Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
MANUELA CAMPOSA SÁNCHEZ-BORDONE
od 12. svibnja 2016.[1]

Predmet C-582/14

Patrick Breyer
protiv
Savezne Republike Njemačke

(zahtjev za prethodnu odluku koji je uputio Bundesgerichtshof (Savezni vrhovni sud, Njemačka))

„Obrada osobnih podataka – Direktiva 95/46/EZ – Članak 2. točka (a) i članak 7. točka (f) – Značenje izraza ‚osobni podaci' – IP adrese – Pohrana pružatelja usluga elektroničkih medija – Nacionalno zakonodavstvo koje ne dopušta uzimanje u obzir legitimnog interesa kojem teži nadzornik"

1. Adresa internetskog protokola (u daljnjem tekstu: IP adresa) niz je binarnih brojeva koji su dodijeljeni određenom uređaju (računalo, tablet, pametni telefon) i koji ga identificiraju i omogućuju mu pristup na mrežu elektroničkih komunikacija. Kako bi uređaj pristupio na internet, mora se koristiti numeričkim nizom koji pribavljaju pružatelji usluga pristupa na mrežu. IP adresa prenosi se na poslužitelj, gdje se pohranjuje mrežna stranica koja se pregledava.

2. Osobito, pružatelji usluga pristupa mreži (najčešće telefonske kompanije) dodjeljuju svojim klijentima privremene, tzv. dinamičke IP adrese za svako spajanje na internet, a koje se mijenjaju prilikom naknadnih spajanja. Te kompanije vode registar u kojem se navodi koju su IP adresu dodijelile u određenom trenutku određenom uređaju[2].

3. Vlasnici mrežnih stranica kojima se pristupa putem dinamičkih IP adresa uobičavaju voditi registre u kojima se navodi koje su se stranice posjetile, kada i s koje dinamičke IP adrese. Nakon što se prekine korisnikova internetska veza, ti se registri tehnički mogu pohraniti bez vremenskog ograničenja.

4. Dinamička IP adresa sama po sebi nije dovoljna da bi pružatelj usluga identificirao korisnika svoje mrežne stranice. Međutim, moći će to učiniti ako kombinira dinamičku IP adresu s ostalim, dodatnim podacima koji se nalaze u posjedu pružatelja usluga pristupa mreži.

1 — Izvorni jezik: španjolski

2 — Članak 5. Direktive 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (SL 2006., L 105, str. 54.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 50., str. 30.) propisivao je, među ostalim, u svrhu istrage, otkrivanja i progona teških kaznenih djela, obvezu da se zadrži „datum i vrijeme prijave i odjave od usluge pristupa internetu […] zajedno s adresom IP-a, bilo da je dinamička ili statička, koju je komunikaciji dodijelio pružatelj usluge pristupa internetu, te korisničko ime pretplatnika ili registriranog korisnika".

5. Predmet spora je pitanje jesu li dinamičke IP adrese osobni podatak u smislu članka 2. točke (a) Direktive 95/46/EZ[3]. Prije odgovora na to pitanje potrebno je odrediti koji značaj ima činjenica da dodatni podaci nisu u posjedu vlasnika mrežne stranice, već treće osobe (konkretno, pružatelja usluga pristupa mreži).

6. Riječ je o novom pitanju za Sud, koji je u točki 51. presude Scarlet Extended[4] utvrdio da su IP adrese „zaštićeni osobni podaci jer omogućuju identifikaciju korisnika", ali u kontekstu u kojem je prikupljanje i identifikaciju IP adresa provodio pružatelj pristupa mreži[5], a ne pružatelj sadržaja, kao što je to sada slučaj.

7. Ako dinamičke IP adrese za pružatelja usluga interneta predstavljaju osobne podatke, tada bi, posljedično, trebalo ispitati je li obrada tih podataka u dosegu područja primjene Direktive 95/46.

8. Moguće je da je riječ o osobnim podacima, ali da oni ne uživaju zaštitu prema Direktivi 95/46, ako je, primjerice, svrha njihove obrade provođenje kaznenog postupka protiv eventualnih napadača na mrežnu stranicu. U takvom se slučaju Direktiva 95/46, na temelju članka 3. stavka 2. podstavka 1., ne primjenjuje.

9. Osim toga, potrebno je razjasniti nastupa li pružatelj usluga koji registrira dinamičke IP adrese kada korisnik pristupi njegovim mrežnim stranicama (u ovom slučaju Savezna Republika Njemačka) kao javna vlast ili kao privatna osoba.

10. Ako bi bila primjenjiva Direktiva 95/46, tada bi, konačno, bilo potrebno precizirati do koje je mjere s njezinim člankom 7. točkom (f) spojiv nacionalni propis koji ograničava doseg nekog njezina uvjeta radi opravdanja obrade osobnih podataka.

I – **Pravni okvir**

A – *Pravo Unije*

11. Uvodna izjava 26. Direktive 95/46 glasi kako slijedi:

„(26) budući da se načela zaštite moraju primjenjivati na sve podatke u vezi s utvrđenim osobama ili osobama koje se mogu utvrditi; budući da je, kako bi se utvrdilo može li se osobu utvrditi, potrebno uzeti u obzir sva sredstva koja nadzornik ili bilo koja druga osoba može opravdano [razumno] koristiti da utvrdi navedenu osobu; budući da se načela zaštite ne primjenjuju na podatke koji su anonimni na takav način da se osoba čiji se podaci obrađuju više ne može utvrditi; budući da pravila ponašanja u smislu članka 27. ove Direktive mogu biti korisni instrument za davanje uputa u vezi s načinom na koji se podaci mogu napraviti anonimnima i zadržati u obliku u kojem utvrđivanje identiteta osobe čiji se podaci obrađuju više nije moguća".

12. Na temelju članka 1. Direktive 95/46:

„1. U skladu s ovom Direktivom, države članice štite temeljna prava i slobode fizičkih osoba, a posebno njihova prava na privatnost u vezi s obradom osobnih podataka.

3 — Direktiva Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.)

4 — Presuda od 24. studenog 2011. (C-70/10, EU:C:2011:771), t. 51.

5 — Isto se dogodilo u presudi od 19. travnja 2012., Bonnier Audio i dr. (C-461/10, EU:C:2012:219), t. 51. i 52.

2. Države članice ne ograničavaju ni zabranjuju slobodni prijenos osobnih podataka između država članica iz razloga povezanih sa zaštitom osiguranom u stavku 1. ovog članka."

13. Prema članku 2. Direktive 95/46:

„U smislu ove Direktive:

a) ‚osobni podaci' znači bilo koji podaci koji se odnose na utvrđenu fizičku osobu ili fizičku osobu koju se može utvrditi (‚osoba čiji se podaci obrađuju'); osoba koja se može utvrditi je osoba čiji je identitet moguće utvrditi, izravno ili neizravno, a posebno navođenjem identifikacijskog broja ili jednog ili više činitelja značajnih za njegov fizički, fiziološki, mentalni, gospodarski, kulturni ili socijalni identitet;

b) ‚obrada osobnih podataka' (‚obrada') znači bilo koji postupak ili skup postupaka koji se provode nad osobnim podacima, bilo automatskim putem ili ne, kao što je prikupljanje, snimanje, organiziranje, pohrana, prilagođavanje ili mijenjanje, vraćanje, obavljanje uvida, uporaba, otkrivanje prijenosom i širenjem ili stavljanje na raspolaganje drugim načinom, poravnavanje ili kombiniranje, blokiranje, brisanje ili uništavanje;

[…]

d) ‚nadzornik' znači fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo koje samo ili zajedno s drugima utvrđuje svrhu i načine obrade osobnih podataka; kada su svrha i načini obrade utvrđeni nacionalnim zakonodavstvom ili pravom Zajednice, nadzornik ili posebna mjerila za njegovo imenovanje mogu se utvrditi nacionalnim zakonodavstvom ili pravom Zajednice;

[…]

f) ‚treća strana' znači bilo koja fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo osim osobe čiji se podaci obrađuju, nadzornika, obrađivača i osoba koje su na temelju izravne ovlasti nadzornika ili obrađivača ovlaštene obrađivati podatke;

[…]".

14. Naslovljen „Područje primjene", članak 3. Direktive 95/46 glasi:

„1. Ova Direktiva se primjenjuje na osobne podatke koji se u cijelosti ili djelomično obrađuju automatskim putem i na obradu podataka koja nije automatska, a koja čini dio sustava arhiviranja ili će činiti dio sustava arhiviranja.

2. Ova se Direktiva ne primjenjuje na obradu osobnih podataka:

— tijekom aktivnosti koja je izvan područja primjene prava Zajednice, kao što je predviđeno u glavama V. i VI. Ugovora o Europskoj uniji i u svakom slučaju na postupke obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se operacija obrade odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava,

[…]".

15. Drugo poglavlje Direktive 95/46, pod nazivom „Opća pravila o zakonitosti obrade osobnih podataka", započinje člankom 5., u kojem se navodi da „države članice u granicama odredbi ovog poglavlja podrobno utvrđuju uvjete pod kojima je obrada podataka zakonita".

16. Na temelju članka 6. Direktive 95/46:

„1. Države članice osiguravaju da su osobni podaci;

(a) obrađeni pošteno i zakonito;

(b) prikupljeni u posebne, izričite i zakonite svrhe te da ih se dalje ne obrađuje na način koji bi bio nespojiv s tom svrhom. Daljnja obrada podataka u povijesne, statističke ili znanstvene svrhe ne smatra se nespojivom pod uvjetom da ta država članica osigura odgovarajuću zaštitu;

(c) prikladni, relevantni i da nisu pretjerani u odnosu na svrhu zbog koje se prikupljaju i/ili dalje obrađuju;

(d) točni i, po potrebi, dopunjeni; potrebno je poduzeti sve odgovarajuće mjere da se podaci koji su netočni ili nepotpuni izbrišu ili isprave, uzimajući u obzir svrhu zbog koje se prikupljaju ili zbog koje se dalje obrađuju;

(e) čuvani u obliku koji omogućava identifikaciju osoba čiji se podaci obrađuju samo tijekom razdoblja potrebnog u svrhe zbog kojih se podaci prikupljaju ili zbog kojih se dalje obrađuju. Države članice dužne su predvidjeti odgovarajuću zaštitu za pohranu osobnih podataka za duža razdoblja ili za povijesnu, statističku ili znanstvenu uporabu.

2. Nadzornik mora osigurati postupanje u skladu sa stavkom 1. ovog članka.”

17. Na temelju članka 7. Direktive 95/46:

„Države članice osiguravaju da se osobni podaci mogu obrađivati jedino ako:

(a) je osoba čiji se podaci obrađuju nedvosmisleno dala svoju suglasnost; ili

(b) je obrada potrebna za izvršavanje ugovora kojem je osoba čiji se podaci obrađuju stranka ili kako bi se poduzele mjere na zahtjev osobe čiji se podaci obrađuju prije sklapanja ugovora; ili

(c) je obrada potrebna za sukladnost sa zakonskom obvezom kojoj nadzornik podliježe; ili

(d) je obrada potrebna kako bi se zaštitili vitalni interesi osobe čiji se podaci obrađuju; ili

e) je obrada potrebna za izvršavanje zadatka koji se provodi zbog javnog interesa ili pri izvršavanju javne ovlasti koju ima nadzornik ili treća strana kojoj se podaci otkrivaju; ili

(f) je obrada potrebna u svrhe zakonitog interesa kojeg ima nadzornik ili treća strana ili strane kojima se podaci otkrivaju, osim kada su ti podaci podređeni interesu za temeljna prava i slobode osobe čiji se podaci obrađuju koja zahtijeva zaštitu na temelju članka 1. stavka 1. ove Direktive.”

18. Na temelju članka 13. Direktive 95/46:

„1. Države članice mogu donijeti propise za ograničavanje područja primjene obveza i prava iz članka 6. stavka 1., članka 10., članka 11. stavka 1. te članka 12. i 21. ove Direktive kada takvo ograničavanje predstavlja potrebne mjere za zaštitu:

(a) nacionalne sigurnosti;

(b) obrane;

(c) javne sigurnosti;

(d) sprečavanja, istrage, otkrivanja i progona kaznenih djela ili kršenja etike zakonom uređenih djelatnosti;

(e) važnoga gospodarskog ili financijskog interesa države članice ili Europske unije, uključujući novčana, proračunska i porezna pitanja;

(f) nadzora, inspekcije ili regulatorne funkcije povezane, čak i povremeno, s izvršavanjem javnih ovlasti u slučajevima iz točke (c), (d) i (e);

(g) zaštite osobe čiji se podaci obrađuju ili prava i slobode drugih.

[…]”

B – *Nacionalno pravo*

19. Odredba članka 12. Telemediengesetza (Zakon o informacijskim uslugama i elektroničkoj komunikaciji; u daljnjem tekstu: TMG) [6] propisuje:

„1. Pružatelj usluga smije prikupljati i koristiti se osobnim podacima radi pružanja telekomunikacijskih usluga samo u mjeri u kojoj je to dopušteno ovim zakonom ili ostalim propisima koji se izričito odnose na navedene usluge ili u kojoj je korisnik dao suglasnost.

2. Pružatelj usluga smije se koristiti osobnim podacima u ostale svrhe radi pružanja telekomunikacijskih usluga samo u mjeri u kojoj je to dopušteno ovim zakonom ili ostalim propisima koji se izričito odnose na navedene usluge ili u kojoj je korisnik dao suglasnost.

3. Ako nije drukčije propisano, odredbe o zaštiti osobnih podataka primijenit će se čak i ako se osobni podaci ne obrađuju na automatski način.”

20. Na temelju članka 15. TMG-a:

„1. Pružatelj usluga smije prikupljati i upotrebljavati osobne podatke korisnika samo kada je to potrebno radi omogućavanja korištenja i obračuna telekomunikacijskih usluga (podaci o korištenju). Podacima o korištenju posebno se smatraju:

1. ° identifikacijski podaci korisnika,

2. ° podaci o početku, završetku i opsegu korištenja i

3. ° podaci o telekomunikacijskim uslugama kojima se korisnik koristio.

2. Pružatelj usluga smije kombinirati podatke o korištenju različitih telekomunikacijskih usluga pojedinog korisnika kad god je to potrebno za obračun usluga.

[…]

4. Nakon završetka korištenja, pružatelj usluga moći će se koristiti podacima kad je to potrebno u svrhu ispostave računa korisniku (podaci o obračunu). Radi poštovanja zakonskih, statutarnih i ugovornih rokova, pružatelj usluga smije blokirati podatke. [...]”.

6 — Zakon od 26. veljače 2007. (BGBl 2007. I, str. 179.)

21. Na temelju članka 3. stavka 1. Bundesdatenschutzgesetza (Savezni zakon o zaštiti podataka; u daljnjem tekstu: BDSG)[7], „osobni podaci su konkretni podaci o osobnim ili stvarnim okolnostima određene ili odredive fizičke osobe (osoba čiji se podaci obrađuju). [...]”.

II – **Činjenice**

22. P. Breyer podnio je tužbu protiv Savezne Republike Njemačke radi prestanka vođenja registra IP adresa.

23. Velik broj njemačkih javnih institucija ima internetske portale dostupne javnosti na kojima nude ažurirane informacije. Kako bi spriječili napade i omogućili kazneni progon napadača, većina portala pohranjuje sav pristup u obliku zbirki podataka ili registara o protokolu. U njima čuvaju, čak i nakon završetka operacije, ime zbirke podataka ili zahtijevane stranice, podatke upisane u poljima tražilica, trenutak spajanja, količinu prenesenih podataka, podatak o uspješnosti spajanja i IP adresu računala s kojeg je učinjeno.

24. P. Breyer, koji je posjetio neke od navedenih stranica, u svojoj tužbi protiv Savezne Republike zahtijevao je da joj se naloži da izravno ili putem treće strane obriše IP adresu iz *host* sustava s kojeg je pristup zatražen, pod uvjetom da nije potrebna radi ponovnog uspostavljanja veze u slučaju pogreške.

25. Tužba P. Breyera odbijena je u prvostupanjskom postupku. Međutim, njegova je žalba djelomično prihvaćena te je Saveznoj Republici naložen prestanak pohranjivanja podataka nakon prestanka svake radnje pristupa. Nalog o prestanku pohranjivanja podataka uvjetovan je time da korisnik tijekom operacije pristupa mreži dâ svoje osobne podatke, uključujući u obliku adrese elektroničke pošte, i da registriranje nije neophodno za ponovnu uspostavu telekomunikacijske usluge.

III – **Postavljeno pitanje**

26. Nakon žalbe u kasacijskom postupku koju su podnijele obje strane, VI. vijeće Bundesgerichtshofa (Savezni vrhovni sud, Njemačka) postavilo je ova prethodna pitanja koja su upućena 17. prosinca 2014.:

„1. Treba li članak 2. točku (a) Direktive 95/46/EZ […] tumačiti na način da adresa internetskog protokola (IP adresa) koju pružatelj usluga pohranjuje prilikom pristupa na svoju internetsku stranicu za njega već tada predstavlja osobni podatak ako treća osoba (ovdje: pružatelj pristupa) raspolaže dodatnim informacijama potrebnima za identifikaciju osobe na koju se one odnose?

2. Protivi li se članku 7. točki (f) Direktive o zaštiti podataka propis nacionalnog prava prema kojem pružatelj usluga može prikupljati i koristiti osobne podatke korisnika bez njegova dopuštenja samo u dijelu u kojem je to potrebno kako bi omogućio i obračunao konkretno korištenje elektroničkih medija dotičnog korisnika i prema kojem svrha osiguravanja općeg funkcioniranja elektroničkih medija ne može opravdati korištenje podataka nakon završetka dotičnog postupka korištenja?”

27. Kako to pojašnjava sud koji je uputio zahtjev, tužitelj bi na temelju njemačkog prava mogao tražiti prestanak pohranjivanja IP adresa ako pohrana predstavlja nezakonito miješanje u opće pravo osobnosti u skladu s propisima o zaštiti podataka, a osobito u njegovo pravo na „informativno samoodređenje” (članak 1004. stavak 1. i članak 823. stavak 1. Bürgerliches Gesetzbucha (njemački Građanski zakonik), u vezi s člankom 1. i 2. Grundgesetza (Osnovni zakon)).

7 — Zakon od 20. prosinca 1990. (BGBl 1990. I, str. 2954.)

28. To bi bilo tako: a) ako bi se IP adresa (u svakom slučaju zajedno s trenutkom pristupa mrežnoj stranici) mogla definirati kao „osobni podatak" u smislu članka 2. točke (a), u vezi s drugom rečenicom uvodne izjave 26. Direktive 95/46, ili u smislu članka 12. stavaka 1. i 3. TMG-a, u vezi s člankom 3. stavkom 1. BDSG-a, i b) ako to ne bi bilo dopušteno u smislu članka 7. točke (f) Direktive 95/46 ili u smislu članka 12. stavaka 1. i 3. te članka 15. stavaka 1. i 4. TMG-a.

29. Bundesgerichtshof (Savezni vrhovni sud) smatra da je u svrhu tumačenja nacionalnog prava (članka 12. stavka 1. TMG-a) prethodno neizbježno razumjeti što se smatra osobnim podacima na koje se referira članak 2. točka (a) Direktive 95/46.

30. Osim toga, sud *a quo* navodi da na temelju članka 15. stavka 1. TMG-a pružatelj usluga isključivo smije prikupljati i koristiti se osobnim podacima korisnika kada je to nužno za omogućavanje korištenja i obračuna telekomunikacijskih usluga (podaci o korištenju) [8], a tumačenje te interne odredbe vezano je uz tumačenje članka 7. točke (f) Direktive 95/46.

IV – **Postupak pred Sudom. Navodi stranaka**

31. Njemačka, austrijska i portugalska vlada te Europska komisija podnijele su svoja pisana očitovanja. Samo je ta institucija, uz P. Breyera, pristupila na raspravu 25. veljače 2016., dok je njemačka vlada odbila pristupiti.

A – *Navodi stranaka u vezi s prvim pitanjem*

32. Prema P. Breyeru, osobni su podaci i oni čija je kombinacija moguća jedino u teoriji, dakle počevši od potencijalne apstraktne opasnosti, pri čemu nije odlučujuće je li se kombinacija i ostvarila. Smatra da to što određeno tijelo relativno nije u mogućnosti identificirati konkretnu osobu na osnovi IP adrese ne znači da ne postoji opasnost za tu osobu. Inače smatra relevantnom činjenicu da Njemačka pohranjuje njegove IP podatke u svrhu eventualne identifikacije napada ili pokretanja kaznenih postupaka, što je dopušteno člankom 133. Telekommunikationsgesetza (Zakona o telekomunikacijama), a što se dogodilo u velikom broju slučajeva.

33. Njemačka vlada smatra da se na prvo pitanje mora odgovoriti negativno. Drži da IP adrese ne otkrivaju „utvrđenu" osobu u smislu članka 2. točke (a) Direktive 95/46. U svrhu određivanja daju li one informaciju o osobi „koja se može utvrditi", u smislu tog istog pravila, provjera *mogućnosti utvrđivanja* mora se izvršiti s pomoću „relativnog" kriterija. To prema njezinu mišljenju proizlazi iz uvodne izjave 26. Direktive 95/46, prema kojoj se moraju uzeti u obzir jedino sredstva koja su podložna „razumnom" korištenju od nadzornika ili treće strane u svrhu identifikacije pojedinca. Takvim bi se utvrđenjem pokazalo da zakonodavac Unije nije želio u područje primjene Direktive 95/46 uključiti one situacije u kojima je identifikacija objektivno moguća od bilo koje treće strane.

34. Njemačka vlada također smatra da se, u smislu članka 2. točke (a) Direktive 95/46, pojam „osobni podaci" mora tumačiti u svjetlu cilja Direktive, dakle zaštite temeljnih prava. Potreba zaštite fizičkih osoba može se razumjeti na različit način ovisno o tome tko posjeduje podatke i raspolaže li ili ne sredstvima koja bi mu poslužila za njihovu identifikaciju.

35. Njemačka vlada smatra da se P. Breyera ne može identificirati s pomoću IP adresa kombiniranih s ostalim podacima koje pohranjuju pružatelji sadržaja. Za tako nešto potrebno je raspolagati podacima kojima raspolažu pružatelji pristupa internetu, koji, u nedostatku pravnog temelja, te podatke ne smiju dostaviti pružateljima sadržaja.

8 — Prema Bundesgerichtshofu (Savezni vrhovni sud), podaci o korištenju su identifikacijski podaci korisnika, podaci o početku i završetku upotrebe i njezinu opsegu te oni koji se odnose na telekomunikacijske usluge kojima se korisnik koristio.

36. S druge strane, austrijska vlada smatra da odgovor treba biti potvrdan. U skladu s uvodnom izjavom 26. Direktive 95/46, da bi se utvrdilo može li se osobu utvrditi, nije potrebno da se svi njezini identifikacijski podaci nalaze u posjedu jednog subjekta. Na taj način, pojedinačna IP adresa mogla bi biti osobni podatak ako treća osoba (primjerice, pružatelj pristupa internetu) raspolaže sredstvima kojima bi mogla identificirati njezina vlasnika bez nerazmjernog napora.

37. Portugalska vlada također naginje potvrdnom odgovoru i smatra da IP adresa u kombinaciji s datumom sesije predstavlja osobni podatak u mjeri u kojoj može dovesti do identifikacije korisnika od osobe koja je pohranila IP adresu.

38. Komisija također predlaže potvrdan odgovor oslanjajući se na usvojeno rješenje Suda u predmetu Scarlet Extended [9]. Budući da pohranjivanje IP adresa služi upravo za identifikaciju korisnika u slučaju kibernetičkih napada, upotreba dodatnih podataka koje registriraju pružatelji pristupa internetu za Komisiju predstavlja sredstvo koje se može „razumno" koristiti u smislu uvodne izjave 26. Direktive 95/46. Naposljetku, Komisija smatra da cilj koji se nastoji postići Direktivom kao i članci 7. i 8. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja) potiču široko tumačenje članka 2. točke (a) Direktive 95/46.

B – *Navodi stranaka u vezi s drugim pitanjem*

39. P. Breyer smatra da članak 7. točka (f) Direktive 95/46 predstavlja opće pravilo čija praktična primjena nalaže konkretiziranje. U skladu s ustaljenom sudskom praksom Suda, potrebno je utvrditi okolnosti u pojedinom slučaju i odrediti postoje li skupine s legitimnim interesom u smislu navedenog pravila, uzimajući u obzir da ne samo da su dopuštena specifična pravila već i da ih je nužno predvidjeti za takve skupine radi primjene tog članka. U takvom bi slučaju i za P. Breyera nacionalni propis bio u skladu s člankom 7. točkom (f) Direktive 95/46 jer ne postoji interes javnog portala da pohrani osobne podatke ili zato što prevaguje interes zaštite anonimnosti. Prema njegovu mišljenju, međutim, sustavna pohrana nije prikladna demokratskom društvu niti je potrebna ni proporcionalna radi osiguranja funkcioniranja elektroničkih medija, koje je potpuno moguće bez registriranja osobnih podataka, kao što to pokazuju slučajevi mrežnih stranica nekih saveznih ministarstava.

40. Njemačka vlada smatra da nije potrebno da razmotri drugo pitanje jer se ono postavlja isključivo u hipotetskom slučaju da je na prvo pitanje odgovoreno potvrdno, što prema njezinu mišljenju nije slučaj iz gore navedenih razloga.

41. Austrijska vlada predlaže odgovor prema kojem se Direktivi 95/46 općenito ne protivi ideja pohrane spornih podataka iz glavnog postupka, kada je to nužno za osiguranje dobrog funkcioniranja elektroničkih medija. Ta vlada smatra da ograničena pohrana IP adresa nakon razdoblja pregleda mrežne stranice može biti zakonita s obzirom na obvezu nadzornika da primijeni zaštitne mjere koje propisuje članak 17. stavak 1. Direktive 95/46. Borba protiv kibernetičkih napada može opravdati analizu podataka koji se odnose na prijašnje napade i zabranu pristupa određenoj internetskoj stranici nekim IP adresama. Proporcionalnost pohrane podataka poput onih iz glavnog postupka, s gledišta svrhe osiguranja dobrog funkcioniranja elektroničkih medija, trebala bi se utvrditi od slučaja do slučaja i uzimajući u obzir načela iz članka 6. stavka 1. Direktive 95/46.

42. Portugalska vlada zastupa stajalište da se članku 7. točki (f) Direktive 95/46 ne protive nacionalni propisi na koje se odnosi glavni postupak jer je njemački zakonodavac već proveo odgovarajuće vrednovanje legitimnih interesa nadzornika, s jedne strane, i prava i sloboda osoba na koje se ti podaci odnose, s druge strane, kao što je to predviđeno navedenom odredbom.

9 — Presuda od 24. studenoga 2011. (C-70/10, EU:C:2011:771), t. 51.

43. Komisija smatra da nacionalni propis kojim je prenesen članak 7. točka (f) Direktive 95/46 mora definirati svrhe obrade podataka na način da su predvidljive za osobu čiji se podaci obrađuju. Prema njezinu shvaćanju, njemački propis ne poštuje taj zahtjev kada u članku 15. stavku 1. TMG-a propisuje da se pohrana IP adresa dopušta onda „kada je to potrebno radi omogućavanja korištenja […] telekomunikacijskih usluga”.

44. Komisija na drugo pitanje predlaže odgovoriti da se toj odredbi protivi tumačenje nacionalnog propisa prema kojem javno tijelo koje djeluje kao pružatelj usluga može prikupiti i koristiti se osobnim podacima korisnika bez njegove suglasnosti, pa i ako je namjeravana svrha osiguranje pravilnog općeg funkcioniranja elektroničkog medija, ako navedeni nacionalni propis ne određuje tu svrhu na dovoljno jasan i precizan način.

V – **Ocjena**

A – *Prvo pitanje*

1. Određivanje opsega postavljenog pitanja

45. S obzirom na to kako je Bundesgerichtshof (Savezni vrhovni sud) formulirao prethodna pitanja, prvo od njih nastoji rasvijetliti predstavlja li IP adresa, s pomoću koje se pristupa mrežnoj stranici, za javno tijelo koje je vlasnik te stranice osobni podatak (u smislu članka 2. točke (a) Direktive 95/46/EZ), ako pružatelj pristupa na mrežu posjeduje dodatne podatke koji omogućavaju identifikaciju konkretne osobe.

46. Tako postavljeno pitanje dovoljno je precizno da se od početka ne nameću druga pitanja koja bi se mogla pojaviti *in abstracto* u vezi s pravnom prirodom IP adresa u kontekstu zaštite osobnih podataka.

47. Kao prvo, Bundesgerichtshof (Savezni vrhovni sud) se referira isključivo na „dinamičke IP adrese”, koje se privremeno dodjeljuju za svaki pojedini pristup mreži i koje se mijenjaju prilikom svakog idućeg pristupa. Stoga „fiksne ili statičke IP adrese”, čija je osobina da su nepromjenjive i omogućavaju stalnu identifikaciju uređaja koji je pristupio na mrežu, ostaju po strani.

48. Kao drugo, sud koji je uputio zahtjev polazi od presumpcije da pružatelj mrežne stranice nije u postupku *a quo* u mogućnosti putem dinamičke IP adrese identificirati korisnike koji posjećuju njegove stranice niti raspolaže sam po sebi dodatnim podacima koji bi kombinirani s IP adresom omogućili njihovu identifikaciju. Čini se da Bundesgerichtshof (Savezni vrhovni sud) smatra da u tom kontekstu dinamička IP adresa ne predstavlja osobni podatak u smislu članka 2. točke (a) Direktive 95/46, *za pružatelja mrežne stranice*.

49. Dvojba suda koji je uputio zahtjev vezana je uz mogućnost da se dinamička IP adresa u odnosu na pružatelja mrežne stranice definira kao osobni podatak *ako treća osoba raspolaže dodatnim informacijama* koje u kombinaciji s njom identificiraju one koji posjećuju njegove mrežne stranice. Svakako je važno napomenuti da Bundesgerichtshof (Savezni vrhovni sud) ne upućuje ni na koju treću stranu posjednika dodatnih podataka, već isključivo na pružatelja pristupa mreži (isključuje, dakle, ostale moguće posjednike podataka te vrste).

50. Na taj način nisu predmet rasprave, među ostalim, i sljedeća pitanja; a) jesu li statičke IP adrese osobni podatak u smislu Direktive 95/46[10], b) smatraju li se dinamičke IP adrese uvijek i u svim uvjetima osobnim podacima u smislu te direktive i, konačno, c) je li kvalifikacija dinamičkih IP adresa kao osobnih podataka neizbježna ako je bilo koja treća strana u stanju koristiti se tim podacima radi identifikacije korisnika na mreži.

51. Radi se, dakle, jedino o odluci predstavlja li dinamička IP adresa osobni podatak za pružatelja usluge interneta, kada telekomunikacijska kompanija koja nudi uslugu pristupa mreži (pružatelj pristupa) raspolaže dodatnim podacima koji u kombinaciji s takvom adresom omogućuju identifikaciju korisnika koji pristupa mrežnoj stranici kojom upravlja navedeni pružatelj usluga.

2. O meritumu

52. Pitanje koje se postavlja u ovom zahtjevu za prethodnu odluku u njemačkoj doktrini i sudskoj praksi predmet je intenzivne rasprave u kojoj su se polarizirala dva različita mišljenja[11]. Prema jednom (koje zastupa „objektivni" ili „apsolutni" kriterij), korisnika je moguće identificirati, čime se IP adresa smatra osobnim podatkom koji je potrebno zaštititi, ako ga je moguće identificirati samo na osnovi kombinacije dinamičke IP adrese i podataka koje drži treća strana (primjerice, pružatelj pristupa mreži), bez obzira na sposobnosti i sredstva koja posjeduje pružatelj usluga interneta.

53. Za zastupnike druge struje (koji zastupaju „relativni" kriterij) mogućnost računanja na pomoć treće strane prilikom identificiranja korisnika nije dovoljna da bi se dinamička IP adresa smatrala osobnim podatkom. Relevantna je sposobnost onoga tko posjeduje podatak da se njime posluži putem vlastitih sredstava u svrhu identifikacije konkretnog korisnika.

54. Bez obzira na kontekst ove kontroverze u nacionalnom pravu, odgovor Suda mora se ograničiti na tumačenje dviju odredbi Direktive 95/46 na koje su ciljali sud *a quo* i stranke u postupku, odnosno njezin članak 2. točku (a)[12] i njezinu uvodnu izjavu 26.[13].

55. Dinamičke IP adrese, već zbog činjenice pružanja informacija o datumu i satu pristupa mrežnoj stranici s određenog računala (ili drugog uređaja), upućuju na određene načine ponašanja internetskih korisnika i time podrazumijevaju potencijalno miješanje u pravo na privatnost[14], koje je zajamčeno člankom 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda i člankom 7. Povelje, u čijem je svjetlu, zajedno s njezinim člankom 8., potrebno tumačiti Direktivu 95/46[15]. U stvari, stranke u postupku ne preispituju ovu tvrdnju i ona kao takva nije ni predmet prethodnog pitanja.

10 — Problem koji je Sud riješio u presudama od 24. studenoga 2011., Scarlet Extended (C-70/10, EU:C:2011:771), t. 51. i od 19. travnja 2012., Bonnier Audio i dr. (C-461/10, EU:C:2012:219). U točkama 51. i 52. potonje Sud je zaključio da komunikacija „u svrhu identifikacije, imena i adrese […] konkretnog internetskog korisnika koji se koristi IP adresom s koje su se navodno na nezakonit način razmjenjivali podaci koji sadržavaju zaštićena djela […] predstavlja obradu osobnih podataka u smislu članka 2. stavka 1. Direktive 2002/58, u vezi s člankom 2. točkom (b) Direktive 95/46".

11 — U vezi s obama doktrinalnim stajalištima vidjeti, primjerice, Schreibauer, M., *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P. i von Lewinski, K. (izd.), Carl Heymanns Verlag/Wolters Kluwer, Koeln, 2014., 4. izd., § 11 Telemediengesetz (4. do 10.). Nink, J., y Pohle, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze", u *Multimedia und Recht*, 9/2015, str. 563. do 567. Heidrich, J., y Wegener, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging", u *Multimedia und Recht*, 8/2015, str. 487. do 492. Leisterer, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr", u *Computer und Recht*, 10/2015, str. 665. do 670.

12 — Navedeno u točki 13.

13 — Navedeno u točki 11.

14 — Na to je podsjetio nezavisni odvjetnik Cruz Villalón u mišljenju u predmetu Scarlet Extended (C-70/10, EU:C:2011:255), t. 76., a tako je to shvatio i europski nadzornik za zaštitu podataka u odlukama od 22. veljače 2010., u vezi s pregovorima koje vodi Europska unija o Trgovačkom sporazumu protiv krivotvorenja (ACTA) (SL 2010., C 147, str. 1., t. 24.), i od 10. svibnja 2010. o prijedlogu Direktive Europskog parlamenta i Vijeća o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije te o zamjeni Okvirne odluke Vijeća 2004/68/PUP (SL 2010., C 323, str. 6, t. 11.).

15 — Vidjeti u tom smislu presudu od 20. svibnja 2003., Österreichischer Rundfunk (C-465/00, C-138/01 i C-139/01, EU:C:2003:294), t. 68. i mišljenje nezavisne odvjetnice Kokott u predmetu Promusicae (C-275/06, EU:C:2007:454), t. 51. i sljedeće.

56. Osoba na koju se odnose navedene pojedinosti nije „identificirana fizička osoba”. Datum i sat pristupa kao i brojčani izvor pristupa ne otkrivaju izravno ni trenutačno osobu kojoj pripada uređaj s kojeg je posjećena mrežna stranica niti identitet korisnika koji njime upravlja (može biti bilo koja fizička osoba).

57. Međutim, u mjeri u kojoj dinamička IP adresa pomaže odrediti, bilo sama ili zajedno s drugim podacima, tko je vlasnik uređaja korištenog za pristup mrežnoj stranici, ona se može definirati kao podatak o „osobi koja se može utvrditi” [16].

58. S obzirom na pristup Bundesgerichtshofa (Savezni vrhovni sud), dinamička IP adresa sama po sebi nije dovoljna za identifikaciju korisnika koji je putem nje pristupio određenoj mrežnoj stranici. Naprotiv, ako bi pružatelj usluga interneta mogao identificirati korisnika s pomoću dinamičke IP adrese, tada bi se bez ikakve sumnje radilo o osobnom podatku u smislu Direktive 95/46. Ne čini se, međutim, da je to smisao prethodnog pitanja, u kojem leži tvrdnja da pružatelji usluga interneta iz spora *a quo* ne mogu identificirati korisnika isključivo putem dinamičke IP adrese.

59. U kombinaciji s ostalim podacima, dinamička IP adresa omogućuje „neizravnu” identifikaciju korisnika, što je tvrdnja s kojom se svi slažu. Dopušta li, bez dodatnih uvjeta, okolnost postojanja takvih dodatnih podataka koji su spojivi s dinamičkom IP adresom definiranje IP adrese kao osobnog podatka u smislu Direktive? Potrebno je razriješiti je li u tom smislu dovoljna apstraktna mogućnost poznavanja tih podataka ili je, suprotno tomu, potrebno da su podaci raspoloživi onomu tko zna dinamičku IP adresu ili trećoj strani.

60. Stranke su usredotočile svoje primjedbe na tumačenje uvodne izjave 26. Direktive 95/46, iz koje ističu izraz „sredstva koja nadzornik ili bilo koja druga osoba može razumno koristiti da utvrdi navedenu osobu”. Pitanje suda koji je uputio zahtjev ne odnosi se na dodatne podatke u posjedu pružateljâ usluga uključenih u glavnom postupku. Također se ne odnosi na bilo koju treću stranu posjednika tih dodatnih podataka (čija bi kombinacija s dinamičkom IP adresom omogućila identifikaciju korisnika), već na pružatelja pristupa mreži.

61. Nije, dakle, potrebno da Sud u ovom slučaju analizira sva sredstva koja bi „razumno” mogao upotrijebiti tuženik u postupku *a quo* kako bi se dinamičke IP adrese koje ovaj ima mogle definirati kao osobni podatak. Budući da Bundesgerichtshof (Savezni vrhovni sud) isključivo upućuje na dodatne podatke u posjedu treće osobe, može se zaključiti da: a) tužena strana ili nema dovoljno vlastitih dodatnih podataka koji omogućuju identifikaciju korisnika, b) ili, ako ima takve podatke, nije se u mogućnosti njima razumno koristiti u tu svrhu kao nadzornik u smislu uvodne izjave 26. Direktive 95/46.

62. Obje hipoteze ovise o stvarnoj konstataciji, koja je u isključivoj nadležnosti suda koji je uputio zahtjev. Sud bi mu mogao ponuditi opće kriterije za tumačenje termina „sredstva koja nadzornik ili bilo koja druga osoba može razumno koristiti da utvrdi navedenu osobu”, kada bi Bundesgerichtshof (Savezni vrhovni sud) imao određenu dvojbu u vezi sa sposobnosti tužene strane da se razumno koristi vlastitim dodatnim podacima. Budući da nije tako, onda je, prema mojem mišljenju, nepotrebno da Sud postavi kriterije tumačenja koji sudu koji je uputio zahtjev nisu nužni niti ih je on tražio.

16 — Može se pretpostaviti, osim ako se dokaže suprotno, da je ta osoba pregledavala sadržaje na internetu i pristupila na odgovarajuću mrežnu stranicu. Čak i da se ne uzme u obzir posljednja pretpostavka, podaci o datumu, satu i brojčanom izvoru s kojeg se pristupilo mrežnoj stranici omogućili bi povezivanje pristupa s vlasnikom uređaja i njegovo dovođenje u izravnu vezu s načinom ponašanja na mreži. Moguća iznimka bile bi IP adrese dodijeljene računalima u prostorima kao što su *internetski caffei*, čiji se anonimni korisnici ne mogu identificirati i čijim vlasnicima promet koji se generirao u takvom prostoru ne pruža nikakve osobne podatke koji su relevantni na način da se može zaključiti o profilu ponašanja njegovih klijenata na mreži. Ovo je jedina iznimka od načela da su IP adrese osobni podatak, koje je prihvatila skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka, osnovana Direktivom 95/46 (tzv. „Skupina iz članka 29.”). Mišljenje 4/2007 od 20. lipnja 2007. o konceptu osobnih podataka, WP 136, dostupno na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

63. Stoga je postavljeno pitanje usredotočeno na rješavanja dvojbe je li za kvalifikaciju dinamičke IP adrese kao osobnog podatka relevantna činjenica da točno određena treća osoba, a to je pružatelj pristupa internetu, raspolaže dodatnim podacima s pomoću kojih se može, u kombinaciji s navedenim adresama, identificirati korisnika koji je posjetio određenu mrežnu stranicu.

64. Ponovno treba navesti uvodnu izjavu 26. Direktive 95/46. Izraz „sva sredstva koja […] *bilo koja druga osoba* može razumno koristiti" [17] mogao bi dovesti do tumačenja prema kojem bi bilo dovoljno da treća osoba može doći u posjed dodatnih podataka (koji se mogu kombinirati s dinamičkom IP adresom u svrhu identifikacije određene osobe) da bi se takva adresa *eo ipso* smatrala osobnim podatkom.

65. Ova maksimalistička interpretacija u praksi bi dovela do definiranja kao osobnog podatka svake vrste podataka, bez obzira na to koliko su sami po sebi nedovoljni za identifikaciju korisnika. Nikad se ne može u potpunosti otkloniti mogućnost da je treća osoba u posjedu podataka podobnih za kombiniranje s drugim podacima, čime bi se mogao otkriti identitet konkretne osobe.

66. Prema mojem mišljenju, mogućnost da tehnički napredak u bliskoj ili daljoj budućnosti otvori pristup sve sofisticiranijim instrumentima dobivanja i obrade podataka opravdava oprez kojim se želi osigurati obrana privatnosti. Prilikom definiranja pravnih kategorija relevantnih za zaštitu podataka pokušalo se uključiti pretpostavke ponašanja dovoljno široke i fleksibilne kako bi se pokrila svaka mogućnost koja se može zamisliti [18].

67. Međutim, vjerujem da ova legitimna zabrinutost ne može ignorirati normativnu volju zakonodavca i da se sustavno tumačenje uvodne izjave 26. Direktive 95/46 ograničava na „sredstva koja [...] mogu razumno koristiti" *druge osobe*.

68. Na isti način kao što uvodna izjava 26. ne cilja na svako sredstvo kojim se nadzornik može koristiti (u ovom slučaju pružatelj usluga interneta), već samo na ona kojima se on može „razumno" koristiti, u istom smislu potrebno je tumačiti da se zakonodavac referira na „druge osobe" kojima se *također na razuman način* može obratiti nadzornik koji namjerava pribaviti dodatne podatke za identifikaciju. To, međutim, nije slučaj kada kontakt s trećima zahtijeva velike troškove u smislu ljudskih i ekonomskih resursa ili je praktički nemoguć ili zabranjen zakonom. Inače, kao što sam to ranije upozorio, bilo bi praktički nemoguće razlikovanje između jednih i drugih sredstava jer bi uvijek bila održiva pretpostavka postojanja treće strane koja bi, bez obzira na to koliko je pružatelju usluga interneta nemoguće istima pristupiti, odmah ili u budućnosti, mogla raspolagati odgovarajućim dodatnim podacima koji bi doprinijeli identifikaciji korisnika.

69. Kao što sam to prethodno naveo, treća strana na koju se referira (Savezni vrhovni sud) pružatelj je pristupa mreži. Zasigurno je on ta treća strana za koju je najrazumnije pretpostaviti da će joj se obratiti pružatelj usluga radi dobivanja određenih dodatnih podataka, ako namjerava učinkovitije, praktičnije i izravnije identificirati korisnika koji je pristupio njegovoj mrežnoj stranici s pomoću dinamičke IP adrese. Ta treća strana ni na koji način nije hipotetska, nepoznata ni nepristupačna, već je glavni protagonist u strukturi interneta za kojeg se sa sigurnošću zna da posjeduje podatke koji su pružatelju usluga potrebni za identifikaciju korisnika. U stvari, kako to objašnjava sud koji je uputio zahtjev, upravo se toj trećoj strani tuženik u glavnom postupku namjerava obratiti za prikupljanje dodatnih podataka koji su mu nužni.

17 — U izvorniku bez isticanja.

18 — Ta opreznost i preventivna svrha temelj su stava koji podupire Skupina iz članka 29., koja smatra, kao što sam to naveo, da treba krenuti od načela da IP adrese predstavljaju osobni podatak, uz jedinu iznimku hipoteze kada je pružatelj usluga u mogućnosti s potpunom sigurnošću odrediti koje adrese pripadaju osobama koje se ne mogu utvrditi kao što mogu biti korisnici *internetskih caffea*. Vidjeti završetak bilješke 16.

70. Pružatelj pristupa internetu obično je treća strana na koju se referira uvodna izjava 26. Direktive 95/46, kojoj pružatelj usluga iz postupka *a quo* može „razumno" pristupiti. Međutim, preostaje razjasniti može li se pribavljanje dodatnih podataka u posjedu treće osobe definirati kao „razumno" izvedivo ili moguće.

71. Njemačka vlada smatra da, s obzirom na to da se informacija u posjedu pružatelja pristupa internetu smatra osobnim podatkom, on je ne može proslijediti ako to nije u skladu s pravnim okvirom koji regulira obradu tih podataka [19].

72. To je bez sumnje točno i, kako bi se moglo koristiti tom informacijom, potrebno je primijeniti propise koji se odnose na osobne podatke. Određena informacija može se „razumno" pribaviti ako se ispune uvjeti koji uređuju pristup toj vrsti podataka, a prvi je od njih mogućnost pohrane podataka i njihova prijenosa drugima. Točno je da je pružatelj pristupa internetu ovlašten odbiti prijenos zatraženih podataka, ali je moguće i suprotno. Potpuno moguće „razumno" prenošenje podataka pretvara dinamičku IP adresu, u skladu s uvodnom izjavom 26. Direktive 95/46, u osobni podatak u odnosu na pružatelja usluga interneta.

73. Radi se o mogućnosti koja je *u okviru zakona* vjerojatna i stoga i „razumna". Razumna sredstva pristupa na koja se odnosi Direktiva 95/46 moraju po definiciji biti zakonita [20]. Od te premise, kao što je i logično, polazi i sud koji je uputio zahtjev, kako to podsjeća njemačka vlada [21]. Na ovaj se način znatno sužavaju pravno relevantni načini pristupa jer bi oni trebali biti isključivo zakoniti. Ali, dok postoje, bez obzira na svoja praktična ograničenja u primjeni, oni predstavljaju „razumno sredstvo" u smislu Direktive 95/46.

74. Posljedično smatram da, u okvirima koje je postavio Bundesgerichtshof (Savezni vrhovni sud), prvo pitanje zaslužuje potvrdan odgovor. Dinamička IP adresa mora se u odnosu na pružatelja usluga interneta smatrati osobnim podatkom s obzirom na postojanje treće strane (pružatelja pristupa mreži) kojoj se razumno može obratiti radi pribavljanja dodatnih podataka koji, kada se kombiniraju s navedenom IP adresom, omogućavaju identifikaciju korisnika.

75. Vjerujem da bi ga rezultat do kojeg bi dovelo rješenje suprotno onomu kojeg sam pobornik u stvari učvrstio. Kada dinamičke IP adrese ne bi predstavljale osobni podatak za pružatelja usluga na internetu, on bi ih mogao čuvati neodređeno dugo i mogao bi u svakom trenutku tražiti od pružatelja pristupa internetu dodatne podatke radi kombiniranja s istima i identificiranja korisnika. U takvim okolnostima, kao što to priznaje njemačka vlada [22], dinamička IP adresa pretvorila bi se u osobni podatak svaki put kada bi se već raspolagalo dodatnim podacima potrebnima za identifikaciju korisnika, primjenjujući propise o zaštiti podataka.

76. Međutim, tada bi se radilo o podatku čija bi pohrana bila moguća jedino ako se do tog trenutka ne bi smatrao osobnim podatkom za pružatelja usluga. Tada bi pružatelj usluga bio taj koji bi pravno kvalificirao dinamičku IP adresu kao osobni podatak pod uvjetom da u budućnosti odluči upotrijebiti tu adresu za identifikaciju korisnika putem kombinacije s dodatnim podacima koje bi pribavio od treće strane. Međutim, prema mojem mišljenju, u svjetlu Direktive 95/46, odlučujuća je razumna mogućnost o postojanju „pristupačne" treće strane koja posjeduje potrebna sredstva za identifikaciju osobe, a ne da se ostvari mogućnost pristupa toj trećoj strani.

19 — Točke 40. i 45. njezinih pisanih očitovanja

20 — U tom kontekstu nevažno je to da je pristup osobnom podatku *de facto* moguć kršenjem propisa o zaštiti podataka.

21 — Točke 47. i 48. njezinih pisanih očitovanja

22 — Točka 36. njezinih pisanih očitovanja

77. Mogao bi se čak prihvatiti stav njemačke vlade da se dinamička IP adresa pretvara u osobni podatak u trenutku kada je dobije pružatelj pristupa internetu. U tim bi se slučajevima trebalo prihvatiti da takva kvalifikacija ima retroaktivan učinak u odnosu na rok pohrane IP adrese, pa je posljedično smatrati nepostojećom ako je prošao rok čuvanja koji bi se primjenjivao da je od početka bila definirana kao osobni podatak. U tim okolnostima ishod bi bio suprotan duhu propisa o zaštiti osobnih podataka. Razlog koji opravdava samo privremenu pohranu tih podataka bio bi iznevjeren u slučaju potencijalnog zakašnjelog priznanja relevantnosti značajke koja je njihov sastavni dio od početka: vlastitog potencijala kao sredstva identifikacije fizičkih osoba, bilo samostalno, bilo u kombinaciji s drugim podacima. Također zbog tog razloga, potpuno utemeljenog na ekonomičnosti, razumnije je pripisati tu značajku od početka.

78. Prema tome, kao prvi zaključak, smatram da se članak 2. točka (a) Direktive 95/46 treba tumačiti na način da IP adresa koju je pohranio pružatelj usluga u vezi s pristupom na njegovu mrežnu stranicu predstavlja za njega osobni podatak, u mjeri u kojoj pružatelj pristupa mreži (internetu) raspolaže dodatnim podacima koji omogućavaju identifikaciju korisnika.

B – *Drugo pitanje*

79. Svojim drugim prethodnim pitanjem Bundesgerichtshof (Savezni vrhovni sud) želi saznati protivi li se članku 7. točki (f) Direktive 95/46 nacionalna norma koja dopušta prikupljanje i korištenje osobnih podataka korisnika bez njegove suglasnosti isključivo kada je to potrebno radi ponude i obračuna konkretne usluge tom korisniku a da se korištenje tih podataka nakon završetka svake operacije korištenja pritom ne može opravdati svrhom osiguranja funkcioniranja usluge.

80. Prije odgovora na to pitanje potrebno je upozoriti na informaciju koju je pružio Bundesgerichtshof (Savezni vrhovni sud), prema kojoj se sporni podaci pohranjuju radi osiguranja pravilnog funkcioniranja internetskih stranica koje su uključene u glavni postupak, čime se omogućuje kazneni progon u slučajevima eventualnih kibernetičkih napada.

81. Najprije treba razmotriti je li obrada IP adresa na koje cilja upućeni zahtjev obuhvaćena iznimkom predviđenom u članku 3. stavku 2. podstavku 1. Direktive 95/46[23].

1. O primjenjivosti Direktive 95/46 na obradu spornih podataka

82. Čini se da Savezna Republika Njemačka sudjeluje u glavnom postupku kao običan pružatelj usluga interneta, odnosno kao fizička osoba (dakle *sine imperio*). Iz te činjenice u načelu proizlazi da obrada podataka koja je predmet ovog spora nije isključena iz područja primjene Direktive 95/46.

83. Riječima Suda iz presude u predmetu Lindqvist[24], aktivnosti iz članka 3. stavka 2. Direktive 95/46 „su, u svakom slučaju, aktivnosti tipične za državu ili za državna tijela i izvan opsega aktivnosti fizičkih osoba”[25]. U mjeri u kojoj je nadzornik obrade podataka koji su predmet rasprave onaj koji unatoč svojstvu javne vlasti djeluje kao privatni subjekt, primjenjuje se Direktiva 95/46.

84. Sud koji je uputio zahtjev isticanjem glavne svrhe koju njemačka uprava želi postići registracijom dinamičkih IP adresa naglašava da nastoji „jamčiti i održavati sigurnost i funkcioniranje svojih telekomunikacijskih usluga”, a osobito potaknuti „otkrivanje i obranu od čestih napada *denial of service* kada se telekomunikacijska infrastruktura paralizira namjernom i koordiniranom lavinom

23 — Ne ulaze u područje primjene Direktive 95/46 „postup[ci] obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost […] i *aktivnosti države u području kaznenog prava*” (u izvorniku bez isticanja).

24 — Presuda od 6. studenoga 2003. (C-101/01, EU:C:2003:596), t. 43.

25 — U istom smislu presuda od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727), t. 41.

velikog broja zahtjeva određenih mrežnih servera”[26]. Pohrana dinamičkih IP adresa u navedenu svrhu uobičajena je kod svakog značajnijeg vlasnika mrežnih stranica i ne implicira izravno ili neizravno izvršavanje javnih ovlasti, čime njihovo uključenje u područje primjene Direktive 95/46 ne stvara značajnije teškoće.

85. Međutim, Bundesgerichtshof (Savezni vrhovni sud) tvrdi da pohrana dinamičkih IP adresa pružatelja usluga uključenih u glavnom postupku također odgovara namjeri kaznenog postupanja protiv počinitelja eventualnih kibernetičkih napada, kada za to dođe trenutak. Je li ta namjera dovoljna da bi se obrada tih podataka isključila iz područja primjene Direktive 95/46?

86. Smatram da bismo se, ako u „područje kaznenog prava” spada izvršenje *ius puniendi* koji posjeduje država od strane pružatelja usluga iz glavnog postupka, suočili s „aktivnosti države u području kaznenog prava” i prema tome s jednom od iznimki predviđenih u članku 3. stavku 2. podstavku 1. Direktive 95/46.

87. U tim uvjetima, na temelju doktrine Suda iz predmeta Huber[27], obrada osobnih podataka od pružatelja usluga u svrhu sigurnosti i tehničkog funkcioniranja njegovih telekomunikacijskih usluga sadržana je u djelokrugu primjene Direktive 95/46, dok bi obrada podataka u okviru državne aktivnosti u području kaznenog prava ostala izuzeta.

88. Također, čak i kada aktivnosti u području kaznenog prava ne bi bile u nadležnosti Savezne Republike Njemačke kao običnog pružatelja usluga lišenog javnih ovlasti – koja bi se, kao i svaka druga fizička osoba, ograničila na prijenos spornih IP adresa državnom tijelu radi poduzimanja represivnih mjera – svrha obrade dinamičkih IP adresa bila bi jedna od aktivnosti izvan područja primjene Direktive 95/46.

89. Tako proizlazi iz sudske prakse ustaljene u predmetu Parlament/Vijeće i Komisija[28], u kojem je Sud potvrdio da činjenica da određene podatke „prikupljaju privatni operatori u trgovačke svrhe i da su upravo oni ti koji organiziraju njihov prijenos trećoj državi” ne znači da taj prijenos „nije uključen u opseg primjene” članka 3. stavka 2. podstavka 1. Direktive 95/46 kada je svrha prijenosa podataka državna aktivnost iz područja kaznenog prava svaki put kada „se unese u okvir koji su stvorile javne vlasti i čiji je cilj zaštita javne sigurnosti”[29].

90. Međutim, ako se, kao što mislim, pod „aktivnostima u području kaznenog prava” smatraju, kako to proizlazi iz odluke o upućivanju zahtjeva, one koje pripadaju pojedincu radi poticanja *ius puniendi* države putem odgovarajućih mjera, tada se ne može reći da obrada dinamičkih IP adresa ima za svrhu aktivnost države u kaznenom području, koje je isključeno iz područja primjene Direktive 95/46.

91. Doista, pohrana i registriranje tog podatka služili bi kao još jedan dokaz kojim bi vlasnik mrežne stranice zahtijevao od države, u svojstvu strane u postupku, progon nezakonitog ponašanja. To bi naposljetku bio instrument za obranu, u okviru kaznenog područja, onih prava koja javni poredak priznaje privatnom subjektu (u ovom slučaju državnom subjektu koji djeluje u okviru privatnog prava). S te se točke gledišta ne razlikuje od inicijative bilo kojeg pružatelja usluga interneta koji očekuje državnu zaštitu u vezi s postupcima iz područja kaznenog prava u skladu s propisima.

26 — Točka 36. odluke o postavljanju prethodnog pitanja

27 — Presuda od 16. prosinca 2008. (C-524/06, EU:C:2008:724), t. 45.

28 — Presuda od 30. svibnja 2006. (C-317/04 i C-318/04, EU:C:2006:346), t. 54. do 59.

29 — *Ibidem*, t. 59. Radilo se o osobnim podacima čija obrada nije bila potrebna za pružanje usluga koje su činile predmet poslovanja privatnih predmetnih subjekata (zračni prijevoznici), ali koje su bili prisiljeni dostaviti vlastima Sjedinjenih Američkih Država radi sprečavanja terorizma i borbe protiv njega.

92. Posljedično, u mjeri u kojoj njemačka uprava djeluje kao pružatelj usluga interneta bez javnih ovlasti, što je na sudu koji je uputio zahtjev da ocijeni, obrada dinamičkih IP adresa kao osobnih podataka ulazi u područje primjene Direktive 95/46.

2. O meritumu

93. Članak 15. stavak 1. TMG-a dopušta prikupljanje i korištenje osobnih podataka korisnika isključivo kada je to nužno radi ponude i obračuna konkretnog korištenja telekomunikacijske usluge. Točnije, pružatelj usluga smije isključivo prikupiti i koristiti se tzv. „podacima o korištenju", odnosno osobnim podacima korisnika koji su nužni za omogućavanje „korištenja i obračuna telekomunikacijskih usluga". Ti se podaci moraju izbrisati kada se operacija završi (odnosno kada je završilo konkretno korištenje telekomunikacijske usluge), osim ako se moraju čuvati „u svrhu obračuna", kao što je to predviđeno člankom 15. stavkom 4. TMG-a.

94. Nakon prestanka veze, čini se da članak 15. TMG-a ne dopušta da se podaci čuvaju iz drugih razloga, čak ni općenito radi osiguranja „korištenja telekomunikacijskih usluga". Budući da upućuje isključivo na svrhe obračuna kao opravdanje za čuvanje podataka, navedena odredba TMG-a može se shvatiti (iako je njezino konačno tumačenje na sudu koji je uputio zahtjev) na način da se podaci o korištenju obrađuju samo za omogućavanje konkretnog uspostavljanja veze i brišu nakon njezina prestanka.

95. Člankom 7. točkom (f) Direktive 95/46[30] dopušta se obrada podataka pod uvjetima koje bih (za nadzornika) ocijenio izdašnijima od onih propisanih u samom tekstu članka 15. TMG-a. Njemačka se odredba može označiti u tom smislu kao restriktivnija u odnosu na odredbu Unije jer u načelu ne predviđa ispunjenje legitimnog interesa koji nije obračun usluge, a to je da bi pružatelj usluga na internetu, Savezna Republika Njemačka, mogao imati legitiman interes u osiguravanju pravilnog funkcioniranja svojih mrežnih stranica i pored svakog korisničkog odnosa[31].

96. Sudska praksa Suda u predmetu ASNEF i FECEMD[32] pruža kriterije za odgovor na drugo prethodno pitanje. Tada je Sud potvrdio stajalište da iz cilja Direktive 95/46 „proizlazi [...] da članak 7. Direktive 95/46 definira opsežan i taksativan popis slučajeva u kojima se obrada osobnih podataka može smatrati zakonitom"[33]. Zbog toga „države članice ne mogu ni članku 7. Direktive 95/46 dodati nova načela u vezi s dopuštanjem obrade osobnih podataka ni nametnuti dodatne zahtjeve koji bi promijenili doseg nekog od šest načela definiranih tim člankom"[34].

97. Člankom 15. TMG-a ne propisuje se dodatni zahtjev uz one koji su utvrđeni člankom 7. Direktive 95/46 za zakonitost obrade podataka, kao što je to bilo u predmetima ASNEF i FECEMD[35], ali ako se restriktivno tumači, na što upućuje sud *a quo*, sužava sadržaj uvjeta iz točke (f) navedene odredbe: tamo gdje se zakonodavac Unije općenito referira na ispunjenje „[...] legitimnog interesa koji ima nadzornik ili treća strana ili strane kojima se podaci otkrivaju", članak 15. TMG-a jedino dotiče potrebu „omogućavanja [konkretnog] korištenja i obračuna telekomunikacijskih usluga".

30 — Navedeno u točki 17.

31 — Vidjeti točku 84. Točno je da vlasnici mrežnih stranica imaju legitiman interes u sprečavanju i borbi protiv uskraćivanja usluga (*denials of service*) koje spominje sud koji je uputio zahtjev, odnosno masovnih napada koji se u određenim slučajevima zajednički poduzimaju protiv pojedinih mrežnih stranica kako bi se zagušile i postale neoperativne.

32 — Presuda od 24. studenoga 2011. (C-468/10 i C-469/10, EU:C:2011:777)

33 — *Ibidem*, t. 30.

34 — *Ibidem*, t. 32.

35 — Slučaj u kojem je nacionalno pravo uvjetima iz članka 7. točke (f) Direktive 95/46 dodalo da će podaci koji su predmet obrade biti navedeni u javno dostupnim izvorima.

98. Isto kao i u predmetima ASNEF i FECEMD [36], i u ovom bi nacionalna mjera ponovno, ako se restriktivno tumači, prije izmijenila načelo iz članka 7. Direktive 95/46 nego što bi isto precizirala, a to je jedino zbog čega vlasti država članica imaju određeni prostor za procjenu u skladu s člankom 5. Direktive 95/46.

99. Doista, prema posljednjoj odredbi, „države članice u granicama odredbi ovog poglavlja [37] podrobno utvrđuju uvjete pod kojima je obrada podataka zakonita". Međutim, kao što je to navedeno u predmetima ASNEF i FECEMD [38], „države članice ne smiju u smislu [navedene odredbe] utvrđivati načela koja se odnose na legitimnost obrade osobnih podataka, a koja se razlikuju od onih navedenih u članku 7. te direktive, ni mijenjati putem dodatnih zahtjeva doseg šest načela postavljenih u navedenom članku 7.".

100. Članak 15. TMG-a u vezi s člankom 7. točkom (f) Direktive 95/46 značajno bi smanjio opseg legitimnog interesa koji je relevantan za opravdanje obrade podataka, pritom se ne ograničavajući samo na njegovo preciziranje ili nijansiranje u granicama članka 5. iste direktive. Osim toga, to bi učinio na kategorički i apsolutan način, bez uvažavanja da se zaštita i osiguranje općeg korištenja telekomunikacijskih usluga mogu odvagivati u odnosu na „interes ili temeljna prava i slobode osobe čiji se podaci obrađuju, koja zahtijeva zaštitu na temelju članka 1. stavka 1." Direktive 95/46, kako je predviđenom njezinim člankom 7. točkom (f).

101. U svakom slučaju, kao i u predmetima ASNEF i FECEMD [39], njemački bi zakonodavac propisao „s trajnim karakterom rezultat odvagivanja suprotstavljenih prava i interesa u vezi s [određenim kategorijama osobnih podataka] bez dopuštanja različitog ishoda s obzirom na posebne okolnosti svakog pojedinog slučaja", na način da se „više ne radi o detaljiziranju u smislu [...] članka 5." Direktive 95/46.

102. U takvim okolnostima smatram da je Bundesgerichtshof (Savezni vrhovni sud) dužan tumačiti nacionalnu normu u skladu s Direktivom 95/46, što podrazumijeva: a) da se u opravdane razloge za obradu tzv. „podataka o korištenju" može uključiti legitiman interes pružatelja telekomunikacijskih usluga da zaštiti njihovo opće korištenje i b) da se taj interes pružatelja usluga može odvagnuti *ad casum* u odnosu na interes ili temeljna prava i slobode korisnika radi određivanja koje pravo zaslužuje zaštitu prema članku 1. stavku 1. Direktive 95/46 [40].

103. Smatram da više ništa nije potrebno dodati uvjetima pod kojima je potrebno izvršiti to odvagivanje u slučaju koji je povod prethodnom pitanju. Bundesgerichtshof (Savezni vrhovni sud) nije uputio pitanje u vezi s tim jer je zaokupljen rješavanjem onoga koje prethodi tom odvagivanju, tj. time može li se to odvagivanje provesti.

104. Na kraju, čini se nepotrebnim naznačiti da sud *a quo* može uzeti u obzir eventualne odredbe koje je usvojila država članica u okviru dopuštenja iz članka 13. stavka 1. točke (d) Direktive 95/46 radi smanjenja dosega obveza i prava predviđenih u članku 6. iste direktive, kada bi bilo potrebno, osim za zaštitu drugih dobara, za omogućavanje „[...] sprečavanja, istrage, otkrivanja i progona kaznenih djela [...]". Na to ne upućuje ni sud koji je uputio zahtjev, koji je bez sumnje svjestan postojanja obaju članaka.

36 — Presuda od 24. studenoga 2011. (C-468/10 i C-469/10, EU:C:2011:777)

37 — Poglavlje II., pod nazivom „Opća pravila za zakonitost obrade osobnih podataka", obuhvaća članke 5. do 21. Direktive 95/46.

38 — Presuda od 24. studenoga 2011. (C-468/10 i C-469/10, EU:C:2011:777), t. 36.

39 — Presuda od 24. studenoga 2011. (C-468/10 i C-469/10, EU:C:2011:777), t. 47.

40 — Na raspravi je zastupnik P. Breyera odbio navod da je registar dinamičkih IP adresa potreban radi zaštite dobrog funkcioniranja internetskih usluga u slučajevima mogućih napada. Ne vjerujem da se na ovaj problem može dati apsolutan odgovor, njegovu rješenju mora prethoditi usporedba između interesa vlasnika mrežne stranice i prava i interesa korisnika u svakom pojedinom slučaju.

105. Posljedično predlažem kao odgovor na drugo prethodno pitanje navesti da se članku 7. točki (f) Direktive 95/46 protivi nacionalna norma čije tumačenje onemogućuje pružatelju usluga prikupiti i obraditi osobne podatke korisnika, bez obzira na njegovu suglasnost, s ciljem osiguranja funkcioniranja telekomunikacijskih usluga nakon završetka svakog pojedinog korištenja.

VI – **Zaključak**

106. Na temelju izloženog, predlažem Sudu da na postavljena pitanja odgovori na sljedeći način:

„1. Na temelju članka 2. točke (a) Direktive 95/46/EZ Parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom protoku takvih podataka, dinamička IP adresa s pomoću koje je korisnik pristupio mrežnoj stranici pružatelja telekomunikacijskih usluga predstavlja za njega ‚osobni podatak' u mjeri u kojoj pružatelj pristupa na mrežu posjeduje druge dodatne podatke koji kombinirani s dinamičkom IP adresom omogućuju identifikaciju korisnika.

2. Članak 7. točku (f) Direktive 95/46 treba tumačiti na način da se cilj osiguranja funkcioniranja telekomunikacijske usluge može u načelu smatrati legitimnim interesom čije ispunjenje opravdava obradu tog osobnog podatka, podložno ocjeni prevaguje li obrada podataka nad interesom ili temeljnim pravima osobe u pitanju. Nacionalni propis koji ne bi omogućio uzeti u obzir taj legitimni interes ne bi bio u skladu s navedenim člankom".