Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
MANUELA CAMPOSA SÁNCHEZ-BORDONE,
predstavljeni 12. maja 2016 [1]

Zadeva C-582/14

Patrick Breyer
proti
Bundesrepublik Deutschland(Predlog za sprejetje predhodne odločbe,

ki ga je vložilo Bundesgerichtshof (zvezno vrhovno sodišče, Nemčija))

„Obdelava osebnih podatkov — Direktiva 95/46/ES — Člen 2(a) in člen 7(f) — Pojem ‚osebni podatki' — IP-naslovi — Shranjevanje s strani ponudnika elektronskih storitev — Nacionalna zakonodaja, ki ne dopušča, da bi se upošteval legitimni interes upravljavca"

1. Naslov internetnega protokola (v nadaljevanju: IP-naslov) je zaporedje binarnih številk, ki se dodeli napravi (računalniku, tablici, pametnemu telefonu), s čimer se jo prepozna in se ji omogoči dostop do elektronskega komunikacijskega omrežja. Naprava mora za to, da se poveže v internet, uporabiti številčno zaporedje, ki ga dodelijo ponudniki dostopa do omrežja. IP-naslov se pošlje strežniku, na katerem gostuje obiskana spletna stran.

2. Natančneje, ponudniki dostopa do omrežja (običajno telekomunikacijske družbe) svojim strankam začasno dodelijo tako imenovane „dinamične IP-naslove" ob vsaki vzpostavitvi povezave z internetom in jih spreminjajo ob vsaki poznejši vzpostavitvi povezave. Pri teh družbah se shranjujejo dnevniške datoteke, v katerih je navedeno, kateri IP-naslov je bil dodeljen določeni napravi v vsakem trenutku. [2]

3. Imetniki spletnih strani, do katerih se dostopa prek dinamičnih IP-naslovov, prav tako običajno vodijo dnevniške datoteke, v katerih se beleži, katere strani so bile obiskane, kdaj in s katerega dinamičnega IP-naslova. Te evidence se s tehničnega vidika lahko hranijo časovno neomejeno, ko se prekine internetna povezava posameznega uporabnika.

4. Sam dinamičen IP-naslov ne zadostuje za to, da bi ponudnik storitev identificiral uporabnika njegove spletne strani. Lahko pa ga identificira, če dinamični IP-naslov poveže z drugimi dodatnimi podatki, ki jih ima ponudnik dostopa do omrežja.

1 — Jezik izvirnika: španščina.

2 — Člen 5 Direktive 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, str. 54) je med drugimi obveznostmi nalagal obveznost, da se za namene preiskovanja, odkrivanja in pregona hudih kaznivih dejanj hranijo „datum in čas prijave ter odjave z internetnega dostopa, […] skupaj z IP naslovom, statičn[im] ali dinamičn[im], ki ga je ponudnik dostopa do interneta dodelil komunikaciji, in uporabniško ime naročnika ali registriranega uporabnika".

5. V tem sporu se razpravlja o tem, ali so dinamični IP-naslovi osebni podatek v smislu člena 2(a) Direktive 95/46/ES.[3] Za odgovor je treba najprej ugotoviti, kakšen je v tem smislu pomen tega, da imetnik spletne strani nima na voljo dodatnih podatkov, ki so potrebni za identifikacijo uporabnika, temveč jih ima tretja oseba (v tem primeru ponudnik dostopa do omrežja).

6. Sodišče tega vprašanja še ni obravnavalo, saj je v točki 51 sodbe Scarlet Extended[4] razsodilo, da so IP-naslovi „varovani osebni podatki, saj omogočajo natančno identifikacijo teh uporabnikov“, vendar v okoliščinah, v katerih je IP-naslove zbiral in identificiral ponudnik dostopa do omrežja,[5] ne pa ponudnik vsebin, kakor v obravnavanem primeru.

7. Če bi bili dinamični IP-naslovi za ponudnika storitev po internetu osebni podatki, bi bilo nato treba preučiti, ali njihova obdelava spada na področje uporabe Direktive 95/46.

8. Mogoče je, da čeprav bi ti bili osebni podatki, ne bi uživali varstva, ki ga nudi Direktiva 95/46, če bi se na primer obdelovali zaradi kazenskih postopkov zoper morebitne napadalce spletne strani. V skladu s členom 3(2), prva alinea, Direktive 95/46 se v takem primeru navedena direktiva ne bi uporabila.

9. Poleg tega je treba pojasniti, ali ponudnik storitev, ki beleži dinamične IP-naslove, ko uporabnik dostopi do njegovih spletnih strani (v tej zadevi Zvezna republika Nemčija), deluje kot javni organ ali kot zasebni subjekt.

10. Če bi se uporabila Direktiva 95/46, pa bi bilo treba nazadnje pojasniti, v kolikšnem obsegu je nacionalna zakonodaja, ki omejuje obseg enega od pogojev, določenih v členu 7(f) navedene direktive, zato da utemelji obdelavo osebnih podatkov, združljiva s tem členom 7(f).

I – **Pravni okvir**

A – *Pravo Unije*

11. V uvodni izjavi 26 Direktive 95/46 je navedeno:

„(26) ker se morajo načela varstva uporabljati za vse informacije v zvezi z določeno ali določljivo osebo; ker bi bilo treba za odločitev o tem, ali je oseba določljiva ali ne, upoštevati vsa sredstva, za katera se [razumno] pričakuje, da jih bo uporabil bodisi upravljavec ali katera koli druga oseba za določitev take osebe; ker se načela varstva ne uporabljajo za podatke, ki so spremenjeni v anonimne tako, da posameznik, na katerega se osebni podatki nanašajo, ni več določljiv; ker so pravila ravnanja v smislu člena 27 lahko koristen instrument za usmerjanje k načinom, s katerimi se lahko podatki spremenijo v anonimne in se ohranijo v obliki, v kateri identifikacija posameznika, na katerega se osebni podatki nanašajo, ni več mogoča“.

12. Člen 1 Direktive 95/46 določa:

„1. V skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.

2. Države članice ne omejujejo niti ne prepovedujejo prostega prenosa osebnih podatkov med državami članicami zaradi razlogov, povezanih z varstvom, ki je zagotovljeno na podlagi odstavka 1.“

3 — Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355).

4 — Sodba z dne 24. novembra 2011 (C-70/10, EU:C:2011:771, točka 51).

5 — Tako je bilo tudi v sodbi z dne 19. aprila 2012, Bonnier Audio in drugi (C-461/10, EU:C:2012:219, točki 51 in 52).

13. Člen 2 Direktive 95/46 določa:

„V tej direktivi:

(a) ‚osebni podatek' pomeni katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (‚posameznik, na katerega se nanašajo osebni podatki'); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto;

(b) ‚obdelava osebnih podatkov' (‚obdelava') pomeni kakršen koli postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki z avtomatskimi sredstvi ali brez njih, kakršno je zbiranje, beleženje, urejanje, shranjevanje, prilagajanje ali predelava, iskanje, posvetovanje, uporaba, posredovanje s prenosom, širjenje ali drugo razpolaganje, prilagajanje ali kombiniranje, blokiranje, izbris ali uničenje;

[…]

(d) ‚upravljavec' pomeni fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov; kadar namene in sredstva obdelave določa nacionalna zakonodaja ali zakonodaja Skupnosti, lahko upravljavca ali posebna merila za njegovo imenovanje določi nacionalna zakonodaja ali zakonodaja Skupnosti;

[…]

(f) ‚tretja stranka [oseba]' pomeni katero koli fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki ni posameznik, na katerega se osebni podatki nanašajo, upravljavec, obdelovalec in oseba, ki je pod neposredno oblastjo upravljavca ali obdelovalca pooblaščena za obdelavo podatkov;

[…]"

14. Pod naslovom „Področje uporabe" člen 3 Direktive 95/46 določa:

„1. Ta direktiva se uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatskimi sredstvi in za drugačno obdelavo kakor z avtomatskimi sredstvi za osebne podatke, ki sestavljajo del zbirke ali so namenjeni sestavljanju dela zbirke.

2. Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

— med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI Pogodbe o Evropski uniji, in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,

[…]"

15. Poglavje II Direktive 95/46, ki se nanaša na „Splošna pravila o zakonitosti obdelave osebnih podatkov", se začne s členom 5, v skladu s katerim „[d]ržave članice v mejah določb tega poglavja natančneje določijo pogoje, pod katerimi je obdelava osebnih podatkov zakonita".

16. Člen 6 Direktive 95/46 določa:

„1. Države članice določijo, da morajo biti osebni podatki:

(a) pošteno in zakonito obdelani;

(b) zbrani za določene, izrecne ter zakonite namene in se ne smejo naprej obdelovati na način, ki je nezdružljiv s temi nameni. Nadaljnja obdelava podatkov v zgodovinske, statistične ali znanstvene namene se ne šteje za nezdružljivo, če države članice zagotovijo ustrezne zaščitne ukrepe;

(c) primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo;

(d) točni in po potrebi ažurirani; uporabiti je treba vse primerne ukrepe za zagotovitev, da se podatki, ki so netočni ali nepopolni, zbrišejo ali popravijo, ob upoštevanju namenov, za katere so bili zbrani ali za katere se naprej obdelujejo;

(e) shranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, le toliko časa, kolikor je potrebno za namene, za katere so bili podatki zbrani ali za katere se naprej obdelujejo. Države članice določijo ustrezne zaščitne ukrepe za osebne podatke, shranjene za daljša obdobja za zgodovinsko, statistično ali znanstveno uporabo.

2. Upravljavec mora zagotoviti, da se ravna v skladu z odstavkom 1.“

17. Člen 7 Direktive 95/46 določa:

„Države članice določijo, da se lahko osebni podatki obdelujejo samo, če:

(a) je posameznik, na katerega se osebni podatki nanašajo, nedvoumno dal svojo privolitev; ali

(b) je obdelava potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki, ali pa za izvajanje ukrepov na zahtevo posameznika, na katerega se osebni podatki nanašajo, pred sklenitvijo pogodbe; ali

(c) je obdelava potrebna za skladnost z zakonsko obveznostjo, ki velja za upravljavca; ali

(d) je obdelava potrebna za varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo; ali

(e) je obdelava potrebna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti, dodeljene upravljavcu ali tretji stranki, ki so ji posredovani podatki; ali

(f) je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1).“

18. Člen 13 Direktive 95/46 določa:

„1. Države članice lahko sprejmejo predpise za omejitev obsega obveznosti in pravic, opredeljenih v členih 6(1), 10, 11(1), 12 in 21, kadar taka omejitev predstavlja potrebni ukrep za zaščito:

(a) državne varnosti;

(b) obrambe;

(c) javne varnosti;

(d) preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali kršitve etike za zakonsko urejene poklice;

(e) pomembnega gospodarskega ali finančnega interesa države članice ali Evropske unije, vključno z denarnimi, proračunskimi in davčnimi zadevami;

(f) spremljanja, pregledovanja ali urejanja, povezanega, četudi občasno, z izvajanjem javne oblasti v primerih iz (c), (d) in (e);

(g) posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.

[…]“

B – *Nacionalno pravo*

19. Člen 12 Telemediengesetz (zakon o telekomunikacijskih storitvah, v nadaljevanju: TMG) [6] določa:

„1. Ponudnik storitev lahko osebne podatke zbira in uporabi v zvezi z zagotavljanjem telekomunikacijskih storitev samo, če ta zakon ali drugi predpis, ki se izrecno nanaša na telekomunikacijske storitve, to dopušča ali če je uporabnik v to privolil.

2. Ponudnik storitev lahko osebne podatke, ki se zbirajo zaradi zagotavljanja telekomunikacijskih storitev, za druge namene uporabi samo, če ta zakon ali drugi predpis, ki se izrecno nanaša na telekomunikacijske storitve, to dopušča ali če je uporabnik v to privolil.

3. Če ni določeno drugače, se uporabljajo veljavni predpisi o varstvu osebnih podatkov, tudi v primeru, če ne gre za avtomatizirano obdelavo podatkov.“

20. Člen 15 TMG določa:

„1. Ponudnik storitev lahko osebne podatke uporabnika zbira in uporabi samo, če je to potrebno za omogočanje uporabe telekomunikacijskih storitev in njihovo zaračunavanje (podatki o uporabi). Podatki o uporabi so zlasti:

1° podatki, ki omogočajo identifikacijo uporabnika,

2° podatki o začetku in koncu ter obsegu uporabe in

3° podatki o telekomunikacijskih storitvah, ki jih je uporabnik uporabil.

2. Ponudnik storitev lahko podatke o uporabi različnih telekomunikacijskih storitev uporabnika povezuje, če je to potrebno za namene zaračunavanja storitev uporabniku.

[…]

4. Ponudnik storitev lahko uporabi podatke o uporabi po koncu postopka uporabe, če je to potrebno za namene zaračunavanja storitev uporabniku (obračunski podatki). Zaradi izpolnjevanja obstoječih zakonskih, statutarnih ali pogodbenih rokov hrambe lahko ponudnik storitev podatke blokira. […]“

6 — Zakon z dne 26. februarja 2007 (BGBl 2007 I, str. 179).

21. V skladu s členom 3(1) Bundesdatenschutzgesetz (zvezni zakon o varstvu podatkov, v nadaljevanju: BDSG)[7] so „osebni podatki […] podatki o osebnih ali stvarnih okoliščinah določene ali določljive fizične osebe (posameznik, na katerega se nanašajo osebni podatki). […]“.

II – **Dejansko stanje**

22. P. Breyer je zoper Zvezno republiko Nemčijo vložil tožbo za opustitev beleženja IP-naslovov.

23. Številne nemške javne ustanove imajo javno dostopne spletne portale, na katerih objavljajo aktualne informacije. Zaradi preprečevanja napadov in omogočanja kazenskega pregona napadalcev večina teh portalov shranjuje podatke o vseh dostopih v dnevniških datotekah. V teh datotekah se tudi po koncu postopka uporabe hranijo podatki o imenu datoteke oziroma strani, do katere je dostopil, pojmih, vnesenih v iskalnike, času dostopa, preneseni količini podatkov, podatki o tem, ali je bil dostop uspešen, in IP-naslov kličočega računalnika.

24. P. Breyer, ki je obiskal več takih spletnih strani, je v svoji tožbi predlagal, naj se Zvezni republiki Nemčiji naloži prenehanje beleženja IP-naslova gostujočega sistema, s katerega je dostopal, zase ali za tretje osebe, če to ni potrebno za ponovno vzpostavitev razpoložljivosti telekomunikacijskih storitev v primeru motenj.

25. Tožba P. Breyerja je bila na prvi stopnji zavrnjena. Vendar pa se je njegovi pritožbi delno ugodilo in Zvezni republiki Nemčiji naložilo, naj preneha beleženje po koncu vsakega dostopa. Odredba za prenehanje je bila pogojena s tem, da tožeča stranka med dostopom predloži svoje osebne podatke, tudi v obliki naslova elektronske pošte, in da beleženje ni nujno potrebno za ponovno vzpostavitev razpoložljivosti telekomunikacijskih storitev.

III – **Predlog za sprejetje predhodne odločbe**

26. Ker sta obe stranki vložili revizijo, je šesti senat Bundesgerichtshof (zvezno vrhovno sodišče, Nemčija) 17. decembra 2014 predložilo ti vprašanji za predhodno odločanje:

„1. Ali je treba člen 2(a) Direktive Evropskega parlamenta in Sveta 95/46/ES […] razlagati tako, da naslov internetnega protokola (v nadaljevanju: IP-naslov), ki ga shrani ponudnik storitev pri dostopu do njegove spletne strani, za tega ponudnika pomeni podatek, ki omogoča identifikacijo posameznika, že v primeru, če ima tretja oseba (tukaj: ponudnik dostopa) na voljo dodatne podatke, potrebne za identifikacijo posameznika, na katerega se nanašajo osebni podatki?

2. Ali člen 7(f) Direktive o varstvu podatkov nasprotuje nacionalnemu predpisu, v skladu s katerim lahko ponudnik osebne podatke brez privolitve uporabnika zbira in uporabi samo, če je to potrebno za omogočanje in zaračunavanje konkretnega dostopa do telekomunikacijskih storitev s strani zadevnega uporabnika, in po katerem cilj zagotavljanja splošnega delovanja telekomunikacijskih storitev ne upravičuje uporabe podatkov po koncu postopka uporabe?“

27. Kakor pojasnjuje predložitveno sodišče, bi tožeča stranka v skladu z nemško zakonodajo lahko zahtevala prenehanje beleženja IP-naslovov, če njihova hramba v skladu z zakonodajo o varstvu podatkov pomeni nezakonit poseg v njeno temeljno osebnostno pravico, in sicer pravico do samostojnega odločanja o uporabi osebnih podatkov (člena 1004(1) in 823(1) Bürgerliches Gesetzbuch (nemški civilni zakonik) v povezavi s členoma 1 in 2 Grundgesetz (temeljni zakon)).

7 — Zakon z dne 20. decembra 1990 (BGBl 1990 I, str. 2954).

28. Tako bi bilo, če: (a) IP-naslov (vsekakor skupaj s trenutkom dostopa do spletne strani) pomeni „osebni podatek“ v smislu člena 2(a) v povezavi z uvodno izjavo 26, drugi stavek, Direktive 95/46 oziroma člena 12(1) in (3) TMG v povezavi s členom 3(1) BDSG in (b), če ne bi bil izpolnjen noben primer pooblastila v smislu člena 7(f) Direktive 95/46 oziroma člena 12(1) in (3) in člena 15(1) in (4) TMG.

29. Po mnenju Bundesgerichtshof (zvezno vrhovno sodišče) je za razlago nacionalne zakonodaje (člena 12(1) TMG) nujno ugotoviti, kako je treba razumeti osebno naravo podatkov, na katere se nanaša člen 2(a) Direktive 95/46.

30. Poleg tega sodišče *a quo* navaja, da ker lahko v skladu s členom 15(1) TMG ponudnik storitev osebne podatke uporabnika zbira in uporabi samo, če je to nujno potrebno za omogočanje uporabe telekomunikacijskih storitev in njihovo zaračunavanje (podatki o uporabi),[8] je razlaga tega pojma nacionalnega prava povezana z razlago člena 7(f) Direktive 95/46.

IV – **Postopek pred Sodiščem in trditve strank**

31. Nemška, avstrijska in portugalska vlada ter Komisija so predložile pisna stališča. Samo Komisija in P. Breyer sta se udeležila obravnave 25. februarja 2016, ki se je nemška vlada ni želela udeležiti.

A – *Trditve strank v zvezi s prvim vprašanjem*

32. Po mnenju P. Breyerja so osebni podatki tudi tisti podatki, katerih kombinacija je mogoča zgolj teoretično, to je izhajajoč iz abstraktne potencialne nevarnosti, pri tem pa ni preveč pomembno, ali do te kombinacije v praksi dejansko pride. Po njegovem mnenju to, da je neki subjekt lahko razmeroma nezmožen identificirati neko osebo na podlagi IP-naslova, ne pomeni, da za to osebo ne obstaja nobena nevarnost. Poleg tega meni, da je pomembno dejstvo, da Nemčija hrani njegove podatke o IP, zato da – po potrebi – identificira morebitne napade ali začne kazenski postopek v skladu s členom 113 Telekommunikationsgesetz (zakon o telekomunikacijah), kar se je zgodilo v številnih primerih.

33. Po mnenju nemške vlade je treba na prvo vprašanje odgovoriti nikalno. Po njenem mnenju dinamični IP-naslovi ne razkrivajo „določene“ osebe v smislu člena 2(a) Direktive 95/46. Za ugotovitev, ali razkrivajo podatke o „določeni“ osebi v smislu navedene določbe, bi bilo *določljivost* treba preučiti na podlagi „relativnega“ merila. Tako po njenem mnenju izhaja iz uvodne izjave 26 Direktive 95/46, v skladu s katero je treba upoštevati samo sredstva, za katera „se [razumno] pričakuje“, da jih bo upravljavec ali tretja oseba uporabila za določitev take osebe. Tako pojasnilo naj bi napeljevalo na to, da zakonodajalec Unije na področje uporabe Direktive 95/46 ni želel vključiti tistih položajev, v katerih je identifikacija s strani katere koli tretje osebe objektivno mogoča.

34. Nemška vlada prav tako meni, da je treba pojem „osebni podatki“ v smislu člena 2(a) Direktive 95/46 razlagati glede na namen te direktive, to je zagotoviti spoštovanje temeljnih pravic. Na nujnost varstva fizičnih oseb bi bilo mogoče gledati drugače glede na to, kdo ima podatke in ali ima na voljo sredstva, s katerimi bi te fizične osebe lahko identificiral.

35. Nemška vlada trdi, da P. Breyerja ni mogoče identificirati na podlagi IP-naslovov v povezavi z drugimi podatki, ki jih hranijo ponudniki vsebin. Za to bi bilo treba uporabiti podatke, ki jih imajo ponudniki dostopa do interneta, ki pa jih brez pravne podlage ne morejo posredovati ponudnikom vsebin.

8 — Po mnenju Bundesgerichtshof (zvezno vrhovno sodišče) so podatki o uporabi, ki omogočajo identifikacijo uporabnika, podatki o začetku in koncu ter obsegu uporabe in podatki o telekomunikacijskih storitvah, ki jih je uporabil uporabnik.

36. Avstrijska vlada, nasprotno, meni, da bi moral biti odgovor pritrdilen. V skladu z uvodno izjavo 26 Direktive 95/46 se ne zahteva, da so vsi podatki, ki omogočajo identifikacijo določene fizične osebe, v rokah enega samega subjekta, zato da bi se ta oseba lahko štela za določljivo. Tako naj bi bil IP-naslov lahko osebni podatek, če bi tretja oseba (kot na primer ponudnik dostopa do interneta) imela na voljo sredstva, s katerimi bi lahko identificirala imetnika tega naslova, ne da bi se za to morala pretirano potruditi.

37. Portugalska vlada se tudi nagiba k pritrdilnemu odgovoru, saj meni, da IP-naslov v povezavi z datumom poizvedbe pomeni osebni podatek, ker lahko pripelje do tega, da subjekt, ki ni tisti, ki je shranil IP-naslov, lahko identificira uporabnika.

38. Komisija prav tako predlaga pritrdilen odgovor in se pri tem opira na rešitev, ki jo se sprejelo Sodišče v zadevi Scarlet Extended.[9] Glede na to, da je namen hrambe IP-naslovov ravno identifikacija uporabnikov v primeru kibernetskih napadov, bi po mnenju Komisije uporaba dodatnih podatkov, ki jih beležijo ponudniki dostopa do interneta, pomenila sredstvo, za katero „se [razumno] pričakuje“, da se bo uporabilo, v smislu uvodne izjave 26 Direktive 95/46. Komisija nazadnje meni, da so tako cilj, ki mu sledi ta direktiva, kot tudi člena 7 in 8 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina), v prid široki razlagi člena 2(a) Direktive 95/46.

B – *Trditve strank v zvezi z drugim vprašanjem*

39. P. Breyer meni, da je člen 7(f) Direktive 95/46 splošna določba, ki jo je treba konkretizirati, zato da se lahko uporabi v praksi. V skladu s sodno prakso Sodišča naj bi zato šlo za presojo okoliščin posameznega primera in ugotovitev, ali obstajajo skupine z legitimnim interesom v smislu navedene določbe, pri čemer ne samo, da je določitev posebnih pravil za take skupine dovoljena, temveč je tudi nujno potrebna za uporabo tega člena. V tem primeru bi bila po mnenju P. Breyerja nacionalna zakonodaja skladna s členom 7(f) Direktive 95/46, ker javni portal nima interesa za hranjenje osebnih podatkov oziroma ker ima interes varstva anonimnosti večjo težo. Po njegovem mnenju kljub temu sistematično shranjevanje osebnih podatkov ni združljivo z demokratično družbo niti ni potrebno za zagotavljanje delovanja elektronskih sredstev, ki je popolnoma mogoče brez beleženja teh osebnih podatkov, kakor dokazujejo spletne strani nekaterih zveznih ministrstev, niti ni sorazmerno z njim.

40. Nemška vlada trdi, da drugega vprašanja ni treba obravnavati, saj je bilo zastavljeno samo za primer, če bi bilo treba na prvo vprašanje odgovoriti pritrdilno, kar pa po njenem mnenju iz zgoraj navedenih razlogov ni mogoče.

41. Avstrijska vlada predlaga, naj se odgovori, da Direktiva 95/46 na splošno ne nasprotuje shranjevanju podatkov, kakršni so sporni v postopku v glavni stvari, če bi to bilo nujno potrebno za dobro delovanje elektronskih medijev. Ta vlada meni, da je omejeno shranjevanje IP-naslovov, ki je daljše, kot pa traja obisk spletne strani, lahko zakonito glede na obveznost upravljavca osebnih podatkov, da izvaja ukrepe za zavarovanje teh podatkov, kakor določa člen 17(1) Direktive 95/46. Boj proti kibernetskim napadom lahko upraviči analizo podatkov v zvezi s prejšnjimi napadi in to, da se nekaterim IP-naslovom zavrne dostop do spletne strani. Sorazmernost shranjevanja podatkov, kakršni se obravnavajo v postopku v glavni stvari, z vidika cilja zagotavljanja dobrega delovanja elektronskih sredstev bi bilo treba presojati v vsakem primeru posebej, ob upoštevanju načel, določenih v členu 6(1) Direktive 95/46.

42. Portugalska vlada trdi, da člen 7(f) Direktive 95/46 ne nasprotuje nacionalnim predpisom, ki se obravnavajo v postopku v glavni stvari, saj je nemški zakonodajalec že pretehtal, tako kot določa navedena določba, legitimne interese upravljavca osebnih podatkov na eni strani ter pravice in svoboščine oseb, na katere se navedeni podatki nanašajo, na drugi strani.

9 — Sodba z dne 24. novembra 2011 (C-70/10, EU:C:2011:771, točka 51).

43. Po mnenju Komisije mora nacionalna zakonodaja, ki vključuje člen 7(f) Direktive 95/46, opredeliti cilje obdelave osebnih podatkov, tako da so predvidljivi za zadevnega posameznika. Meni, da nemška zakonodaja ne spoštuje te zahteve, ko v členu 15(1) TMG določa, da je shranjevanje IP-naslovov dovoljeno „če je to potrebno za omogočanje uporabe […] telekomunikacijskih storitev“.

44. Komisija torej predlaga, naj se na drugo vprašanje odgovori, da ta določba nasprotuje razlagi nacionalne določbe, v skladu s katero javni organ, ki deluje kot ponudnik storitev, lahko zbira in uporabi osebne podatke uporabnika brez njegove privolitve, celo če bi bil cilj, ki se uresničuje, zagotavljati dobro splošno delovanje elektronskega sredstva, če navedena nacionalna določba tega cilja ne določa dovolj jasno in natančno.

V – **Presoja**

A – *Prvo vprašanje*

1. Razmejitev zastavljenega vprašanja

45. Glede na to, kako je Bundesgerichtshof (zvezno vrhovno sodišče) oblikovalo prvo od svojih vprašanj za predhodno odločanje, je namen tega vprašanja pojasniti, ali IP-naslov, s katerim se dostopa do spletne strani, za javni subjekt, ki je imetnik te strani, pomeni osebni podatek (v smislu člena 2(a) Direktive 95/46/ES), če ima ponudnik dostopa do omrežja dodatne podatke, ki omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki.

46. Tako oblikovano vprašanje je dovolj natančno, da takoj izključi druga, ki bi se lahko *in abstracto* zastavila o pravni naravi IP-naslovov v okviru varstva osebnih podatkov.

47. Prvič, Bundesgerichtshof (zvezno vrhovno sodišče) se izključno sklicuje na „dinamične IP-naslove“, to so naslovi, ki se začasno dodelijo ob vsaki vzpostavitvi povezave na omrežje in se spreminjajo ob vsaki naknadni povezavi. „Statični IP-naslovi“, za katere je značilno, da se ne spreminjajo in omogočajo stalno identifikacijo naprave, povezane na omrežje, torej niso predmet obravnave.

48. Drugič, predložitveno sodišče izhaja iz domneve, da ponudnik spletne strani v postopku *a quo* z dinamičnim IP-naslovom ne more identificirati oseb, ki obiskujejo njegove stani, niti nima dodatnih podatkov, ki bi skupaj z navedenim IP-naslovom omogočili identifikacijo. Bundesgerichtshof (zvezno vrhovno sodišče) meni, da v tem okviru dinamični IP-naslov *za ponudnika spletne strani* ni osebni podatek v smislu člena 2(a) Direktive 95/46.

49. Dvom predložitvenega sodišča se nanaša na možnost, da bi se dinamični IP-naslov za ponudnika spletne strani opredelil kot osebni podatek, *če ima tretja oseba dodatne podatke*, ki skupaj z navedenim IP-naslovom določijo, kdo obiskuje njegove strani. Vendar, in to je še ena podrobnost, ki je tu pomembna, se Bundesgerichtshof (zvezno vrhovno sodišče) ne sklicuje na katero koli tretjo osebo, ki bi imela dodatne podatke, temveč na ponudnika dostopa do omrežja (kar torej izključuje druge morebitne imetnike takih podatkov).

50. Torej ne gre, med drugim, za to: (a) ali so statični IP-naslovi osebni podatki v skladu z Direktivo 95/46;[10] (b) ali so dinamični IP-naslovi – vselej in v katerih koli okoliščinah – osebni podatki v smislu Direktive 95/46 in, nazadnje, (c) ali je opredelitev dinamičnih IP-naslovov kot osebnih podatkov neizogibna, kakor hitro obstaja tretja oseba, ne glede na to, katera, ki jih lahko uporabi za identifikacijo uporabnikov omrežja.

51. Gre torej zgolj za to, da se ugotovi, ali je dinamičen IP-naslov osebni podatek za ponudnika storitev po internetu, če ima družba za komunikacije, ki ponuja dostop do omrežja (ponudnik dostopa), dodatne podatke, ki skupaj z navedenim naslovom omogočajo identifikacijo osebe, ki dostopa do spletne strani, ki jo upravlja ponudnik storitev po internetu.

2. Vsebinska presoja

52. O vprašanju, ki se zastavlja v tem predlogu za sprejetje predhodne odločbe, se v nemški doktrini in sodni praksi razvneto razpravlja, pri čemer se ta razprava deli na dva pola.[11] Ena stran (ki zagovarja „objektivno“ ali „absolutno“ merilo) zagovarja, da je uporabnik določljiv – in je IP-naslov torej osebni podatek, ki ga je mogoče varovati – če je ne glede na to, kakšne so zmožnosti in sredstva ponudnika storitev po internetu, njegova identifikacija mogoča zgolj s povezavo tega dinamičnega IP-naslova in podatkov, ki jih predloži tretja oseba (na primer ponudnik dostopa do omrežja).

53. Za zagovornike druge strani (ki zastopajo „relativno“ merilo) to, da se računa na pomoč tretje osebe pri končni identifikaciji uporabnika, ne zadostuje, da bi se dinamičen IP-naslov štel za osebni podatek. Pomembna je zmožnost tistega, ki ima dostop do podatka, da ga uporabi s svojimi sredstvi in osebo tako identificira.

54. Ne glede na to, kakšne so okoliščine tega spora v nacionalnem pravu, mora Sodišče svoj odgovor omejiti na razlago dveh določb Direktive 95/46, na kateri so se sklicevali tako sodišče *a quo* kot tudi stranki v postopku, in sicer sta to člen 2(a)[12] in uvodna izjava 26[13] navedene direktive.

10 — Vprašanje, ki ga je Sodišče obravnavalo v sodbah z dne 24. novembra 2011, Scarlet Extended (C-70/10, EU:C:2011:771, točka 51), in z dne 19. aprila 2012, Bonnier Audio in drugi (C-461/10, EU:C:2012:219). V točkah 51 in 52 zadnjenavedene sodbe je Sodišče sklenilo, da posredovanje „imena in naslova […] uporabnika interneta, ki uporablja specifičen IP-naslov, prek katerega naj bi potekala nezakonita izmenjava zaščitenih del, in sicer zaradi identifikacije zadevne osebe, […] pomeni obdelavo osebnih podatkov v smislu člena 2, prvi odstavek, Direktive 2002/58 v povezavi s členom 2(b) Direktive 95/46“.

11 — Glede obeh teoretičnih stališč glej, na primer, Schreibauer, M., v *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., in von Lewinski, K. (ur.), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, 4. izdaja, § 11 Telemediengesetz (od 4 do 10). Nink, J., in Pohle, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze“, v *Multimedia und Recht*, 9/2015, str. od 563 do 567. Heidrich, J., in Wegener, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging“, v *Multimedia und Recht*, 8/2015, str. od 487 do 492. Leisterer, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr“, v *Computer und Recht*, 10/2015, str. od 665 do 670.

12 — Naveden v točki 13.

13 — Navedena v točki 11.

55. Dinamični IP-naslovi že samo zato, ker vsebujejo informacijo o datumu in uri, ko je bila z računalnika (ali druge naprave) obiskana spletna stran, razkrivajo nekatere vzorce vedenja uporabnikov interneta in zato pomenijo potencialen poseg v pravico do zasebnega življenja,[14] ki jo zagotavljata člen 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin ter člen 7 Listine, glede na katera je treba razlagati Direktivo 95/46 (ki jo je treba razlagati tudi glede na člen 8 Listine).[15] Stranke v postopku dejansko ne dvomijo o tej premisi, ki kot taka niti ni predmet predloga za sprejetje predhodne odločbe.

56. Oseba, na katero se navedene podrobnosti nanašajo, ni „določena fizična oseba“. Datum in ura povezave ter numerični naslov ne razkrivajo niti neposredno niti takoj, kdo je fizična oseba, ki je imetnica naprave, s katere je bila spletna stran obiskana, niti identitete uporabnika, ki jo upravlja (lahko je katera koli fizična oseba).

57. Vendar je mogoče dinamičen IP-naslov v obsegu, v katerem pomaga določiti – bodisi sam bodisi skupaj z drugimi podatki – kdo je imetnik naprave, ki je bila uporabljena za dostop do spletne strani, opredeliti kot podatek o „določljivi osebi“.[16]

58. Glede na predlog za sprejetje predhodne odločbe Bundesgerichtshof (zvezno vrhovno sodišče) sam dinamični IP-naslov ne zadostuje za določitev uporabnika, ki je s tega naslova obiskal spletno stran. Če pa bi ponudnik storitev po internetu prek dinamičnega IP-naslova lahko določil uporabnika, bi nedvomno šlo za osebni podatek v smislu Direktive 95/46. Vendar menim, da to ni smisel vprašanja za predhodno odločanje, v katerem je navedeno, da ponudniki storitev po internetu, vpletenih v spor *a quo*, ne morejo določiti uporabnika zgolj na podlagi dinamičnega IP-naslova.

59. V povezavi z drugimi podatki dinamičen IP-naslov omogoča „posredno“ identifikacijo uporabnika, glede česar se vsi strinjajo. Ali možnost, da obstajajo ti dodatni podatki, ki jih je mogoče povezati z dinamičnim IP-naslovom, dovoljuje, da se ta naslov kar tako opredeli kot osebni podatek v smislu Direktive? Ugotoviti je treba, ali v ta namen zadostuje sama abstraktna možnost poznavanja teh podatkov, ali pa morajo biti ti podatki na voljo tistemu, ki že pozna dinamičen IP-naslov, ali tretji osebi.

60. Stranke so svoja stališča osredotočile na razlago uvodne izjave 26 Direktive 95/46, iz vsebine katere izpostavljajo besede „sredstva, za katera se pričakuje, da jih bo uporabil bodisi upravljavec ali katera koli druga oseba za določitev take osebe“. Vprašanje predložitvenega sodišča se ne nanaša na dodatne podatke, ki so na voljo ponudnikom storitve, ki so vpleteni v postopek v glavni stvari. Niti ne namiguje na katero koli tretjo osebo, ki ima te dodatne podatke (ki skupaj z dinamičnim IP-naslovom omogočajo identifikacijo uporabnika), temveč na ponudnika dostopa do omrežja.

14 — Tako je opozoril generalni pravobranilec P. Cruz Villalón v sklepnih predlogih, predstavljenih v zadevi Scarlet Extended (C-70/10, EU:C:2011:255, točka 76), tako pa jo razume tudi Evropski nadzornik za varstvo podatkov v svojih mnenjih z dne 22. februarja 2010 o trenutnih pogajanjih Evropske unije o trgovinskem sporazumu o boju proti ponarejanju (ACTA) (UL 2010, C 147, str. 1, točka 24) in z dne 10. maja 2010 o predlogu direktive Evropskega parlamenta in Sveta o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji, ki razveljavlja Okvirni sklep 2004/68/PNZ (UL 2010, C 323, str. 6, točka 11).

15 — Glej v tem smislu sodbo z dne 20. maja 2003, Österreichischer Rundfunk (C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 68), in sklepne predloge generalne pravobranilke J. Kokott, predstavljene v zadevi Promusicae (C-275/06, EU:C:2007:454, točka 51 in naslednje).

16 — Domnevati je treba, razen če se ne dokaže nasprotno, da je navedena oseba tista, ki je brskala po internetu in vstopila na ustrezno spletno stran. Vendar bi tudi ne glede na to zadnjo domnevo podatek o datumu, uri in numeričnem naslovu dostopa do spletne strani omogočil povezati ta dostop z imetnikom naprave in posredno z vzorci njegovega vedenja po internetu. Mogoče izjeme bi bili IP-naslovi, dodeljeni računalnikom v lokalih, kot so *ciber cafés*, katerih anonimni uporabniki so nedoločljivi in o lastnikih katerih promet, ustvarjen v lokalu, ne ponuja nobenega pomembnega osebnega podatka. To je sicer edina izjema od načela, da so IP-naslovi osebni podatki, ki je za Delovno skupino za varstvo posameznikov pri obdelavi osebnih podatkov, ustanovljeno z Direktivo 95/46 (tako imenovana Skupina iz člena 29), sprejemljiva. Glej njeno Mnenje 4/2007 z dne 20. junija 2007 o pojmu osebnih podatkov, WP 136, na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

61. Torej ni nujno, da v tem primeru Sodišče analizira vsa sredstva, „za katera se [razumno] pričakuje“, da bi jih tožena stranka v postopku *a quo* lahko uporabila, zato da bi bilo dinamične IP-naslove, ki jih ima na voljo, mogoče opredeliti kot osebne podatke. Ker se Bundesgerichtshof (zvezno vrhovno sodišče) sklicuje zgolj na dodatne podatke, ki so v rokah tretje osebe, je mogoče sklepati: (a) bodisi da sama tožena stranka nima dodatnih podatkov, ki omogočajo identifikacijo uporabnika, (b) bodisi da ima te podatke na dosegu, a jih v skladu z uvodno izjavo 26 Direktive 95/46 kot upravljavec teh podatkov ne more razumno uporabiti s tem namenom.

62. Obe možnosti sta odvisni od ugotovitve dejstev, kar pa je naloga zgolj predložitvenega sodišča. Če bi Bundesgerichtshof (zvezno vrhovno sodišče) kakor koli dvomilo o zmožnosti tožene stranke, da razumno uporabi lastne dodatne podatke, bi Sodišče lahko opredelilo splošna merila za razlago besed „sredstva, za katera se [razumno] pričakuje, da jih bo uporabil […] upravljavec“. Ker pa ni tako, bi bilo po mojem mnenju neumestno, če bi Sodišče zdaj opredelilo nekatera merila za razlago, ki niso nujno potrebna predložitvenemu sodišču in za katera niti ni zaprosilo.

63. Jedro vprašanja za predhodno odločanje je torej omejeno na ugotovitev, ali je za opredelitev dinamičnih IP-naslovov kot osebnih podatkov pomembna okoliščina, da ima točno določena tretja oseba – ponudnik dostopa do interneta – na voljo dodatne podatke, ki skupaj s temi naslovi lahko omogočijo identifikacijo uporabnika, ki je obiskal določeno spletno stran.

64. Znova je treba omeniti uvodno izjavo 26 Direktive 95/46. Besede „sredstva, za katera se [razumno] pričakuje, da jih bo uporabil[a] […] *katera koli druga oseba*“ [17] bi lahko pripeljale do razlage, v skladu s katero bi zadostovalo, da bi neka tretja oseba lahko pridobila dodatne podatke (ki bi jih bilo mogoče združiti z dinamičnim IP-naslovom, da bi se identificirala oseba), zato da bi se štelo, da je ta naslov *eo ipso* osebni podatek.

65. Ta maksimalistična razlaga bi v praksi povzročila, da bi se vsakovrstne informacije opredelile kot osebni podatek, tudi če nikakor ne bi zadostovale za identifikacijo uporabnika. Nikoli se ne sme z absolutno gotovostjo zavreči, da ni tretje osebe, ki ima dodatne podatke, ki bi jih bilo mogoče povezati z navedeno informacijo in ki bi torej lahko razkrili identiteto osebe.

66. Menim, da možnost, da napredek tehničnih sredstev v bolj ali manj bližnji prihodnosti očitno tlakuje pot dostopu do orodij za pridobitev in obdelavo podatkov, ki so vedno bolj izpopolnjeni, upravičuje varnostne ukrepe, s katerimi se želi zagotoviti varstvo zasebnosti. Pri opredelitvi pravnih kategorij, ki so pomembne za področje varstva podatkov, se je prizadevalo, da bi se vključili dovolj široki in prožni primeri ravnanja, zato da se pokrijejo vsi mogoči primeri. [18]

67. Vendar menim, da ta skrb – ki je sicer popolnoma legitimna – ne sme pripeljati do tega, da bi se prezrla zakonodajna volja zakonodajalca in da se sistematična razlaga uvodne izjave 26 Direktive 95/46 omeji na „sredstva, za katera se [razumno] pričakuje, da jih bo[do] uporabil[e]“ *določene tretje osebe*.

68. Tako kot se uvodna izjava 26 ne nanaša na katera koli sredstva, ki jih lahko uporabi upravljavec (v tem primeru ponudnik storitev po internetu), temveč samo na tista, za „katera se [razumno] pričakuje“, da jih ta lahko uporabi, je treba tudi razumeti, da se zakonodajalec sklicuje na „tretje osebe“, na katere se lahko *prav tako razumno* obrne upravljavec, ki namerava pridobiti dodatne podatke za identifikacijo. To ne bi bilo tako, če bi bil stik s temi tretjimi osebami dejansko zelo drag z vidika človeških in finančnih virov ali praktično neizvedljiv ali prepovedan z zakonom. Sicer bi bilo, kot sem opozoril

17 — V izvirniku ni v ležečem tisku.

18 — Ta previdnostni in preventivni namen je podlaga za stališče Skupine iz člena 29, po mnenju katere je, kakor sem že navedel, treba izhajati iz načela, da so IP-naslovi osebni podatek, in ki kot edino izjemo priznava primer, v katerem je ponudnik storitve zmožen z absolutno gotovostjo določiti, da gre za naslove, ki pripadajo določljivim osebam, kot so lahko uporabniki *ciber café*. Glej opombo 16, *in fine*.

zgoraj, praktično nemogoče razlikovati med enimi in drugimi sredstvi, saj bi si bilo vedno treba predstavljati možnost obstoja tretje osebe, ki bi – čeprav bi se izkazala za nedosegljivo ponudniku storitev po internetu – lahko imela – zdaj ali v prihodnosti – ustrezne dodatne podatke, ki bi prispevali k identifikaciji uporabnika.

69. Kot sem že navedel, je tretja oseba, na katero se sklicuje Bundesgerichtshof (zvezno vrhovno sodišče), ponudnik dostopa do omrežja. Gotovo je najprimerneje pomisliti na tretjo osebo, na katero se obrne ponudnik storitev, da bi pridobil natančne dodatne podatke, če želi najbolj učinkovito, praktično in neposredno določiti uporabnika, ki je obiskal njegovo spletno stran, na podlagi dinamičnega IP-naslova. Nikakor ne gre za hipotetično, neznano ali nedostopno tretjo osebo, temveč za glavnega protagonista v strukturi interneta, za katerega se z gotovostjo ve, da ima podatke, ki jih ponudnik storitve potrebuje za identifikacijo uporabnika. Kot navaja predložitveno sodišče, gre dejansko za to konkretno tretjo osebo, na katero se namerava obrniti tožena stranka v postopku v glavni stvari, zato da bi pridobila dodatne podatke, ki jih potrebuje.

70. Ponudnik dostopa do interneta je običajno tretja oseba, na katero se nanaša uvodna izjava 26 Direktive 95/46, za katero „se [razumno] pričakuje“, da se bo nanjo obrnil ponudnik storitev v postopku *a quo*. Vendar je treba še pojasniti, ali je mogoče pridobitev dodatnih podatkov, ki jih ima ta tretja oseba, opredeliti kot „razumno“ mogočo ali izvedljivo.

71. Nemška vlada meni, da ker je informacija, ki jo ima ponudnik dostopa do interneta, osebni podatek, je ta ne sme kar tako posredovati, temveč samo v skladu z zakonodajo, ki ureja obdelavo teh podatkov. [19]

72. Nedvomno je tako, saj je treba za uporabo te informacije upoštevati zakonodajo, ki velja za osebne podatke. Informacijo je mogoče „razumno“ pridobiti, če so izpolnjeni pogoji, ki veljajo za dostop do takih podatkov, prvi od katerih je zakonska možnost njihovega shranjevanja in posredovanja drugim. Res je, da ponudnik dostopa do interneta lahko zavrne posredovanje zadevnih podatkov, vendar je mogoče tudi nasprotno. Možnost posredovanja podatkov, ki je popolnoma „razumna“, sama po sebi spremeni dinamičen IP-naslov v osebni podatek za ponudnika internetnih storitev v skladu z navedbami v uvodni izjavi 26 Direktive 95/46.

73. Gre za možnost *v okviru zakona* in je zato „razumna“. Razumna sredstva dostopa, na katera se nanaša Direktiva 95/46, morajo biti po definiciji zakonita sredstva. [20] To je premisa, iz katere seveda izhaja predložitveno sodišče, kakor spomni nemška vlada. [21] Tako se pomembno zmanjšajo pravno pomembne možnosti dostopa, saj morajo biti izključno zakonite. Vendar medtem ko te obstajajo, kljub temu da lahko zelo omejujejo praktično uporabljivost, predpostavljajo „razumno sredstvo“ v smislu Direktive 95/46.

74. Zato menim, da je treba na prvo vprašanje, kakor ga je zastavilo Bundesgerichtshof (zvezno vrhovno sodišče), odgovoriti pritrdilno. Dinamičen IP-naslov je treba za ponudnika storitev po internetu opredeliti kot osebni podatek glede na obstoj tretje osebe (ponudnik dostopa do omrežja), na katero se lahko razumno obrne, da bi pridobil druge dodatne podatke, ki skupaj z navedenim naslovom omogočajo identifikacijo uporabnika.

19 — Točki 40 in 45 njenega pisnega stališča.

20 — V tem okviru ni pomembno, da bi bil dostop do osebnega podatka *de facto* mogoč s kršitvijo zakonov o varstvu podatkov.

21 — Točki 47 in 48 njenega pisnega stališča.

75. Menim, da izid, do katerega bi pripeljala rešitev, drugačna od te, ki jo predlagam, še okrepi to rešitev. Če dinamični IP-naslovi ne bi bili osebni podatek za ponudnika storitev po internetu, bi jih ta lahko hranil neomejeno in bi lahko od ponudnika dostopa do interneta kadar koli zahteval dodatne podatke, da bi jih združil z navedenim naslovom in identificiral uporabnika. V teh okoliščinah, kakor priznava nemška vlada,[22] bi se dinamičen IP-naslov spremenil v osebni podatek, če bi že imel dodatne veljavne podatke za identifikacijo uporabnika, ki bi se uporabili v skladu z zakonodajo o varstvu podatkov.

76. Torej bi šlo za podatek, katerega shranjevanje bi bilo zgolj mogoče, če se do takrat ne bi obravnaval kot osebni podatek za ponudnika storitev. Zato je pravna opredelitev dinamičnega IP-naslova kot osebnega podatka v rokah tega ponudnika odvisna od možnosti, da se bo enkrat v prihodnosti odločil, da ga uporabi za identifikacijo uporabnika, tako da ga bo združil z dodatnimi podatki, ki jih bo moral pridobiti od tretje osebe. Vendar menim, da je glede na Direktivo 95/46 odločilna – razumna – možnost obstoja „dostopne“ tretje osebe, ki ima potrebna sredstva, na podlagi katerih lahko identificira osebo, in ne to, da se možnost zaprositi to tretjo osebo za pomoč udejanji.

77. Mogoče bi bilo dopustiti celo, kakor zagovarja nemška vlada, da se dinamičen IP-naslov spremeni v osebni podatek takoj, ko ga ponudnik dostopa do interneta prejme. Vendar bi bilo torej treba sprejeti, da bi glede na datum shranjevanja IP-naslova šlo za opredelitev z retroaktivnim učinkom, in ga posledično, ker ga ne bi bilo, če bi se čas, v katerem se je lahko shranil, iztekel, ne bi bilo mogoče že od začetka opredeliti kot osebni podatek. Te okoliščine bi lahko pripeljale do izida, ki bi nasprotoval namenu zakonodaje o varstvu osebnih podatkov. Razlog, ki upravičuje zgolj začasno shranjevanje teh podatkov, bi bil izkrivljen v primeru morebitne pozne ugotovitve prednosti, ki jo imajo od začetka: njihove zmožnosti, da sami ali skupaj z drugimi podatki omogočijo identifikacijo fizične osebe. Zaradi čiste ekonomije jim je tudi iz tega razloga primerneje pripisati to lastnost od samega začetka.

78. Zato v okviru prvega predloga menim, da je treba člen 2(a) Direktive 95/46 razlagati tako, da IP-naslov, ki ga shrani ponudnik storitev pri dostopu do njegove spletne strani, za tega ponudnika pomeni osebni podatek, če ponudnik dostopa do omrežja (interneta) razpolaga z dodatnimi podatki, ki omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki.

B – *Drugo vprašanje*

79. Z drugim od vprašanj za predhodno odločanje Bundesgerichtshof (zvezno vrhovno sodišče) želi izvedeti, ali člen 7(f) Direktive 95/46 nasprotuje nacionalni zakonodaji, ki dopušča samo zbiranje in uporabo osebnih podatkov uporabnika brez njegove privolitve, če je to potrebno za omogočanje in zaračunavanje konkretne uporabe telekomunikacijskih storitev s strani zadevnega uporabnika, ne da bi cilj zagotavljanja splošnega delovanja telekomunikacijskih storitev lahko upravičil uporabo teh podatkov po koncu postopka uporabe.

80. Preden odgovorim, moram pojasniti informacijo, ki jo je predložilo Bundesgerichtshof (zvezno vrhovno sodišče), v skladu s katero se sporni podatki shranjujejo, zato da se zagotovi dobro delovanje spletnih strani, ki se obravnavajo v postopku v glavni stvari, in se po potrebi omogoči kazenski pregon kibernetskih napadov, katerih predmet so lahko te spletne strani.

81. Zato se je treba predvsem vprašati, ali obdelava IP-naslovov, na katere se nanaša predlog za sprejetje predhodne odločbe, spada v izjemo, predvideno v členu 3(2), prva alinea, Direktive 95/46.[23]

22 — Točka 36 njenega pisnega stališča.

23 — Na področje uporabe Direktive 95/46 ne spadajo „postopki obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo […] in pri *dejavnostih države na področju kazenskega prava*“ (v izvirniku ni v ležečem tisku).

1. Uporaba Direktive 95/46 za obdelavo spornih podatkov

82. V postopku v glavni stvari Zvezna republika Nemčija deluje, tako se zdi, zgolj kot ponudnik storitev po internetu, to pomeni kot zasebni subjekt (in torej *sine imperio*). Iz tega dejstva je mogoče sklepati, da obdelava podatkov, ki je predmet tega spora, načeloma ni izključena s področja uporabe Direktive 95/46.

83. Kakor se je izrazilo Sodišče v sodbi Lindqvist [24], so dejavnosti iz člena 3(2) Direktive 95/46 „v vseh primerih dejavnosti, značilne za države ali državne organe in nepovezane s področjem dejavnosti posameznikov“. [25] Direktiva 95/46 se uporabi v obsegu, v katerem obravnavane podatke obdeluje nekdo, ki kljub temu, da je javni organ, dejansko deluje kot zasebni subjekt.

84. Predložitveno sodišče izpostavlja glavni namen, ki mu sledi nemška uprava z beleženjem dinamičnih IP-naslovov, in poudarja, da je namen „zagotavljanje in ohranitev zanesljivega izvajanja njihovih telekomunikacijskih storitev“; zlasti prispevanje k „odkrivanju in odvračanju pogostih napadov „denial of service“), pri katerih se onesposobi telekomunikacijska infrastruktura s ciljnim in koordiniranim napadom na posamezne spletne strežnike v obliki velikega povpraševanja“. [26] Shranjevanje dinamičnih IP-naslovov s tem namenom je skupno vsakemu imetniku pomembnih spletnih strani in niti neposredno niti posredno ne pomeni izvajanja javne oblasti, zaradi česar njegova vključitev na področje uporabe Direktive 95/46 ne pomeni pretirane težave.

85. Vendar Bundesgerichtshof (zvezno vrhovno sodišče) trdi, da ponudniki storitev, ki se obravnavajo v postopku v glavni stvari, shranjujejo dinamične IP-naslove tudi z namenom, da se v primernem trenutku sproži kazenski postopek proti avtorjem morebitnih kibernetskih napadov. Ali ta namen zadostuje za to, da se obdelava teh podatkov izključi s področja uporabe Direktive 95/46?

86. Menim, da če se s „kazenskim postopkom“ razume to, da ponudniki storitve, ki so tožene stranke v postopku v glavni stvari, izvajajo *ius puniendi* države, se znajdemo pred „dejavnostmi države na področju kazenskega prava“ in torej pred eno od izjem, predvidenih v členu 3(2), prva alinea, Direktive 95/46.

87. V teh okoliščinah bi v skladu s sodno prakso Sodišča v zadevi Huber [27] obdelava osebnih podatkov s strani ponudnikov storitev zaradi varnosti in tehničnega delovanja njihovih telekomunikacijskih storitev spadala na področje uporabe Direktive 95/46, medtem ko obdelava podatkov zaradi dejavnosti države na kazenskem področju tja ne bi spadala.

88. Na enak način, čeprav za sam kazenski postopek ne bi odgovarjala Zvezna republika Nemčija, ki je zgolj ponudnica storitev, ki ne deluje oblastno, temveč bi tako kot kateri koli zasebni subjekt zgolj posredovala sporne IP-naslove državnemu organu, pristojnemu za izvajanje kazenskega pregona, bi bil namen obdelave dinamičnih IP-naslovov prav tako dejavnost, ki je izključena s področja uporabe Direktive 95/46.

24 — Sodba z dne 6. novembra 2003 (C-101/01, EU:C:2003:596, točka 43).

25 — V istem smislu sodba z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia (C-73/07, EU:C:2008:727, točka 41).

26 — Točka 36 predložitvenega sklepa.

27 — Sodba z dne 16. decembra 2008 (C-524/06, EU:C:2008:724, točka 45).

89. Tako izhaja iz sodne prakse, ustaljene z zadevo Parlament/Svet in Komisija,[28] v kateri je Sodišče potrdilo, da dejstvo, da so nekatere osebne podatke „zbrali zasebni subjekti za ekonomske namene in da jih ti prenesejo v tretjo državo“, ne pomeni, da ta prenos „ne spada na področje uporabe“ člena 3(2), prva alinea, Direktive 95/46, če je namen prenosa dejavnost države na kazenskem področju in če v tem primeru prenos „spada v okvir, ki ga določijo javni organi, in se nanaša na javno varnost“.[29]

90. Nasprotno, mislim, da če je treba glede na to, kar je mogoče razbrati iz predložitvenega sklepa, s „kazenskim postopkom“ razumeti postopanje posameznika kot subjekta, ki ima aktivno legitimacijo za izvajanje *ius puniendi* države z ustreznim dejanjem, torej ni mogoče trditi, da je namen obdelave dinamičnih IP-naslovov dejavnost države na kazenskem področju, ki je izključena s področja uporabe Direktive 95/46.

91. Shranjevanje in beleženje tega podatka naj bi bila namreč namenjena kot še eno dokazno sredstvo več, s katerim lahko imetnik spletne strani državi predlaga pregon nezakonitega ravnanja na predlog stranke. Nazadnje naj bi bil instrument, s katerim se po kazenski poti varujejo pravice, ki jih pravni red priznava zasebnemu subjektu (v tem primeru javnemu subjektu, ki deluje v okviru zasebnega prava). S tega vidika se ne razlikuje od pobude katerega koli drugega ponudnika storitev po internetu, ki išče varstvo države v skladu s postopki kazenskega pregona, določenimi v pravnem redu.

92. Zato v obsegu, v katerem nemška uprava ravna kot ponudnica storitev po internetu in pri tem ne izvaja javne oblasti, o čemer mora presojati predložitveno sodišče, spada obdelava dinamičnih IP-naslovov kot osebnih podatkov na področje uporabe Direktive 95/46.

2. Vsebinska presoja

93. Člen 15(1) TMG zgolj dovoljuje zbiranje in uporabo osebnih podatkov, če je to nujno potrebno za omogočanje in zaračunavanje konkretne uporabe telekomunikacijske storitve. Natančneje, ponudnik storitev lahko zbira in uporabi samo tako imenovane „podatke o uporabi“, torej osebne podatke uporabnika, ki so nujno potrebni, da se omogoči „uporaba telekomunikacijskih storitev in njihovo zaračunavanje“. Te podatke je treba izbrisati, kakor hitro se postopek uporabe konča (to je, ko se konkretna uporaba telekomunikacijske storitve konča), razen če se obdržijo „za namene zaračunavanja“ v skladu z določbo odstavka 4 člena 15 TMG.

94. Ko je povezava enkrat prekinjena, člen 15 TMG očitno izključi možnost, da bi se podatki o uporabi shranjevali iz drugih razlogov; niti za splošno zagotavljanje „uporabe telekomunikacijskih storitev“. S tem ko se ta določba TMG sklicuje izključno na namene zaračunavanja kot razlog za shranjevanje podatkov, jo je mogoče razumeti (čeprav je za njeno dokončno razlago pristojno predložitveno sodišče), kot da zahteva, da se podatki o uporabi uporabijo samo zato, da omogočijo konkretno povezavo in da se zbrišejo, ko se povezava konča.

28 — Sodba z dne 30. maja 2006 (C-317/04 in C-318/04, EU:C:2006:346, točke od 54 do 59).

29 — *Ibidem*, točka 59. Nanašala se je na osebne podatke, katerih obdelava ni bila nujna za opravljanje storitev, ki so bile dejavnost zadevnih zasebnih gospodarskih subjektov (letalskih družb), vendar ki so jih bili ti zavezani posredovati organom Združenih držav zaradi preprečevanja terorizma in boja proti njemu.

95. Člen 7(f) Direktive 95/46[30] dovoljuje obdelavo osebnih podatkov pod pogoji, ki bi jih opredelil kot bolj velikodušne (za upravljavca) od tistih, ki so določeni v členu 15 TMG. V tem primeru je mogoče nemški določbi očitati, da je bolj omejujoča kot določba Unije, saj načeloma ne upošteva drugega legitimnega interesa, ki ni povezan z zaračunavanjem storitve, čeprav bi Zvezna republika Nemčija kot ponudnica storitev po internetu tudi lahko imela legitimen interes zagotavljati dobro delovanje svojih spletnih strani, kar presega samo vzpostavitev povezave.[31]

96. Sodna praksa Sodišča v sodbi ASNEF in FECEMD[32] daje smernice za odgovor na drugo vprašanje za predhodno odločanje. Sodišče je tej zadevi potrdilo, da iz cilja, ki mu sledi Direktiva 95/46, „izhaja […], da je v členu 7 Direktive 95/46 določen izčrpen in taksativen seznam primerov, v katerih je mogoče šteti, da je obdelava osebnih podatkov dopustna“.[33] Nato pa je navedlo, da „države članice ne smejo niti dodati novih načel glede zakonitosti obdelave osebnih podatkov iz člena 7 Direktive 95/46 niti določiti dodatnih zahtev, ki bi spreminjale obseg enega od šestih načel, določenih v tem členu“.[34]

97. Člen 15 TMG ne dodaja nove zahteve k tistim, ki so določene v členu 7 Direktive 95/46, zato da bi bila obdelava podatkov zakonita – kakor se je zgodilo v zadevah ASNEF in FECEMD –[35]vendar če se razlaga ozko, na kar namiguje sodišče *a quo*, zoži vsebino pogoja, določenega v točki (f) navedene določbe: kjer se zakonodajalec Unije na splošno sklicuje na „[…] zakonite interese, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani“, naj bi člen 15 TMG zgolj navajal potrebo, da „se omogoči [konkretna] uporaba in zaračunavanje telekomunikacijskih storitev“.

98. Tako kot v zadevah ASNEF in FECEMD[36] bi tudi v tem primeru nacionalni ukrep – ponovno, če bi se razlagal ozko, kot je bilo pojasnjeno zgoraj – spremenil obseg načela iz člena 7 Direktive 95/46, ne pa zgolj natančneje opredelil, kar je edino, za kar imajo v skladu s členom 5 Direktive 95/46 organi vsake države članice določeno polje proste presoje.

99. V skladu z zadnjenavedeno določbo namreč „[d]ržave članice v mejah določb tega poglavja[37] natančneje določijo pogoje, pod katerimi je obdelava osebnih podatkov zakonita“. Vendar, kakor je bilo potrjeno v zadevah ASNEF in FECEMD,[38] „na podlagi [navedene določbe] države članice ne smejo dodati drugih načel glede zakonitosti obdelave osebnih podatkov, kot so tista iz člena 7 te direktive, niti z dodatnimi zahtevami spremeniti obsega šestih načel, določenih v navedenem členu 7“.

100. Člen 15 TMG bi glede na člen 7(f) Direktive 95/46 bistveno zožil obseg legitimnega interesa, ki je pomemben za utemeljitev obdelave podatkov, ne da bi to podrobneje opredelil ali pojasnil v okviru tega, kar je dovoljeno s členom 5 navedene direktive. Poleg tega naj bi to storil kategorično in absolutno, ne da bi dopustil, da sta lahko varstvo in zagotavljanje splošne uporabe telekomunikacijske storitve predmet tehtanja „temeljn[ih] pravic[…] in svoboščin[…] posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1)“ Direktive 95/46, kakor določa člen 7(f) te direktive.

30 — Navedena v točki 17.

31 — Glej točko 84. Res je, da imajo imetniki spletnih strani legitimen interes, da preprečujejo in se borijo proti zavrnitvam storitve („denials of service“), ki jih omenja predložitveno sodišče, to so množični napadi, ki se občasno usklajeno izvedejo proti nekaterim spletnim stranem, da jih prenasitijo s podatki in ohromijo.

32 — Sodba z dne 24. novembra 2011 (C-468/10 in C-469/10, EU:C:2011:777).

33 — *Ibidem*, točka 30.

34 — *Ibidem*, točka 32

35 — Primer, v katerem je nacionalna zakonodaja k zahtevam člena 7(f) Direktive 95/46 dodala zahtevo, da morajo biti podatki, ki so predmet obdelave, v javno dostopnih virih.

36 — Sodba z dne 24. novembra 2011 (C-468/10 in C-469/10, EU:C:2011:777).

37 — Poglavje II z naslovom „Splošna pravila o zakonitosti obdelave osebnih podatkov“, ki zajema člene od 5 do 21 Direktive 95/46.

38 — Sodba z dne 24. novembra 2011 (C-468/10 in C-469/10, EU:C:2011:777, točka 36).

101. Nazadnje in enako kot v zadevah ASNEF in FECEMD [39] naj bi nemški zakonodajalec določil „dokončno […] izid tehtanja nasprotujočih si pravic in interesov [v zvezi z določenimi kategorijami osebnih podatkov], ne da bi omogočal drugačen izid zaradi posebnih okoliščin konkretnega primera“, tako da „[n]e gre pa za natančnejšo določitev v smislu […] člena 5“ Direktive 95/46.

102. V teh okoliščinah menim, da je Bundesgerichtshof (zvezno vrhovno sodišče) dolžno razlagati nacionalno zakonodajo v skladu z Direktivo 95/46, kar pomeni: (a) da je med razloge, ki utemeljujejo obdelavo tako imenovanih „podatkov o uporabi“, mogoče vključiti legitimen interes ponudnika telekomunikacijskih storitev, zato da se zavaruje splošna uporaba teh storitev, in (b) da je mogoče ta interes ponudnika storitve pretehtati *ad casum* ter ga primerjati z interesom ali pravicami in temeljnimi svoboščinami uporabnika, zato da se ugotovi, kateri interes je treba varovati v skladu s členom 1(1) Direktive 95/46. [40]

103. Menim, da ni treba dodati ničesar več o pogojih, pod katerimi je treba to tehtati v primeru, ki je bil povod za predlog za sprejetje predhodne odločbe. Glede tega Bundesgerichtshof (zvezno vrhovno sodišče) ni zastavilo nobenega vprašanja, saj se zavzema za rešitev vprašanja, ki je predhodno tej presoji na podlagi tehtanja, in sicer ali je tako presojo mogoče izvesti.

104. Nazadnje se mi zdi odveč navesti, da sodišče *a quo* lahko upošteva morebitne zakonske določbe, ki jih sprejme država članica v okviru pooblastila, podeljenega s členom 13(1)(d) Direktive 95/46, za omejitev obsega obveznosti in pravic, opredeljenih v členu 6 te direktive, če bi bila taka omejitev potrebna za zaščito, med drugimi dobrinami, „[…] preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj […]“. Predložitveno sodišče ne omenja niti tega primera, saj se nedvomno zaveda obstoja obeh členov.

105. Zato predlagam, da se na drugo vprašanje za predhodno odločanje odgovori, da člen 7(f) Direktive 95/46 nasprotuje nacionalni določbi, katere razlaga preprečuje ponudniku storitev, da zbira in obdeluje osebne podatke uporabnika brez njegove privolitve z namenom zagotavljanja delovanja telekomunikacijske storitve po koncu vsakega postopka uporabe.

VI – **Predlog**

106. Glede na vse zgoraj predstavljeno Sodišču predlagam, naj na vprašanji za predhodno odločanje odgovori:

1. V skladu s členom 2(a) Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov dinamičen IP-naslov, prek katerega je uporabnik dostopil do spletne strani ponudnika telekomunikacijskih storitev, za zadnjenavedenega pomeni „osebni podatek“, če ima ponudnik dostopa do omrežja druge dodatne podatke, ki skupaj z dinamičnim IP-naslovom omogočajo identifikacijo uporabnika.

2. Člen 7(f) Direktive 95/46 je treba razlagati tako, da se cilj zagotavljanja delovanja telekomunikacijske storitve lahko načeloma šteje za legitimni interes, ki upravičuje obdelavo tega osebnega podatka, pri čemer je treba presoditi, ali prevlada nad interesom ali temeljnimi pravicami zadevne osebe. Nacionalna določba, v skladu s katero ni mogoče upoštevati tega legitimnega interesa, ni v skladu z navedenim členom.

39 — *Ibidem*, točka 47.

40 — Na obravnavi je zagovornik P. Breyerja izpodbijal, da bi bilo beleženje dinamičnih IP-naslovov nujno za varstvo dobrega delovanja internetnih storitev pred morebitnimi napadi. Menim, da ni mogoče dati absolutnega odgovora na to vprašanje, za katerega rešitev je, nasprotno, treba najprej v vsakem posameznem primeru tehtati med interesom imetnika spletne strani ter pravicami in interesi uporabnikov.