összepárosítja a hálózat-hozzáférést nyújtó szolgáltató birtokában lévő egyéb kiegészítő adatokkal.

1 — Eredeti nyelv: spanyol.

2 — A nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló, 2006. március 15-i 2006/24/EK európai parlamenti és tanácsi irányelv (HL L 105., 54. o.) 5. cikke – egyéb kötelezettségek között – előírta, hogy a súlyos jogsértések kivizsgálása, felderítése és szankcionálása céljából tárolni kell „az internet-hozzáférési szolgáltatásba való belépés és az onnan való kilépés napját és időpontját, […] az internethozzáférés-szolgáltató által a közléshez rendelt, dinamikus vagy statikus IP-címmel együtt, valamint az előfizető vagy nyilvántartott felhasználó felhasználói azonosítóját”.

5. A jogvita tárgya annak eldöntése, hogy a dinamikus IP-címek személyes adatnak minősülnek-e a 95/46/EK irányelv[3] 2. cikkének a) pontja értelmében. A válaszhoz előzetesen meg kell határozni, hogy e tekintetben milyen jelentőséggel bír az, hogy a felhasználó azonosításához szükséges kiegészítő adatok nem az internetes oldal tulajdonosának, hanem egy harmadik személynek (konkrétan a hálózat-hozzáférést nyújtó szolgáltatónak) a birtokában vannak.

6. A Bíróság számára ez egy eddig még nem tárgyalt kérdés, mivel a Scarlet Extended ítélet[4] 51. pontjában a Bíróság kimondta, hogy az IP-címek „védett személyes adatok, hiszen lehetővé teszik az említett felhasználók pontos azonosítását”, ezt azonban egy olyan helyzetben tette, amelyben az IP-címeket a hálózat-hozzáférést nyújtó szolgáltató gyűjtötte és azonosította,[5] nem a tartalomszolgáltató, ahogyan ez a jelen ügyben történik.

7. Ha a dinamikus IP-címek az internetszolgáltatók szempontjából véve személyes adatoknak minősülnek, ezt követően meg kell vizsgálni, hogy feldolgozásuk a 95/46 irányelv hatálya alá tartozik-e.

8. Elképzelhető, még ha személyes adatokról van is szó, hogy nem részesülnek a 95/46 irányelv szerinti védelemben, ha például a feldolgozás célja az internetes oldal esetleges támadói ellen irányuló büntetőeljárás megindítása. Ebben az esetben a 95/46 irányelv, a 3. cikke (2) bekezdésének első franciabekezdése alapján, nem lenne alkalmazható.

9. Kérdéses ezenkívül, hogy a dinamikus IP-címeket tároló szolgáltató (a jelen esetben a Németországi Szövetségi Köztársaság) közhatalommal rendelkező szervként vagy inkább magánszemélyként végzi-e tevékenységét, amikor valamely felhasználónak hozzáférést enged az internetes oldalaihoz.

10. Ha a 94/46 irányelv alkalmazható, akkor pontosítani kellene, hogy a 7. cikkének f) pontjával milyen mértékben egyeztethető össze az olyan nemzeti szabályozás, amely korlátozza az általa megállapított egyik feltétel terjedelmét a személyes adatok feldolgozásának igazolása céljából.

I – **Jogi háttér**

A – *Az uniós jog*

11. A 95/46 irányelv (26) preambulumbekezdésének szövege az alábbi:

„(26) mivel a védelem elveit minden azonosított vagy azonosítható személyre vonatkozó információ esetében alkalmazni kell; mivel annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására; mivel a védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható; mivel a 27. cikk szerinti eljárási szabályzat hasznos eszköz lehet útmutatásként ahhoz, hogy hogyan kell az adatokat anonimmá tenni, és olyan formában megőrizni, amelyben a szóban forgó adatok azonosítása a továbbiakban már nem lehetséges”.

3 — A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv (HL L 281., 31. o.; magyar nyelvű különkiadás 13. fejezet, 15. kötet, 355. o.).

4 — 2011. november 24-i ítélet (C-70/10, EU:C:2011:771), 51. pont.

5 — Így történt a 2012. április 19-i Bonnier Audio és társai ítéletben is (C-461/10, EU:C:2012:219), 51 és 52. pont.

12. A 95/46 irányelv 1. cikke értelmében:

„(1) A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében.

(2) A tagállamok nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt.”

13. A 95/46 irányelv 2. cikke szerint:

„Ezen irányelv alkalmazásában:

a) »személyes adat«: az azonosított vagy azonosítható természetes személyre (»érintettre«) vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén;

b) a »személyes adatok feldolgozása« (»feldolgozás«): a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közléstovábbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés;

[…]

d) »adatkezelő«: az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját; ha a célokat és módokat egy adott nemzeti vagy közösségi jogszabály határozza meg, az adatkezelőt vagy a kinevezésére vonatkozó külön szempontokat ez a nemzeti vagy közösségi jogszabály jelöli ki;

[…]

f) »harmadik személy«: az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel, a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására;

[…]”.

14. Az 95/46 irányelv „Hatály” című 3. cikke előírja, hogy:

„(1) Ezen irányelvet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

(2) Az irányelv nem alkalmazandó az alábbi személyesadat-feldolgozásokra:

– a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek;

[…]”.

15. A 95/46 irányelvnek „A személyes adatok feldolgozásának jogszerűségére vonatkozó általános szabályok” címet viselő II. fejezete az 5. cikkel kezdődik, amelynek értelmében „a tagállamok, e fejezet rendelkezéseinek korlátai között, részletesen meghatározzák, hogy a személyes adatok feldolgozása milyen feltételek mellett jogszerű”.

16. A 95/46 irányelv 6. cikke alapján:

„(1) A tagállamok rendelkeznek arról, hogy a személyes adatok:

a) feldolgozását tisztességesen és törvényesen kell végezni;

b) gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon; a személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat;

c) gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek;

d) pontosak, és ha szükséges, időszerűek kell legyenek; minden észszerű intézkedést meg kell tenni annak érdekében, hogy a hibás vagy hiányos adatok, tekintettel gyűjtésük vagy további feldolgozásuk céljaira, törlésre vagy helyesbítésre kerüljenek;

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé. A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.

(2) Az adatkezelő feladata gondoskodni arról, hogy az (1) bekezdés rendelkezései teljesüljenek.”

17. A 95/46 irányelv 7. cikke szerint:

„A tagállamok rendelkeznek arról, hogy a személyes adatok csak abban az esetben dolgozhatók fel, ha:

a) az érintett ahhoz egyértelmű hozzájárulását adta; vagy

b) az adatfeldolgozás olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az adatfeldolgozás a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy

c) az adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges; vagy

d) ha feldolgozásuk az érintett létfontosságú érdekei védelméhez szükséges; vagy

e) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy

f) az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az 1. cikk (1) bekezdése értelmében védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében."

18. A 95/46 irányelv 13. cikkének rendelkezései szerint:

„(1) A tagállamok jogszabályokat fogadhatnak el a 6. cikk (1) bekezdésében, a 10. cikkben, a 11. cikk (1) bekezdésében, valamint a 12. és a 21. cikkben foglalt jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás az alábbiak biztosításához szükséges:

a) nemzetbiztonság;

b) honvédelem;

c) közbiztonság;

d) bűncselekmények vagy a szabályozott foglalkozások etikai vétségeinek megelőzése, vizsgálata, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;

e) valamely tagállam vagy az Európai Unió fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket;

f) a c), d) és e) pontban említett esetekben esetlegesen a hatósági feladatok gyakorlásához kapcsolódó ellenőrzési, felügyeleti és szabályozási tevékenység;

g) az érintett, vagy mások jogainak és szabadságainak védelme.

[…]"

B – *A nemzeti jog*

19. A Telemediengesetz[6] (az elektronikus médiáról szóló törvény, a továbbiakban: TMG) 12. §-a előírja, hogy:

„(1) A szolgáltató csak akkor gyűjthet és használhat fel személyes adatokat elektronikus média hozzáférhetővé tételével összefüggésben, ha ezt e törvény vagy kifejezetten az elektronikus médiára vonatkozó más jogszabály lehetővé teszi, vagy a felhasználó ebbe beleegyezett.

(2) A szolgáltató az elektronikus média hozzáférhetővé tételével összefüggésben gyűjtött személyes adatokat csak akkor használhatja fel más célra, ha ezt e törvény vagy kifejezetten az elektronikus médiára vonatkozó más jogszabály lehetővé teszi, vagy a felhasználó ebbe beleegyezett.

(3) Eltérő rendelkezés hiányában a személyes adatok védelmére vonatkozó hatályos rendelkezések alkalmazandók akkor is, ha az adatok feldolgozására nem automatizált módon kerül sor."

6 — 2007. február 26-i törvény (BGBl 2007 I., 179. o.).

20. A TMG 15. §-a értelmében:

„(1) A szolgáltató csak akkor gyűjtheti és használhatja fel a felhasználó személyes adatait, ha ez az elektronikus médium igénybevételének lehetővé tételéhez és elszámolásához szükséges (használati adatok). Használati adatok különösen a következők:

1. a felhasználó azonosítására szolgáló jellemzők;

2. a konkrét használat kezdetére és végére, valamint terjedelmére vonatkozó adatok és

3. a felhasználó által igénybe vett elektronikus médiára vonatkozó adatok.

(2) A szolgáltató akkor összesítheti a felhasználó különböző elektronikus média igénybevételére vonatkozó használati adatait, ha ez a felhasználóval való elszámoláshoz szükséges.

[…]

(4) A szolgáltató akkor használhatja fel a használati adatokat a használat befejeztét követően is, ha azok szükségesek a felhasználóval való elszámoláshoz (elszámolási adatok). A fennálló jogszabályi, alapszabályi vagy szerződéses megőrzési határidőknek való megfelelés céljából a szolgáltató zárolhatja az adatokat. [...]”

21. A Bundesdatenschutzgesetz[7] (adatvédelemről szóló szövetségi törvény, a továbbiakban: BDSG) 3. §-ának (1) bekezdése értelmében „[a] személyes adatok egy azonosított vagy azonosítható természetes személy (érintett) személyes vagy tárgyi körülményeire vonatkozó egyedi adatok. [...]”

II – **A tényállás**

22. P. Breyer abbahagyásra kötelezés iránti keresetet indított a Németországi Szövetségi Köztársasággal szemben az IP-címek tárolása miatt.

23. Számos szövetségi intézmény működtet a nyilvánosság számára hozzáférhető internetes honlapokat, amelyeken időszerű információkat tesznek közzé. A támadások elhárítására és a támadókkal szembeni büntetőeljárás megindításának lehetővé tétele érdekében e honlapok többségénél minden hozzáférést rögzítenek a naplófájlokban vagy nyilvántartásokban. E naplófájlok a művelet befejeztét követően is tárolják a lehívott adat, illetve a felkeresett oldal nevét, a keresőmezőkbe gépelt fogalmakat, a lehívás, illetve a felkeresés időpontját, a közvetített adatmennyiséget, a lehívás, illetve a felkeresés sikerességéről szóló jelentést, valamint a hozzáférő számítógép IP-címét.

24. P. Breyer, aki több ilyen oldalt is felkeresett, keresetében annak abbahagyására kérte kötelezni a Szövetségi Köztársaságot, hogy a hozzáférő gazdarendszer IP-címét tárolja vagy harmadik személyekkel tároltassa, amennyiben a tárolás nem szükséges az elektronikus médium elérhetőségének üzemzavar esetén történő helyreállításához.

25. P. Breyer keresetét első fokon elutasították. A fellebbezésének viszont részben helyt adtak, és a konkrét felkeresést követően történő tárolás abbahagyására kötelezték a Szövetségi Köztársaságot. Az abbahagyásra kötelezés feltételéül azt szabták, hogy a felperes a hozzáférés során megadja személyes adatait, elektronikus levélcím formájában is, és a tárolás ne legyen nélkülözhetetlen az elektronikus médium elérhetőségének helyreállításához.

7 — 1990. december 20-i törvény (BGBl 1990 I., 2954. o.).

III – **Az előzetes döntéshozatalra előterjesztett kérdés**

26. Miután mindkét fél felülvizsgálati kérelmet nyújtott be, a Bundesgerichtshof (szövetségi legfelsőbb bíróság, Németország) VI. tanácsa 2014. december 17-én előzetes döntéshozatal céljából az alábbi kérdéseket terjesztette elő:

„1) Úgy kell-e értelmezni a [...] 95/46/EK irányelv 2. cikkének a) pontját, hogy a szolgáltató által az internetes honlapjának felkeresésével összefüggésben tárolt internetprotokoll cím (IP-cím) a szolgáltató számára már akkor is személyes adatot képez, ha valamely harmadik személy (a jelen ügyben: a hozzáférés-szolgáltató) rendelkezik az érintett azonosításához szükséges pluszinformációval?

2) Ellentétes-e az adatvédelmi irányelv 7. cikkének f) pontjával az olyan nemzeti jogi rendelkezés, amely szerint a szolgáltató csak akkor gyűjtheti és használhatja fel a felhasználó személyes adatait annak beleegyezése nélkül, ha ez az elektronikus médium adott felhasználó általi konkrét igénybevételének lehetővé tételéhez és elszámolásához szükséges, és amely szerint az elektronikus médium általános működőképessége biztosításának célja nem indokolhatja a felhasználást a konkrét használat befejeztét követően?”

27. A kérdést előterjesztő bíróság magyarázata szerint a felperes a német jog alapján akkor követelhetné az IP-címek tárolásának abbahagyását, ha tárolása esetében a felperes általános személyiségi jogainak – konkrétabban a felperes „információs önrendelkezési” jogának – az adatvédelmi jog szerint nem megengedett megsértéséről lenne szó (a Bürgerliches Gesetzbuch [német polgári törvénykönyv] a Grundgesetz [alaptörvény] 1. és 2. cikkével összefüggésben értelmezett 1004. §-ának (1) bekezdése, 823. §-ának (1) bekezdése).

28. Ez az eset akkor állna fenn, ha: a) az IP-címek – legalábbis az internetes oldalhoz való hozzáférés időpontjával együtt – az adatvédelmi irányelv (26) preambulumbekezdésének második tagmondatával összefüggésben értelmezett 2. cikkének a) pontja, illetve a TMG-nek a BDSG 3. §-ának (1) bekezdésével összefüggésben értelmezett 12. §-ának (1) és (3) bekezdése értelmében vett „személyes adatnak” minősülnének, és b) nem állna fenn az adatvédelmi irányelv 7. cikkének f) pontja, illetve a TMG 12. §-ának (1) és (3) bekezdése, 15. §-ának (1) és (4) bekezdése szerinti megengedő feltételek valamelyike.

29. A Bundesgerichtshof (szövetségi legfelsőbb bíróság) szerint a nemzeti jog (a TMG 12. §-a (1) bekezdésének) értelmezése szempontjából mindenképpen tudni kell, hogyan értelmezendő a 95/46 irányelv 2. cikkének a) pontja szerinti személyes jelleg.

30. Ezenkívül az alapeljárásban eljáró bíróság rámutat arra, hogy a TMG 15. §-ának (1) bekezdése szerint – mely szerint a szolgáltató csak akkor gyűjtheti és használhatja fel a felhasználó személyes adatait, ha ez az elektronikus médium igénybevételének lehetővé tételéhez és elszámolásához szükséges (használati adatok) [8] – e belső rendelkezés értelmezése összefügg a 95/46 irányelv 7. cikke f) pontjának értelmezésével.

IV – **A Bíróság előtti eljárás. A felek érvei**

31. A német, az osztrák és a portugál kormány, valamint a Bizottság írásbeli észrevételt terjesztett elő. Csak ez utóbbi intézmény és P. Breyer vett részt a 2016. február 25-én tartott nyilvános tárgyaláson, amelyen a német kormány nem kívánt részt venni.

8 — A Bundesgerichtshof (szövetségi legfelsőbb bíróság) szerint használati adatok különösen a felhasználó azonosítására szolgáló jellemzők, a konkrét használat kezdetére és végére, valamint terjedelmére vonatkozó adatok és a felhasználó által igénybe vett elektronikus médiára vonatkozó adatok.

A – *A felek első kérdéssel kapcsolatos érvei*

32. P. Breyer szerint személyes adatoknak minősülnek azok az adatok is, amelyek kizárólag elméleti szinten párosíthatók össze, azaz egy lehetséges absztrakt kockázat alapján, amelynél kevésbé számít, hogy a gyakorlatban ez az összepárosítás tényleg megvalósul-e. Véleménye szerint az a tény, hogy egy szervezet nem teljesen képes beazonosítani egy személyt az IP-címet felhasználva, nem jelenti azt, hogy az adott személy számára ez ne jelentene kockázatot. Ezenkívül, véleménye szerint releváns tény, hogy Németország azért tárolja az IP-adatokat, hogy adott esetben esetleges támadásokat azonosítson, vagy büntetőeljárásokat indítson, ahogyan azt a Telekommunikationsgesetz (távközlési törvény) 113. §-a lehetővé teszi, és ahogy az számos esetben előfordult.

33. A német kormány szerint az első kérdésre nemleges választ kell adni. Véleménye szerint a dinamikus IP-címek nem fednek fel „azonosított” személyt a 95/46 irányelv 2. cikkének a) pontja értelmében. Annak eldöntéséhez, hogy az ugyanezen rendelkezés értelmében vett „azonosítható” személyre nézve nyújt-e információt, „relatív” megközelítéssel kell elvégezni az *azonosíthatóság* vizsgálatát. Véleménye szerint ez tűnik ki a 95/46 irányelv (26) preambulumbekezdéséből, amely szerint minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy harmadik személy „valószínűleg” felhasználna valamely személy azonosítására. E pontosítás jelezheti, hogy az uniós jogalkotó nem kívánt a 95/46 irányelv hatálya alá vonni olyan helyzeteket, amelyekben az azonosítás bármely harmadik személy részéről objektíve lehetséges.

34. A német kormány azt is állítja, hogy a 95/46 irányelv 2. cikkének a) pontja értelmében vett „személyes adat” fogalmát az irányelv célkitűzésével összhangban kell értelmezni, azaz biztosítani kell az alapvető jogok tiszteletben tartását. A természetes személyek védelmének szükségessége eltérő módon igazolható azzal összefüggésben, hogy ki rendelkezik az adatokkal, és hogy rendelkezik-e az azonosításukra felhasználható módszerekkel.

35. A német kormány előadja, hogy P. Breyer nem azonosítható a tartalomszolgáltatók által tárolt egyéb adatokkal összepárosított IP-címek alapján. Ennek érdekében az internet-hozzáférést nyújtó szolgáltatók rendelkezésére álló információit fel kell dolgozni, akik jogi szabályozás hiányában azt nem biztosíthatják a tartalomszolgáltatók számára.

36. Az osztrák kormány szerint éppen ellenkezőleg, a kérdésre igenlő választ kell adni. A 95/46 irányelv (26) preambulumbekezdése alapján valamely személy azonosíthatóságához nincs szükség arra, hogy az összes azonosítási adat egyetlen szerv kezében legyen. Egy IP-cím tehát személyes adat lehet, ha egy harmadik személy (mint például a internet-hozzáférést nyújtó szolgáltató) – különösebb erőfeszítések kifejtése nélkül is – rendelkezik a cím előfizetőjének azonosítására irányuló módszerrel.

37. A portugál kormány szintén az igenlő válasz felé hajlik, és megállapítja, hogy az IP-cím, a felkeresési időpontjával összevetve, személyes adatnak minősül, amennyiben azt eredményezi, hogy az IP-címet tároló szervtől eltérő szerv azonosítja a felhasználót.

38. A Bizottság is igenlő választ javasol adni, és a Bíróság által a Scarlet Extended-ügyben [9] alkalmazott megoldásra támaszkodik. A Bizottság szerint, mivel az IP-címeket éppen a felhasználók kibertámadások esetén történő azonosítása érdekében tárolják, az internet-hozzáférést nyújtó szolgáltató által tárolt kiegészítő adatok alkalmazása olyan módszert képezhet, amelyet a 95/46 irányelv (26) preambulumbekezdése értelmében „valószínűleg” felhasználhatnak. Végeredményben, a Bizottság véleménye szerint, mind az irányelv által kitűzött cél, mind az Európai Unió Alapjogi Chartájának (a továbbiakban: Charta) 7. és 8. cikke a 95/46 irányelv 2. cikke a) pontjának tág értelmezése mellett szól.

9 — 2011. november 24-i ítélet (C-70/10, EU:C:2011:771), 51. pont.

B – *A felek második kérdéssel kapcsolatos érvei*

39. P. Breyer szerint a 95/46 irányelv 7. cikkének f) pontja generálklauzulát képez, amelynek gyakorlati alkalmazása további pontosítást igényel. A Bíróság ítélkezési gyakorlata alapján tehát a konkrét ügy körülményeinek értékeléséről és annak meghatározásáról lehet szó, hogy vannak-e jogos érdekkel rendelkező csoportok a szóban forgó rendelkezés értelmében, így nem csak lehetséges, hanem nélkülözhetetlen az e csoportokra vonatkozó egyedi szabályok előírása a cikk alkalmazása céljából. Ebben az esetben és P. Breyer szerint, a nemzeti szabályozás összeegyeztethető a 95/46 irányelv 7. cikkének f) pontjával, mivel az internetes oldalnak nem fűződik érdeke a személyes adatok tárolásához, vagy mert az anonimitás megőrzéséhez fűződő érdek hangsúlyosabb. Véleménye szerint ugyanakkor az adatok rendszerezett és a személyes jelleg megőrzésével történő tárolása nem egyeztethető össze a demokratikus társadalmakkal, és az elektronikus média működőképességének biztosításához nem szükséges, illetve azzal nem arányos, hiszen az tökéletesen megvalósítható a személyes adatok tárolása nélkül is, ahogy azt néhány szövetségi minisztérium honlapja is bizonyítja.

40. A német kormány azt állítja, hogy nem szükséges vizsgálni a második kérdést, amely kizárólag abban az esetben kerül előterjesztésre, amennyiben az első kérdésre igenlő választ kellene adni, ez az eset azonban véleménye szerint a fent kifejtett indokok miatt nem áll fenn.

41. Az osztrák kormány azt a választ javasolja adni a kérdésre, hogy a 95/46 irányelv általában véve nem ellentétes az alapeljárás tárgyát képezőkhöz hasonló adatok tárolásával, ha az elengedhetetlen az elektronikus média megfelelő működésének biztosításához. E kormány szerint az IP-címeknek az internetes honlapok felkeresésének időtartamán túl, korlátozott ideig történő tárolása jogszerű lehet, amennyiben tiszteletben tartja a személyes adatokat kezelő szervnek az ezen adatok védelmére irányuló, a 95/46 irányelv 17. cikkének (1) bekezdésében előírt intézkedések alkalmazására vonatkozó kötelezettségét. A kibertámadások elleni küzdelem igazolhatja a korábbi támadásokra vonatkozó adatok elemzését, és azt is, hogy néhány IP-cím tekintetében megtagadják az internetes oldalhoz való hozzáférést. Az alapeljárásban szereplő adatokhoz hasonló adatok tárolásának arányosságát az elektronikus média megfelelő működőképessége biztosításának célja szempontjából, esetről esetre kellene értékelni, a 95/46 irányelv 6. cikkében foglalt elvekre tekintettel.

42. A portugál kormány azt állítja, hogy a 95/46 irányelv 7. cikkének f) pontjával nem ellentétesek az alapeljárásban alkalmazott nemzeti szabályok, mert a német jogalkotó már elvégezte az említett rendelkezésben előírt súlyozást, egyrészt a személyes adatokat kezelő szerv jogos érdekei, másrészt az említett adatokkal érintett személyek jogai és szabadságai között.

43. A Bizottság szerint a 95/46 irányelv 7. cikkének f) pontját átültető nemzeti szabályozásnak úgy kell meghatároznia a személyes adatok feldolgozásának céljait, hogy azok az érintett egyén számára kiszámíthatóak legyenek. Véleménye szerint a német szabályozás nem felel meg e követelménynek azáltal, hogy a TMG 15. §-ának (1) bekezdésében előírja, hogy az IP-címek tárolása akkor engedélyezett, „ha ez az elektronikus médium igénybevételének lehetővé tételéhez [...] szükséges”.

44. A Bizottság a második kérdést tehát úgy javasolja megválaszolni, hogy e rendelkezéssel ellentétes az olyan nemzeti jogi rendelkezés – amely szerint a szolgáltatóként eljáró állami szerv még akkor is gyűjtheti és felhasználhatja a felhasználó személyes adatait annak beleegyezése nélkül, ha a célkitűzése az elektronikus médium általános megfelelő működőképességére irányul –, ha az említett nemzeti jogi rendelkezés nem állapítja meg kellően világosan és pontosan e célkitűzést.

V – **Értékelés**

A – *Az első kérdés*

1. Az előterjesztett kérdés terjedelmének körülhatárolása

45. Az alapján, ahogy azt a Bundesgerichtshof (szövetségi legfelsőbb bíróság) megfogalmazta, az előzetes döntéshozatalra előterjesztett első kérdése annak tisztázására irányul, hogy egy olyan IP-cím, amelyről egy internetes oldalt felkeresnek, az ezen oldal tulajdonosának minősülő hatóság számára (a 95/46/EK irányelv 2. cikkének a) pontja értelmében vett) személyes adatot képez-e, amennyiben a hálózat-hozzáférést nyújtó szolgáltató rendelkezik az érintett azonosítását lehetővé tevő kiegészítő adatokkal.

46. Az így megfogalmazott kérdés eléggé pontos ahhoz, hogy eleve kizárja az IP-cím jogi jellegével kapcsolatban absztrakt módon felvetődő egyéb kérdéseket a személyes adatok védelmével összefüggésben.

47. Egyfelől, a Bundesgerichtshof (szövetségi legfelsőbb bíróság) kizárólag a „dinamikus IP-címekre” hivatkozik, vagyis azokra, amelyeket az egyes hálózati csatlakozásokhoz rendelnek, és amelyek a későbbi csatlakozások alkalmával módosulnak. A „fix vagy statikus IP-címek” tehát, amelyeket állandóság és a hálózathoz csatlakoztatott készülék folyamatos azonosításának lehetősége jellemez, nem tartoznak ide.

48. Másfelől, a kérdést előterjesztő bíróság abból a vélelemből indul ki, hogy az internetes honlap szolgáltatója az alapeljárásban nincs abban a helyzetben, hogy a dinamikus IP-cím segítségével beazonosítsa az oldalait felkereső személyeket, és ő maga nem rendelkezik azokkal a kiegészítő adatokkal sem, amelyek az említett IP-címmel összepárosítva biztosítanák a beazonosítást. Úgy tűnik, hogy a Bundesgerichtshof (szövetségi legfelsőbb bíróság) szerint ebben az összefüggésben a dinamikus IP-cím nem minősülhet a 95/46 irányelv 2. cikkének a) pontja szerinti személyes adatnak *az internetes honlap szolgáltatója számára*.

49. A kérdést előterjesztő bíróság kétsége azon lehetőséggel kapcsolatos, hogy a dinamikus IP-cím az internetes honlap szolgáltatója számára személyes adatnak minősül-e, *ha valamely harmadik személy rendelkezik olyan kiegészítő adatokkal*, amelyek az IP-címmel összepárosítva beazonosíthatóvá teszik a honlapjaikat felkereső személyeket. Márpedig, és egy további releváns pontosításként, a Bundesgerichtshof (szövetségi legfelsőbb bíróság) nem a kiegészítő adatokkal rendelkező bármely harmadik személyre hivatkozik, hanem csak a hálózat-hozzáférést nyújtó szolgáltatókra (kizárja tehát az ilyen jellegű adatokkal rendelkező más szolgáltatókat).

50. Így nem képezik vita tárgyát többek között a következők: a) az, hogy a statikus IP-címek a 95/46 irányelv szerinti személyes adatoknak minősülnek-e;[10] b) az, hogy a dinamikus IP-címek mindig és minden körülmények között ezen irányelv értelmében vett személyes adatok-e, és végül, c) az, hogy a dinamikus IP-címek személyes adatoknak való minősítése elkerülhetetlen-e, amint adódik egy harmadik fél, bármiféle is legyen, amely képes azt a hálózat felhasználóinak azonosítására felhasználni.

10 — A Bíróság által a 2011. november 24-i Scarlet Extended-ítéletben (C-70/10, EU:C:2011:771), 51. pont és a 2012. április 19-i Bonnier Audio és társai ítéletben (C-461/10, EU:C:2012:219) megválaszolt kérdés. Ez utóbbi ítélet 51. és 52. pontjában a Bíróság megállapította, hogy „az azonosítás érdekében [...] egy olyan IP-címmel rendelkező internethasználó nevének és címének közlése, amely címről feltehetőleg védelem alatt álló műveket tartalmazó fájlok jogellenes cseréjét valósították meg, […] személyes adatok kezelésének minősül a 95/46 irányelv 2. cikke b) pontjának összefüggésében értelmezett 2002/58 irányelv 2. cikkének első bekezdése alapján”.

51. Kizárólag annak eldöntéséről van tehát szó, hogy a dinamikus IP-cím személyes adatot képez-e az internetszolgáltató szempontjából, ha a hálózathoz való csatlakozást biztosító távközlési cég (hozzáférést nyújtó szolgáltató) olyan kiegészítő adatokat kezel, amelyeket a szóban forgó címmel összepárosítva beazonosítható az a személy, aki az internetszolgáltató által üzemeltetett internetes honlapot felkereste.

2. A kérdés érdeméről

52. A jelen előzetes döntéshozatalra utaló határozat által felvetett kérdés a szakirodalomban és a német ítélkezési gyakorlatban heves viták tárgyát képezi, két véleménytáborra osztottan.[11] Az egyik szerint (amelyik az „objektív" és az „abszolút" kritériumot választja) a felhasználó beazonosítható (és ezért az IP-cím védendő személyes adatnak minősül), ha – bármilyen alkalmatossággal vagy eszközzel rendelkezzen is az internetszolgáltató – a dinamikus IP-címnek valamely harmadik személy (például, a hálózathoz való hozzáférést nyújtó szolgáltató) által rendelkezésre bocsátott adatokkal való összepárosítása segítségével a beazonosítása egyszerűen megoldható.

53. A másik vélemény támogatói szerint (akik a „relatív" kritériumot támogatják), a felhasználó végső azonosítása során egy harmadik személy segítségének lehetséges igénybevétele nem elegendő ahhoz, hogy a dinamikus IP-címnek személyes jelleget tulajdonítsanak. Az adatokhoz hozzáférő személy azon képessége a releváns, amellyel saját módszerei szerint felhasználja az adatot, és így azonosítani tud egy személyt.

54. Bármilyen jellegűek is legyenek a belső jog értelmében e jogvita körülményei, a Bíróság válaszának a 95/46 irányelv két rendelkezésének értelmezésére kell korlátozódnia, amely rendelkezésekre, azaz a 2. cikk a) pontjára[12] és a (26) preambulumbekezdésre,[13] az alapeljárásban eljáró bíróság és az eljárás felei is hivatkoztak.

55. A dinamikus IP-címek egyszerűen azzal, hogy információt nyújtanak arról, hogy egy számítógépről (vagy más eszközről) mely napon és időpontban kerestek fel egy internetes honlapot, az internetes felhasználók magatartásával kapcsolatosan bizonyos szabályokat mutatnak, és ezért a magánélet tiszteletben tartásához való azon jog lehetséges megsértését eredményezik,[14] amelyet az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény 8. cikke és a Charta 7. cikke is biztosít, amely rendelkezésekre, valamint a Charta 8. cikkére tekintettel a 95/46 irányelvet is értelmezni kell.[15] A peres felek valójában nem vonják kétségbe ezen előzetes megállapítást, amely mint ilyen szintén nem képezi az előzetes döntéshozatalra előterjesztett kérdés tárgyát.

11 — A két szakirodalmi álláspontról lásd például: Schreibauer, M., in: *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., és von Lewinski, K. (szerk.), Carl Heymanns Verlag és Wolters Kluwer kiadó, Köln, 2014., 4. kiadás, Telemediengesetz (4–10) 11. §. Nink, J. és Pohle, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze", in: *Multimedia und Recht*, 2015. 9. sz., 563–567. pont. Heidrich, J. és Wegener, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging", in: *Multimedia und Recht*, 2015. 8. sz., 487–492. o. Leisterer, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr", in: *Computer und Recht*, 2015. 10. sz., 665–670. o.

12 — A 13. pontban idézett rendelkezés.

13 — A 11. pontban idézett rendelkezés.

14 — Cruz Villalón főtanácsnok erre emlékeztetett a Scarlet Extended ügyre vonatkozó indítványában (C-70/10, EU:C:2011:255), 76. pont, és így gondolja az európai adatvédelmi biztos az Európai Unió által a hamisítás elleni kereskedelmi megállapodásról (ACTA) folytatott tárgyalásokról szóló, 2010. február 22-i véleményében (HL 2010. C 147., 1. o., 24. pont) és a gyermekek szexuális zaklatásáról, szexuális kizsákmányolásáról és a gyermekpornográfia elleni küzdelemről szóló európai parlamenti és tanácsi irányelv iránti javaslatról és a 2004/68/IB kerethatározat hatályon kívül helyezéséről szóló, 2010. május 10-i véleményében (HL 2010. C 323., 6. o., 11. pont).

15 — Lásd e tekintetben: 2003. május 20-i Österreichischer Rundfunk ítélet (C-465/00, C-138/01 és C-139/01, EU:C:2003:294), 68. pont és Kokott főtanácsnok Promusicae-ügyre vonatkozó indítványa (C-275/06, EU:C:2007:454), 51. és azt követő pontok.

56. Az a személy, akire az említett részletes adatok vonatkoznak, nem minősül „azonosított természetes személynek”. Valamely kapcsolódás napja és időpontja, valamint számmal meghatározott eredete sem közvetlenül, sem azonnali jelleggel nem fedik fel azon természetes személy kilétét, akinek az eszközéről felkeresik az internetes honlapot, és az azt kezelő felhasználót (aki bármilyen természetes személy lehet) sem azonosítják.

57. Mindazonáltal, amennyiben a dinamikus IP-cím – akár önmagában, akár az adatok egyesítésével – segít meghatározni az internetes honlap felkeresésénél használt eszköz tulajdonosának személyét, „azonosítható személyre” vonatkozó információnak minősíthető. [16]

58. A Bundesgerichtshof (szövetségi legfelsőbb bíróság) felvetése szerint a dinamikus IP-cím önmagában nem elegendő azon felhasználó azonosítására, aki e címen keresztül keresett fel egy internetes honlapot. Ha az internetszolgáltató ezzel szemben a dinamikus IP-cím útján azonosítani tudná a felhasználót, kétségtelenül a 95/46 irányelv szerinti személyes adatról lenne szó. Nem úgy tűnik azonban, hogy az előzetes döntéshozatalra előterjesztett kérdés erre irányulna, amely kérdés azon alapul, hogy az alapeljárásban érintett internetszolgáltatók kizárólag a dinamikus IP-cím alapján nem tudják azonosítani a felhasználót.

59. A dinamikus IP-cím, más adatokkal összepárosítva, biztosítani tudja a felhasználó „közvetett” azonosítását, amely megállapítással mindenki egyetért. Az az eshetőség, hogy esetleg léteznek a dinamikus IP-címhez kapcsolható kiegészítő adatok, vajon minden további nélkül megengedi-e, hogy a dinamikus IP-címet az irányelv értelmében vett személyes adatok csoportjába soroljuk? Azt kell eldönteni, hogy ebből a szempontból elegendő-e az adatok megismerésének elvont, puszta lehetősége, vagy ellenkezőleg, azoknak a dinamikus IP-címet már ismerő személy vagy harmadik személy rendelkezésére kell állniuk.

60. A felek az észrevételeiket a 95/46 irányelv (26) preambulumbekezdésének értelmezésére összpontosították, amelynek szövegéből kiemelik az „olyan módszert [...], amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására” fordulatot. A kérdést előterjesztő bíróság által feltett kérdés nem azon kiegészítő adatokra vonatkozik, amelyek az alapeljárásban érintett internetszolgáltatók birtokában vannak. Nem is e kiegészítő adatokkal rendelkező harmadik személyekre hivatkozik (amely adatok összesítése a dinamikus IP-címmel a felhasználó azonosítását biztosítja), hanem a hálózati hozzáférést nyújtó szolgáltatókra irányul.

61. Nincs szükség tehát arra, hogy a jelen ügyben a Bíróság minden olyan eszközt megvizsgáljon, amelyet az alperes az alapeljárásban „valószínűleg” felhasználna ahhoz, hogy a rendelkezésre álló dinamikus IP-címek személyes adatoknak minősülhessenek. Mivel a Bundesgerichtshof (szövetségi legfelsőbb bíróság) kizárólag a harmadik személyek birtokában lévő kiegészítő adatokra hivatkozik, arra lehet következtetni, hogy: a) az alperes nem rendelkezik olyan saját kiegészítő adatokkal, amelyek a felhasználó azonosítását lehetővé teszik, vagy b) rendelkezésére állnak ilyen adatok, de nincs abban a helyzetben, hogy adatkezelőként ilyen szándékkal valószínűleg felhasználná azokat a 95/46 irányelv (26) preambulumbekezdése szerint.

16 — Ellenkező bizonyítás hiányában vélelmezni kell, hogy az említett személy böngészett az interneten és felkereste az adott internetes honlapot. Ugyanakkor ez utóbbi feltételezés mellőzése esetén is, az internetes honlap felkeresésének napjára, időpontjára és számmal meghatározott eredetére vonatkozó információ alapján lehetővé válik e hozzáférés összekapcsolása az eszköz tulajdonosával és közvetlenül a hálózaton tanúsított magatartásának szabályaival. Elképzelhető kivételek lehetnek az internetes kávézókhoz hasonló helyek azon számítógépeihez rendelt IP-címek, amelyek anonim felhasználói azonosíthatatlanok, és tulajdonosaikról a helyiség forgalma nem nyújt semmilyen releváns személyes információt. Egyébként ez az egyetlen olyan kivétel azon elv alól, miszerint az IP-címek személyes adatoknak minősülnek, amelyet a 95/46 irányelv által létrehozott, személyesadat-feldolgozás vonatkozásában az egyének védelmével foglalkozó csoport (úgynevezett 29. cikk szerinti munkacsoport) is elfogad. A csoport személyes adatok fogalmáról szóló, WP 136, 2007. június 20-i 4/2007. sz. véleménye a http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm oldalon olvasható.

62. Mindkét eset a ténybeli körülményeknek a kérdést előterjesztő bíróság feladatát képező megállapításától függ. A Bíróság megadhatna általános jellegű szempontokat azon módszerek fogalmának értelmezéséhez, amelyeket „az adatkezelő [...] valószínűleg felhasználna”, ha a Bundesgerichtshofnak (szövetségi legfelsőbb bíróság) azzal kapcsolatban lennének kételyei, hogy az alperes képes-e észszerű módon felhasználni a saját kiegészítő adatait. Mivel a jelen esetben nem ez a helyzet, véleményem szerint kizárt, hogy a Bíróság most olyan értelmezési szempontokat adjon meg, amelyek nélkülözhetők a kérdést előterjesztő bíróság számára, vagy amelyeket nem is kért.

63. Az előzetes döntéshozatalra előterjesztett kérdés lényege tehát annak eldöntésére korlátozódik, hogy a dinamikus IP-címek személyes adatoknak való minősítése szempontjából releváns-e az a körülmény, hogy igen konkrét harmadik személy – internet-hozzáférést nyújtó szolgáltató – olyan kiegészítő adatokkal rendelkezik, amelyek e címekkel összepárosítva alkalmasak egy meghatározott internetes honlapot felkereső felhasználó azonosítására.

64. Ismét csak a 95/46 irányelv (26) preambulumbekezdésére kell hivatkozni. Az „olyan módszert, amit [...] *más személy*[17] valószínűleg felhasználna” fordulat olyan értelmezés alapjául szolgálhat, amely szerint elegendő lenne, ha valamely más személy kiegészítő adatokat tudna megszerezni (amelyek valamely személy azonosítása céljából összepárosíthatók egy dinamikus IP-címmel), ahhoz, hogy e cím *eo ipso* személyes adatnak minősüljön.

65. E maximálisan kiterjesztő értelmezés eredményeképpen a gyakorlatban mindenfajta információt személyes adatnak kellene tekinteni, bármennyire hiányos is önmagában valamely felhasználó azonosításához. Soha nem zárható ki abszolút bizonyossággal, hogy nincs olyan kiegészítő adatokat birtokló harmadik személy, amely adatok az adott információval összepárosíthatók, és következésképpen alkalmasak valamely személy azonosságának felfedésére.

66. Véleményem szerint annak lehetősége, hogy a többé-kevésbé közeli jövőben a műszaki eszközök fejlődése érzékelhetően az adatszerzésre és -feldolgozásra irányuló egyre kifinomultabb eszközökhöz való hozzáféréshez vezet, igazolja az elővigyázatosságot, amelyet a magánélet védelme érdekében kívánnak érvényesíteni. Az adatvédelem területén releváns jogi kategóriák meghatározása során igyekeztek ezekbe olyan magatartásformákat belefoglalni, amelyek kellően tágak és rugalmasak bármely elképzelhető eset lefedésére.[18]

67. Úgy vélem azonban, hogy ez – az egyébként nagyon is jogos – aggodalom nem vezethet a jogalkotó szabályozási céljainak mellőzéséhez, és hogy a 95/46 irányelv (26) preambulumbekezdésének rendszertani értelmezése nem korlátozódhat az „olyan módszerekre, amelyeket *más személyek* valószínűleg felhasználnának”.

68. Hasonlóképpen, ahhoz, hogy a (26) preambulumbekezdés ne az adatkezelő (jelen esetben az internetszolgáltató) által használható bármely módszerre, hanem csak azokra vonatkozzon, amelyeket ez utóbbi „valószínűleg” felhasználhat, ez úgy is érthető, hogy a jogalkotó azon „más személyekre” hivatkozik, akikhez az adatkezelő – *szintén valószínűleg [értsd: észszerű módon*] – az azonosításhoz szükséges kiegészítő adatok megszerzése érdekében fordulhat. Nem így történik, ha e harmadik személyekkel felvett kapcsolat emberi és anyagi erőforrás szempontjából valójában nagyon költséges, vagy gyakorlatilag megvalósíthatatlan, vagy azt a törvény tiltja. Máskülönben, ahogy azt korábban

17 — Az eredeti szövegben kiemelés nélkül.

18 — Ez az óvatos és megelőző jellegű kijelentés képezi a 29. cikk szerinti munkacsoport által képviselt álláspont alapját, akik szerint, ahogy azt jeleztem, azon elvből kell kiindulni, hogy az IP-címek személyes adatnak minősülnek, egyetlen kivételként elfogadva azt az esetet, amikor a szolgáltató abszolút bizonyossággal meg tudná határozni, hogy olyan címekről van szó, amelyek olyan azonosíthatatlan személyekhez tartoznak, mint például egy internetkávézó felhasználói. Lásd: 16. lábjegyzet vége.

megjegyeztem, gyakorlatilag nem lehetne különbséget tenni az egyik és másik módszer között, mivel mindig elképzelhető lenne olyan harmadik személlyel kapcsolatos feltevés eshetősége, amely, lévén, hogy az internetszolgáltató számára hozzáférhetetlen, most vagy a jövőben rendelkezhet valamely felhasználó azonosításának támogatására alkalmas kiegészítő adatokkal.

69. Ahogy azt előrebocsátottam, a Bundesgerichtshof (szövetségi legfelsőbb bíróság) által hivatkozott harmadik személy a hálózat-hozzáférést nyújtó szolgáltató. Biztos, hogy a harmadik személlyel kapcsolatban észszerűen feltételezhető, hogy a szükséges kiegészítő adatok megszerzése érdekében a szolgáltatóhoz fordul, ha a leghatékonyabb, leggyakorlatibb és legközvetlenebb módon kívánja azonosítani az internetes honlapját felkereső felhasználót a dinamikus IP-cím segítségével. Semmiképpen nem egy feltételezett, ismeretlen és hozzáférhetetlen harmadik személyről, hanem az internet rendszerének egyik főszereplőjéről van szó, akiről bizonyosan tudható, hogy rendelkezik a szolgáltató által a felhasználó azonosításához kért adatokkal. Ugyanis, ahogy azt a kérdést előterjesztő bíróság előadja, arról a konkrét harmadik személyről van szó, akihez az alapeljárásban az alperes a számára nélkülözhetetlen kiegészítő adatok megszerzése céljából fordulni kíván.

70. Az internet-hozzáférést nyújtó szolgáltató tipikusan az a harmadik személy, akire a 95/46 irányelv (26) preambulumbekezdése hivatkozik, akihez az alapeljárás szolgáltatója legvalószínűbb módon fordulhat. Tisztázni kell azonban még, hogy a harmadik személy birtokában lévő kiegészítő adatok megszerzése „valószínűleg” kivitelezhetőnek vagy megvalósíthatónak minősülhet-e.

71. A német kormány azt állítja, hogy mivel az internet-hozzáférést nyújtó szolgáltató birtokában lévő információ személyes adatnak minősül, nem bocsáthatja feltétel nélkül rendelkezésre, hanem az ilyen adatok kezelését szabályozó jogszabályok alapján teheti ezt meg. [19]

72. Kétségtelenül így van, mivel az információ felhasználásához figyelembe kell venni a személyes adatokra irányadó jogszabályokat. Valamely információ akkor szerezhető meg „valószínűleg”, ha az ilyen fajta adatokra irányadó feltételek teljesülnek, közülük az első pedig a tárolásukra és másoknak történő továbbításukra vonatkozó jogi lehetőség. Kétségtelen, hogy az internet-hozzáférést nyújtó szolgáltató elutasíthatja a kért adatok átadását, de az ellenkezője is elképzelhető. Az adatátvitel teljesen „valószínű” lehetősége az internetszolgáltató szempontjából önmagától személyes adattá teszi a dinamikus IP-címet a 95/46 irányelv (26) preambulumbekezdésében foglaltak alapján.

73. A *törvény keretein belüli*, ezért „észszerű” ténybeli eshetőségről van szó. A 95/46 irányelv által hivatkozott valószínű hozzáférési módszereknek meghatározásuknál fogva jogszerű módszereknek kell lenniük. [20] Ez az az előfeltevés, amelyből természetesen a kérdést előterjesztő bíróság kiindul, amint arra a német kormány emlékeztet. [21] Így jelentősen csökkenek a jogilag releváns hozzáférési módok, mivel kizárólag jogszerű módoknak kell lenniük. Míg azonban ezek fennállnak, bármennyire is korlátozó jellegűek a gyakorlati alkalmazásuk során, „valószínű módszert” jelentenek a 95/46 irányelv értelmében.

74. Következésképpen úgy vélem, hogy a Bundesgerichtshof (szövetségi legfelsőbb bíróság) által előterjesztett formában az első kérdésre igenlő választ kell adni. A dinamikus IP-címet az internetszolgáltató szempontjából személyes adatnak kell tekintetni, figyelemmel arra, hogy van olyan harmadik személy (hálózat-hozzáférést nyújtó szolgáltató), amelyhez az IP-címmel összepárosításra kerülő olyan kiegészítő adat megszerzése érdekében valószínűleg fordulni lehet, amely lehetővé teszi a felhasználó azonosítását.

19 — Írásbeli észrevételei 40. és 45. pontja.

20 — Ebben az összefüggésben nem releváns, hogy a személyes adatokhoz való hozzáférés *tényleg* lehetséges-e az adatvédelmi törvények megsértésével.

21 — Írásbeli észrevételei 47. és 48. pontja.

75. Az eredmény, amelyhez az általam javasolt megoldással ellenkező megoldás vezethet, úgy vélem, hogy azt erősíti. Ha a dinamikus IP-címek nem minősülnek személyes adatnak az internetszolgáltató szempontjából, ez utóbbi végtelen ideig tárolhatja az adatokat, és bármikor kérheti az internet-hozzáférést nyújtó szolgáltatótól a kiegészítő adatokat, hogy azokkal összepárosítsa az IP-címet, és azonosítsa a felhasználót. Ilyen körülmények között, ahogy azt a német kormány is elismeri,[22] a dinamikus IP-cím személyes adattá válik, mivel a felhasználó azonosításához már rendelkezésre állnak az érvényes kiegészítő adatok, és e tekintetben az adatvédelemre vonatkozó jogszabályokat kell alkalmazni.

76. Márpedig olyan adatról van szó, amelynek tárolása csak akkor lehetséges, ha addig a szolgáltató szerint nem minősült személyes adatnak. Így a szolgáltató dönthet a dinamikus IP-cím személyes adatként való jogi minősítéséről, amely annak eshetőségétől függ, hogy a jövőben valamikor úgy dönthet, hogy a harmadik személytől kért kiegészítő adatokkal összepárosítva felhasználja azt a felhasználó azonosítására. Véleményem szerint azonban a 95/46 irányelv értelmében annak – valószínű – lehetősége bír jelentőséggel, hogy van egy „hozzáférhető” harmadik személy, aki valamely személy azonosításához szükséges eszközökkel rendelkezik, és nem pedig az meghatározó, hogy a harmadik személy igénybevételének lehetősége megvalósul-e.

77. Az a megközelítés is elfogadható, a német kormánnyal egyetértésben, hogy a dinamikus IP-cím csak akkortól válik személyes adattá, amikor azt az internet-hozzáférést nyújtó szolgáltató megkapja. Ezzel együtt azt is el kellene ismerni, hogy e minősítésnek visszaható hatálya van az IP-cím tárolásának határidejét illetően, és ennek következtében azt nem létezőnek kellene tekinteni a tárolásra előírt határidő elteltével, ha már az elején személyes adatnak minősítették. Ilyen körülmények között, ez a személyes adatok védelmére vonatkozó jogszabályok szellemével ellentétes eredményre vezetne. Az ezen adatok pusztán időszakos tárolását igazoló indok meghiúsulhat olyan minőség jelentőségének esetleg késedelmes megállapításával, amely kezdettől fogva az adatok részét képezi: így a valamely természetes személy – önállóan vagy más adatokkal együtt történő – azonosításának eszközeként érvényesülő hatékonyságuk. Szintén ezen – egyszerűen gazdasági – ok miatt indokoltabb kezdettől fogva ilyen jellegűnek tekinteni.

78. Első következtetésként tehát úgy vélem, hogy a 95/46 irányelv 2. cikkének a) pontját úgy kell értelmezni, hogy a szolgáltató által valamely internetes honlap felkeresésével kapcsolatban tárolt IP-cím a szolgáltató szempontjából személyes adatnak minősül, amennyiben a hálózat (internet-)hozzáférést nyújtó szolgáltató rendelkezik az érintett azonosítását lehetővé tevő kiegészítő adatokkal.

B – *Második kérdés*

79. Az előzetes döntéshozatalra előterjesztett második kérdésével a Bundesgerichtshof (szövetségi legfelsőbb bíróság) arra kíván választ kapni, hogy a 95/46 irányelv 7. cikkének f) pontjával ellentétes-e az olyan nemzeti jogi rendelkezés, amely csak akkor fogadja el valamely felhasználó személyes adatainak gyűjtését és felhasználását annak beleegyezése nélkül, ha ez az elektronikus médium adott felhasználó általi konkrét igénybevételének lehetővé tételéhez és elszámolásához szükséges, anélkül, hogy az elektronikus médium általános működőképessége biztosításának célja indokolhatná az adatok felhasználását a konkrét használat befejeztét követően.

80. A válaszadás előtt pontosítani kell a Bundesgerichtshof (szövetségi legfelsőbb bíróság) által nyújtott információt, amely szerint a vitatott adatokat az alapeljárásban érintett internetes honlapok megfelelő működésének biztosítása érdekében tárolják, adott esetben lehetővé téve az adatok ellen irányuló kibertámadások büntetőjogi üldözését.

22 — Írásbeli észrevételeinek 36. pontja.

81. Mindenekelőtt tehát kérdéses, hogy az előzetes döntéshozatal iránti kérelemben hivatkozott IP-címek feldolgozása a 95/46 irányelv 3. cikke (2) bekezdésének első franciabekezdésében foglalt kivétel hatálya alá tartozik-e.[23]

1. A 95/46 irányelv alkalmazhatóságáról a vita tárgyát képező adatok feldolgozása tekintetében

82. A Németországi Szövetségi Köztársaság az alapeljárásban látszólag egyszerű internetszolgáltatóként, azaz magánszemélyként (és ezért *sine imperio*) jár el. E tényből következik, hogy elvileg a jelen jogvita tárgyát képező adatok feldolgozása nem tartozik a 95/46 irányelvben foglalt kivételek hatálya alá.

83. A Lindqvist-ítéletben[24] a Bíróság megfogalmazása szerint a 95/46 irányelv 3. cikkének (2) bekezdése szerinti tevékenységek „minden esetben az állam vagy az állami hatóságok sajátos tevékenységei, és nem tartoznak a magánszemélyek tevékenységei közé”.[25] Amennyiben a vita tárgyát képező adatokat olyan személy kezeli, aki hatósági jogállása ellenére valójában magánjogi jogalanyként jár el, a 95/46 irányelv alkalmazandó.

84. A kérdést előterjesztő bíróság a német közigazgatási hatóságok által a dinamikus IP-címek tárolásával elérendő elsődleges cél kiemelésekor hangsúlyozza, hogy célja az „elektronikus médiumai biztonságának és működőképességének biztosítása és fenntartása”; különösen elősegíteni a gyakori „Denial-of-Service” (szolgáltatásmegtagadással járó) támadások felismerését és elhárítását, amely támadások során a távközlési infrastruktúrát önálló webszerverek nagyszámú kéréssel történő célzott és összehangolt elárasztása útján bénítják meg”.[26] A dinamikus IP-címek e célból történő tárolása megszokott a valamennyire jelentős weboldalak minden tulajdonosa számára, és sem közvetlenül, sem közvetve nem jelenti a közhatalom gyakorlását, ezért nem jár túlzott nehézséggel a 95/46 irányelv hatálya alá történő sorolása.

85. A Bundesgerichtshof (szövetségi legfelsőbb bíróság) azonban azt állítja, hogy az alapeljárásban érintett szolgáltatók által a dinamikus IP-címek tárolása büntetőeljárási célnak is eleget tesz, a megfelelő időben az esetleges kibertámadások kitervelői ellen. Vajon e cél elegendő-e ahhoz, hogy kizárjuk az adatfeldolgozást a 95/46 irányelv hatálya alól?

86. Véleményem szerint, ha „büntetőeljárás” alatt az állam büntetőhatalmának az alapeljárás alperesei – vagyis a szolgáltatók – általi gyakorlását kell érteni, akkor „a büntetőjog területén végzett állami tevékenységről”, és így a 95/46 irányelv 3. cikke (2) bekezdésének első franciabekezdésében foglalt kivételről van szó.

87. Ilyen körülmények között a Bíróság által a Huber-ügyben[27] kialakított ítélkezési gyakorlat alapján a személyes adatoknak a szolgáltatók által az elektronikus médiumok biztonsága és általános működőképessége érdekében történő feldolgozása a 95/46 irányelv hatálya alá tartozik, míg az adatoknak a büntetőjog területén végzett állami tevékenység céljából történő feldolgozása nem tartozik az irányelv hatálya alá.

23 — Nem tartoznak a 95/46 irányelv hatálya alá „a közbiztonsággal, a védelemmel, a nemzetbiztonsággal [...], továbbá *a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek*” (az eredeti szövegben kiemelés nélkül szerepel).

24 — A 2003. november 6-i ítélet (C-101/01, EU:C:2003:596), 43. pont.

25 — Szintén e tekintetben: 2008. december 16-i Satakunnan Markkinapörssi és Satamedia ítélet (C-73/07, EU:C:2008:727), 41. pont.

26 — Az előzetes döntéshozatal iránti kérelem előterjesztéséről szóló végzés 36. pontja.

27 — 2008. december 16-i ítélet (C-524/06, EU:C:2008:724), 45. pont.

88. Hasonlóképpen, még ha az úgynevezett büntetőeljárás lefolytatása nem a Németországi Szövetségi Köztársaság mint közhatalmi funkcióval nem rendelkező egyszerű szolgáltató feladata lenne is, hanem csupán – mint bármely magánszemély – a vitatott IP-címeknek a megtorló intézkedések gyakorlására jogosult állami szerv részére történő továbbítására szorítkozna, a dinamikus IP-címek feldolgozása akkor is a 95/46 irányelv hatályán kívül eső tevékenységre irányulna.

89. Ez következik a Parlament kontra Tanács és Bizottság ügyben [28] rögzített ítélkezési gyakorlatból, amelyben a Bíróság megállapította, hogy azon tény, miszerint meghatározott személyes „adatokat gazdasági szereplők kereskedelmi célból gyűjtik, és harmadik államba történő továbbításukat e gazdasági szereplők szervezik meg”, nem jelenti azt, hogy az adattovábbítás „ne tartozna a 95/46 irányelv 3. cikke (2) bekezdése első franciabekezdésének hatálya alá”, ha az adattovábbítás célja a büntetőjog területén végzett állami tevékenységekre irányul, mivel ilyen esetben annak „háttere közhatalmi jellegű és közbiztonsági célú” [29].

90. Ezzel szemben, ha jól gondolom, hogy a „büntetőeljárás” alatt – amint az az előzetes döntéshozatalra utaló végzésből kiderül – azt az eljárást kell érteni, amelyet valamely magánszemély, mint az állam büntetőhatalmának (*ius punendi*) gyakorlására jogosult alany indít a megfelelő keresettel, akkor nem állapítható meg, hogy a dinamikus IP-címek feldolgozásának a büntetőjog területén végzett azon állami tevékenység a célja, amely nem tartozik a 95/46 irányelv hatálya alá.

91. Az ilyen adat tárolása és rögzítése ugyanis csak egy újabb bizonyítási eszközként szolgál, amellyel az internetes honlap tulajdonosa peres félként a jogellenes magatartás megtorlását kéri az államtól. Végeredményben ez a jogrend által a magánszemélyek (a jelen esetben a magánjogi jogrend szerint eljáró állami szerv) tekintetében elismert jogok büntetőjogi védelmének egyik eszközét jelenti. Ebből a szempontból nem különböztetik meg bármely más internetszolgáltató kérelmétől, amelynek célja az állami védelem, a jogrend által megállapított büntetőeljárás keretében megindított eljárások alapján.

92. Következésképpen, amennyiben a német állami szervek közhatalmi funkcióval nem rendelkező internetszolgáltatóként járnak el, amelynek megállapítása a kérdést előterjesztő bíróság feladata, a dinamikus IP-címek személyes adatokként való feldolgozása a 95/46 irányelv hatálya alá tartozik.

2. A kérdés érdeméről

93. A TMG 15. §-ának (1) bekezdése csak akkor engedi meg a felhasználó személyes adatainak gyűjtését és felhasználását, ha ez az elektronikus médium konkrét igénybevételének lehetővé tételéhez és elszámolásához elengedhetetlen. Pontosabban a szolgáltató csak ekkor gyűjthet és használhat fel úgynevezett „használati adatokat”, azaz a felhasználó azon személyes adatait, amelyek „az elektronikus médium konkrét igénybevételének lehetővé tételéhez és elszámolásához” nélkülözhetetlenek. Az adatokat törölni kell a művelet befejeztével (azaz az elektronikus médium konkrét igénybevételének megszűnésével), kivéve, ha az elszámoláshoz meg kell őrizni a TMG 15. §-a (4) bekezdésének rendelkezése szerint.

94. Úgy tűnik, hogy a TMG 15. §-a a kapcsolódás befejeztét követően kizárja azt, hogy a használati adatokat egyéb okok miatt tárolják; ez „az elektronikus médium igénybevételének” általános jellegű biztosítása céljából sem lehetséges. Mivel az adatok tárolását igazoló okként kizárólag elszámolási célokra hivatkozik, a TMG e rendelkezése úgy értelmezhető (bár végső értelmezése a kérdést előterjesztő bíróság feladata), mintha azt követelné meg, hogy a használati adatokat egy konkrét kapcsolat lehetővé tételére alkalmazzák, és töröljék, ha az befejeződik.

28 — 2006. május 30-i ítélet (C-317/04 és C-318/04, EU:C:2006:346), 54–59. pont.

29 — Ugyanott, 59. pont. Olyan személyes adatokról volt szó, amelyek feldolgozása az érintett gazdasági magánszereplők (légitársaságok) üzletét képező szolgáltatások nyújtásához nem volt szükséges, de kötelesek voltak azokat az Egyesült Államok hatóságainak továbbítani a terrorizmus megelőzése és a terrorizmus elleni harc érdekében.

95. A 95/46 irányelv 7. cikkének f) pontja [30] a személyes adatok feldolgozását a TMG 15. §-a szövegének rendelkezéséhez képest (az adatkezelő szempontjából) nagyvonalúbbnak minősíthető értelemben teszi jogszerűvé. A német szabály e tekintetben korlátozóbb jellegűnek minősíthető, mint az uniós szabály, mivel alapvetően nem rendelkezik a szolgáltatás elszámolásához kapcsolódó érdeken kívül egyéb jogos érdek érvényesítéséről, ezáltal internetszolgáltatóként a Németországi Szövetségi Köztársaságnak szintén jogos érdeke fűződhet az internetes honlapjai megfelelő működőképességének biztosításához, az egyes használati kapcsolatokon túlmenően. [31]

96. A Bíróság által az ASNEF és FECEMD ítéletében [32] kifejtett ítélkezési gyakorlat szempontokat ad az előzetes döntéshozatalra előterjesztett második kérdés megválaszolásához. A Bíróság akkor kimondta, hogy a 95/46 irányelv célkitűzéséből „az következik, hogy a 95/46 irányelv 7. cikke kimerítő és korlátozó jellegű felsorolását írja elő azon eseteknek, amelyekben a személyes adatok kezelése jogszerűnek minősíthető”. [33] Ebből következik, hogy „a tagállamok nem alkothatnak a személyes adatok kezelésének megengedhetőségére vonatkozó, a 95/46 irányelv 7. cikkében szereplőkhöz képest új elveket, és olyan további követelményeket sem írhatnak elő, amelyek módosítanák az e cikkben előírt hat elv akár egyikének a hatályát” [34].

97. A TMG 15. §-a a 95/46 irányelv 7. cikkében előírtakat nem egészíti ki további feltétellel az adatfeldolgozás jogszerűségéhez – ahogy ez az ASNEF és FECEMD egyesített ügyekben történt –, [35] de az alapügyben eljáró bíróság által hivatkozott megszorító értelmezés esetén az említett rendelkezés f) pontjában foglalt feltétel veszít tartalmából: ott, ahol az uniós jogalkotó általános jelleggel hivatkozik „az adatkezelő, vagy az adatokat megkapó harmadik fél vagy felek jogszerű érdekének érvényesítésére”, a TMG 15. §-a kizárólag „az elektronikus médium [konkrét] igénybevétele lehetővé tételének és elszámolásának” szükségességét veszi figyelembe.

98. Az ASNEF és FECEMD egyesített ügyekben [36] történtekhez hasonlóan, e nemzeti intézkedés is – ismételten a fent kifejtett megszorító értelmezés esetén – inkább módosítja a 95/46 irányelv 7. cikke szerinti elv terjedelmét, minthogy annak pontosítására szorítkozna, az egyetlen dolog, amellyel kapcsolatban az egyes tagállamok hatóságai bizonyos mértékű mérlegelési mozgástérrel rendelkeznek a 95/46 irányelv 5. cikke alapján.

99. Ez utóbbi rendelkezés szerint ugyanis „a tagállamok, e fejezet rendelkezéseinek korlátai között,[[37]] részletesen meghatározzák, hogy a személyes adatok feldolgozása milyen feltételek mellett jogszerű”. Ahogy azonban azt az ASNEF és FECEMD egyesített ügyekben [38] megállapítást nyert, „[az említett rendelkezés] alapján a tagállamok nem vezethetnek be a személyes adatok kezelésének megengedhetőségére vonatkozó, a 95/46 irányelv 7. cikkében előírtaktól eltérő elveket, és további követelmények által nem módosíthatják a hivatkozott 7. cikkben előírt hat elv akár egyikének hatályát sem”.

30 — Szövege a 17. pontban idézve.

31 — Lásd: 84. pont. Kétségtelen, hogy az internetes honlapok tulajdonosainak jogos érdeke fűződik a szolgáltatásmegtagadás („denials of service”) megelőzéséhez és elhárításához, amelyre a kérdést előterjesztő bíróság hivatkozik, azaz olyan nagyszámú támadásokról van szó, amelyeket alkalmanként célzottan indítanak néhány internetes oldal ellen, hogy azokat elárasszák és működésképtelenné tegyék.

32 — 2011. november 24-i ítélet (C-468/10 és C-469/10, EU:C:2011:777).

33 — Ugyanott, 30. pont.

34 — Ugyanott, 32. pont.

35 — Amely esetben a nemzeti jogalkotó kiegészítette a 95/46 irányelv 7. cikkének f) pontja szerinti követelményeket azzal, hogy a feldolgozás tárgyát képező adatoknak a nyilvánosság számára hozzáférhető forrásokban kell szerepelniük.

36 — 2011. november 24-i ítélet (C-468/10 és C-469/10, EU:C:2011:777).

37 — „A személyes adatok feldolgozásának jogszerűségére vonatkozó általános szabályok” című II. fejezet, amely magában foglalja a 95/46 irányelv 5–21. cikkét.

38 — 2011. november 24-i ítélet (C-468/10 és C-469/10, EU:C:2011:777), 36. pont.

100. A TMG 15. §-a a 95/46 irányelv 7. cikkének f) pontjához képest jelentősen csökkenti az adatfeldolgozás igazolása számára releváns jogos érdek körét, anélkül, hogy azt pontosítania vagy árnyalnia kellene ugyanezen irányelv 5. cikke által biztosított lehetőségek keretében. Egyébként ezt kategorikusan és abszolút módon teszi, anélkül, hogy megengedné, hogy az elektronikus médium általános igénybevételének védelmét és biztosítását mérlegeljék „az érintettnek a 95/46 irányelv 1. cikkének (1) bekezdése értelmében védelmet élvező érdekei vagy alapvető jogai és szabadságai” szempontjából, az irányelv 7. cikke f) pontjának előírása szerint.

101. Végeredményben az ASNEF és FECEMD egyesített ügyhöz hasonlóan,[39] a német nemzeti jogalkotó „[a személyes adatok bizonyos kategóriái] tekintetében végleges módon előírta a súlyozás eredményét, anélkül hogy eltérő eredményt tenne lehetővé az adott eset sajátos körülményei okán”, ezáltal „már nem a 95/46 irányelv 5. cikke [...] értelmében vett pontosításról van szó”.

102. Ilyen körülmények között úgy vélem, hogy a Bundesgerichtshofnak (szövetségi legfelsőbb bíróság) a 95/46 irányelvvel összhangban kell értelmeznie a nemzeti jogszabályokat, ez azt jelenti, hogy: a) az úgynevezett „használati adatok” feldolgozását igazoló okok közé sorolható az elektronikus média szolgáltatónak ezek általános igénybe vételének védelméhez fűződő jogos érdeke és b) az adott esetre vonatkozóan súlyozni lehet a szolgáltató ezen érdekét, összevetve a felhasználó érdekével vagy alapvető jogaival és szabadságaival annak tisztázása érdekében, hogy melyik részesülhet a 95/46 irányelv 1. cikkének (1) bekezdése szerinti védelemben.[40]

103. Véleményem szerint semmi mást nem kell hozzátenni e súlyozás elvégzésének körülményeivel kapcsolatban, amennyiben az megalapozza az előzetes döntéshozatalra történő utalást. A Bundesgerichtshofnak (szövetségi legfelsőbb bíróság) nincs kérdése e tekintetben, de aggódik e súlyozást megelőző kérdés megoldása miatt; azaz hogy az említett mérlegelés elvégezhető-e.

104. Végül feleslegesnek tűnik megjegyezni, hogy az alapeljárásban eljáró bíróság figyelembe veheti a tagállamok által a 95/46 irányelv 13. cikke (1) bekezdésének d) pontjában foglalt felhatalmazás keretében elfogadott esetleges jogi rendelkezéseket az ugyanezen irányelv 6. cikkében előírt kötelezettségek és jogok terjedelmének korlátozására, amennyiben ez szükséges többek között, „[…] a bűncselekmények megelőzésének, nyomozásának, felderítésének és szankcionálásának […]” biztosítása érdekében. A kérdést előterjesztő bíróság sem erre az esetre hivatkozott, bár kétségkívül ismeri mindkét jogszabályt.

105. Következésképpen, az előzetes döntéshozatalra előterjesztett második kérdésre azt a választ javaslom adni, hogy a 95/46 irányelv 7. cikkének f) pontjával nem ellentétes az olyan nemzeti szabály, amelynek értelmezése megakadályozza a szolgáltatót, hogy a felhasználó személyes adatait – a konkrét használat befejeztét követően is – gyűjtse és feldolgozza annak beleegyezése nélkül, az elektronikus média általános működőképességének biztosítása céljából.

VI – **Végkövetkeztetések**

106. A fent kifejtettek alapján azt javaslom a Bíróságnak, hogy az előzetes döntéshozatalra előterjesztett kérdésekre az alábbi válaszokat adja:

„1) A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv 2. cikkének a) pontja alapján az a dinamikus IP-cím, amelyről a felhasználó felkereste valamely elektronikus

39 — Ugyanott, 47. pont.

40 — A tárgyaláson P. Breyer jogi képviselője elutasította, hogy a dinamikus IP-címek tárolása az internetszolgáltatások biztonságos működésének a támadásokkal szembeni védelméhez lenne szükséges. Nem hiszem, hogy teljes mértékben megválaszolható e kérdés, ellenkezőleg, a megválaszolása előtt az egyes konkrét esetekben össze kell vetni az internetes oldal tulajdonosának érdekét és a felhasználók jogait, illetve érdekeit.

médiaszolgáltató internetes honlapját, ez utóbbi szolgáltató szempontjából »személyes adatnak« minősül, amennyiben valamely hálózat-hozzáférést nyújtó szolgáltató birtokában vannak olyan egyéb kiegészítő adatok, amelyek a dinamikus IP-címhez rendelve lehetővé teszik a felhasználó azonosítását.

2) A 95/46 irányelv 7. cikkének f) pontját úgy kell értelmezni, hogy az elektronikus média általános működőképességének biztosítására irányuló célkitűzés főszabály szerint jogos érdeknek minősülhet, amelynek érvényesítése igazolja e személyes adat feldolgozását, amennyiben e célkitűzést az érintett személy érdekéhez vagy alapvető jogaihoz viszonyítva magasabb rendű célnak tekintik. Az olyan nemzeti rendelkezés, amely nem tenné lehetővé e jogos érdek figyelembevételét, összeegyeztethetetlen lenne az említett cikkel.”