Zbornik sudske prakse

PRESUDA SUDA (drugo vijeće)

19. listopada 2016.*

„Zahtjev za prethodnu odluku – Obrada osobnih podataka – Direktiva 95/46/EZ – Članak 2. točka (a) – Članak 7. točka (f) – Pojam ‚osobni podaci' – Adrese internetskog protokola – Pohranjivanje koje provodi pružatelj usluga internetskih medija – Nacionalni propis koji ne omogućuje da nadzornik uzme o obzir postavljeni zakoniti interes"

U predmetu C-582/14,

povodom zahtjeva za prethodnu odluku na temelju članka 267. UFEU-a, koji je uputio Bundesgerichtshof (Savezni vrhovni sud, Njemačka), odlukom od 28. listopada 2014., koju je Sud zaprimio 17. prosinca 2014., u postupku

Patrick Breyer

protiv

Savezne Republike Njemačke,

SUD (drugo vijeće),

u sastavu: M. Ilešič, predsjednik vijeća, A. Prechal, A. Rosas (izvjestitelj), C. Toader, i E. Jarašiūnas, suci,

nezavisni odvjetnik: M. Campos Sánchez-Bordona,

tajnik: V. Giacobbo-Peyronnel, administratorica,

uzimajući u obzir pisani postupak i nakon rasprave održane 25. veljače 2016.,

uzimajući u obzir očitovanja koja su podnijeli:

— za P. Breyera, M. Starostik, *Rechtsanwalt*,

— za njemačku vladu, A. Lippstreu i T. Henze, u svojstvu agenata,

— za austrijsku vladu, G. Eberhard, u svojstvu agenta,

— za portugalsku vladu, L. Inez Fernandes i C. Vieira Guerra, u svojstvu agenata,

— za Europsku komisiju, P. J. O. Van Nuffel, H. Krämer, P. Costa de Oliveira i J. Vondung, u svojstvu agenata,

saslušavši mišljenje nezavisnog odvjetnika na raspravi održanoj 12. svibnja 2016.,

* Jezik postupka: njemački

donosi sljedeću

Presudu

1 Zahtjev za prethodnu odluku odnosi se na tumačenje članka 2. točke (a) i članka 7. točke (f) Direktive 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca 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.).

2 Zahtjev je upućen u okviru spora između Patricka Breyera i Bundesrepublik Deutschland (Savezna Republika Njemačka) u pogledu registracije i pohranjivanja od strane potonje adrese internetskog protokola (u daljnjem tekstu: IP adresa) P. Breyera prilikom njegova posjeta nekoliko internetskih stranica njemačkih saveznih službi.

Pravni okvir

Pravo Unije

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

„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 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”.

4 U skladu s člankom 1. navedene direktive:

„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.

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.”

5 Članak 2. te direktive propisuje:

„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 njezin 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;

[...]"

6 Članak 3. Direktive 95/46, naslovljen „Područje primjene", propisuje:

„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,

[...]"

7 Članak 5. navedene direktive propisuje:

„Države članice u granicama odredbi ovog poglavlja podrobno utvrđuju uvjete pod kojima je obrada podataka zakonita."

8 Članak 7. te direktive glasi kako slijedi:

„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 stranka kojoj se podaci otkrivaju;

ili

(f) je obrada potrebna u svrhe zakonitog interesa koji ima nadzornik ili treća stranka ili stranke 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.”

9 Članak 13. stavak 1. Direktive 95/46 propisuje:

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

[...]

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

[...]”

Njemačko pravo

10 Članak 12. Telemediengesetza (Zakon o internetskim medijima) od 26. veljače 2007. (BGBl. 2007. I, str. 179.; u daljnjem tekstu: TMG) propisuje:

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

2. Pružatelj usluga smije se koristiti osobnim podacima prikupljenima radi osiguranja internetskih medija u ostale svrhe samo u mjeri u kojoj je to dopušteno ovim zakonom ili ostalim propisima koji se izričito odnose na navedene medije 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.”

11 Članak 15. TMG-a predviđa:

„1. Pružatelj usluga smije prikupljati i upotrebljavati osobne podatke korisnika samo kada je to potrebno radi omogućavanja korištenja i obračuna internetskih medija (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 internetskim medijima kojima se korisnik koristio.

2. Pružatelj usluga smije kombinirati podatke o korištenju različitih internetskih medija 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. [...]"

12 Na temelju članka 3. stavka 1. Bundesdatenschutzgesetza (Savezni zakon o zaštiti podataka) od 20. prosinca 1990. (BGBl. 1990. I, str. 2954.), „osobni podaci su konkretni podaci o osobnim ili stvarnim okolnostima određene ili odredive fizičke osobe (osoba čiji se podaci obrađuju). [...]"

Glavni postupak i prethodna pitanja

13 P. Breyer posjetio je nekoliko internetskih stranica njemačkih saveznih službi. Na tim stranicama, dostupnima javnosti, te službe pružaju ažurirane informacije.

14 Kako bi spriječili napade i omogućili kazneni progon napadača, većina tih stranica registrira svaki posjet u dnevničkim datotekama. U njima čuvaju, nakon završetka sesije posjeta tim stranicama, ime posjećene stranice ili datoteke, podatke upisane u poljima tražilica, datum i vrijeme posjeta, količinu prenesenih podataka, podatak o uspješnosti povezivanja i IP adresu računala s kojeg je obavljen posjet.

15 IP adrese su nizovi brojeva koji se dodjeljuju računalima povezanima na internet kako bi se omogućila komunikacija među njima putem te mreže. Ako se posjeti internetska stranica, IP adresa računala koje šalje zahtjev šalje se poslužitelju na kojem se nalazi stranica koja se posjećuje. Ta je komunikacija potrebna kako bi se zatraženi podaci mogli prenijeti na pravilno odredište.

16 Nadalje, iz odluke kojom se upućuje zahtjev i iz spisa kojim raspolaže Sud proizlazi da računalima korisnika interneta pružatelji internetskog pristupa dodjeljuju ili „statičnu" IP adresu ili „dinamičnu" IP adresu, tj. IP adresu koja se mijenja prilikom svakog novog povezivanja na internet. Za razliku od statičnih IP adresa, dinamične IP adrese ne omogućuju uspostavu veze, preko datoteka dostupnih javnosti, između određenog računala i fizičke veze s mrežom kojom se koristi pružatelj internetskog pristupa.

17 P. Breyer je njemačkim upravnim sudovima podnio tužbu kojom traži da se Saveznoj Republici Njemačkoj zabrani pohranjivanje i povjeravanje trećim osobama na pohranjivanje, nakon sesije posjeta stranicama dostupnima javnosti internetskih medija njemačkih saveznih službi IP adrese pristupatelja P. Breyera jer to pohranjivanje u slučaju poremećaja nije potrebno za ponovnu uspostavu rada tih medija.

18 Budući da je tužba P. Breyera odbijena u prvostupanjskom postupku, on je podnio žalbu protiv odluke o odbijanju.

19 Žalbeni sud djelomično je preinačio tu odluku. Osudio je Saveznu Republiku Njemačku na zabranu pohranjivanja ili povjeravanja trećim osobama na pohranjivanje, nakon svakog posjeta, IP adrese sustava s kojega je pristupao P. Breyer, koja je prenesena prilikom njegova posjeta stranicama dostupnima javnosti internetskih medija njemačkih saveznih službi, kad je ta adresa pohranjena zajedno s datumom sesije posjeta na koji se odnosi i ako je P. Breyer otkrio svoj identitet tijekom te sesije, uključujući adresom elektroničke pošte u kojoj se spominje njegov identitet jer to pohranjivanje u slučaju poremećaja nije potrebno za ponovnu uspostavu rada tih medija.

20 Prema mišljenju tog žalbenog suda, dinamična IP adresa, zajedno s datumom sesije posjeta na koji se odnosi, jest, ako je dotični korisnik internetske stranice otkrio svoj identitet tijekom te sesije, osobni podatak jer operator te stranice može identificirati tog korisnika povezujući njegovo ime i IP adresu njegova računala.

21 Međutim, navedeni žalbeni sud ocijenio je da ne treba prihvatiti žalbu P. Breyera u drugim dijelovima. Naime, u slučaju u kojem P. Breyer ne navodi svoj identitet tijekom sesije posjeta jedino bi pružatelj internetskog pristupa mogao povezati IP adresu i konkretnog pretplatnika. Nasuprot tomu, IP adresa u posjedu Savezne Republike Njemačke, u njezinu svojstvu pružatelja usluga internetskih medija, nije osobni podatak, čak i zajedno s datumom sesije posjeta na koji se odnosi, s obzirom na to da identitet korisnika internetskih stranica o kojima je riječ ta država članica ne bi mogla utvrditi.

22 Patrick Breyer i Savezna Republika Njemačka podnijeli su svaki svoju reviziju Bundesgerichtshofu (Savezni vrhovni sud, Njemačka) protiv odluke žalbenog suda. P. Breyer zahtijeva da se u cijelosti prihvati njegov zahtjev za zabranu. Savezna Republika Njemačka zahtijeva odbijanje tog zahtjeva.

23 Sud koji je uputio zahtjev pojašnjava da su dinamične IP adrese računala P. Breyera, koje je Savezna Republika Njemačka pohranila u svojstvu pružatelja usluga internetskih medija, barem u kontekstu drugih podataka koji se pohranjuju u dnevničke datoteke, posebni podaci o materijalnoj situaciji P. Breyera, s obzirom na to da daju naznaku o njegovim posjetima određenim stranicama ili određenim datotekama na internetu na određene datume.

24 Međutim, podaci koji se na taj način pohranjuju ne omogućuju izravno utvrđivanje identiteta P. Breyera. Naime, operatori internetskih stranica o kojima je riječ u glavnom postupku mogli bi identificirati P. Breyera samo ako bi im njegov pružatelj internetskog pristupa proslijedio podatke o identitetu tog korisnika. Kvalifikacija tih podataka kao „osobnih” ovisila bi, prema tome, o tome može li se utvrditi identitet P. Breyera.

25 Bundesgerichtshof (Savezni vrhovni sud) navodi da postoji doktrinalan spor o pitanju treba li, radi utvrđivanja može li se utvrditi identitet osobe, primijeniti „objektivni” kriterij ili „relativni” kriterij. Primjena „objektivnog” kriterija imala bi za posljedicu da bi se za podatke poput IP adresa o kojima je riječ u glavnom postupku, nakon sesija posjeta internetskim stranicama o kojima je riječ, moglo smatrati da su osobne naravi čak i ako samo treća osoba može utvrditi identitet osobe o kojoj je riječ, pri čemu je ta treća osoba u ovom slučaju pružatelj internetskog pristupa P. Breyera koji je pohranjivao dodatne podatke koji omogućuju njegovu identifikaciju pomoću navedenih IP adresa. Prema „relativnom” kriteriju, takvi podaci mogli bi se smatrati osobnima u odnosu na jedno tijelo, poput pružatelja internetskog pristupa P. Breyera, jer omogućuju točnu identifikaciju korisnika (vidjeti u tom smislu presudu od 24. studenoga 2011., Scarlet Extended, C-70/10, EU:C:2011:771, t. 51.), ali ne i osobnima u odnosu na drugo tijelo, poput operatora internetskih stranica koje je posjetio P. Breyer, s obzirom na to da taj operator ne bi raspolagao, u slučaju da P. Breyer nije otkrio svoj identitet tijekom sesija posjeta tim stranicama, informacijama potrebnima za svoju identifikaciju bez prekomjernog napora.

26 U slučaju da dinamične IP adrese računala P. Breyera treba smatrati, zajedno s datumom sesije na koji se odnose, osobnim podacima, sud koji je uputio zahtjev želi znati je li pohranjivanje tih IP adresa nakon te sesije dopušteno na temelju članka 7. točke (f) te direktive.

27 U tom smislu Bundesgerichtshof (Savezni vrhovni sud) pojašnjava, s jedne strane, da pružatelji usluga internetskih medija mogu, u skladu s člankom 15. stavkom 1. TMG-a, prikupljati i upotrebljavati osobne podatke korisnika samo u mjeri u kojoj je to potrebno kako bi se omogućilo i obračunalo korištenje tim medijima. S druge strane, sud koji je uputio zahtjev navodi da je, prema mišljenju Savezne Republike Njemačke, pohranjivanje tih podataka nužno kako bi se zajamčila sigurnost i neprekinuto dobro funkcioniranje stranica službi internetskih medija koje ona čini dostupnima

javnosti, omogućujući osobito prepoznavanje informatičkih napada, tzv. „napada uskraćivanja usluge”, koji imaju za cilj paralizirati funkcioniranje tih stranica ciljanim i koordiniranim zasipanjem određenih internetskih poslužitelja velikim brojem zahtjeva, i borbu protiv tih napada.

28 Prema mišljenju suda koji je uputio zahtjev, ako i u mjeri u kojoj je potrebno da pružatelj usluga internetskih medija poduzme mjere za borbu protiv takvih napada, te se mjere mogu smatrati potrebnima za „omogućavanje [...] upotrebe elektroničkih medija” u skladu s člankom 15. TMG-a. Međutim, doktrina većinom zastupa stajalište prema kojem su, s jedne strane, prikupljanje i upotreba osobnih podataka korisnika internetske stranice dopušteni samo radi omogućivanja pravilne upotrebe te stranice i, s druge strane, ti se podaci moraju pobrisati na kraju sesije posjeta o kojem je riječ ako nisu potrebni za obračunavanje. Međutim, takvo restriktivno tumačenje članka 15. stavka 1. TMG-a protivilo bi se tomu da se pohranjivanje IP adresa dopusti kako bi se općenito zajamčile sigurnost i neprekinutost dobrog funkcioniranja internetskih medija.

29 Sud koji je uputio zahtjev pita se je li potonje tumačenje, koje je tumačenje koje zagovara žalbeni sud, u skladu s člankom 7. točkom (f) Direktive 95/46, osobito s obzirom na kriterije koje je Sud razvio u točkama 29. i dalje presude od 24. studenoga 2011., ASNEF i FECEMD (C-468/10 i C-469/10, EU:C:2011:777).

30 U tim je okolnostima Bundesgerichtshof (Savezni vrhovni sud) odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:

„1. Treba li članak 2. točku (a) Direktive 95/46/EZ tumačiti na način da IP adresa koju pružatelj usluga [internetskih medija] 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) [te direktive] odredba nacionalnog prava prema kojoj pružatelj usluga [internetskih medija] može prikupljati i koristiti osobne podatke korisnika bez njegove dozvole samo u dijelu u kojem je to potrebno kako bi omogućio i obračunao konkretno korištenje internetskih medija dotičnog korisnika i prema kojem svrha osiguravanja općeg funkcioniranja internetskog medija ne može opravdati korištenje podataka nakon završetka sesije [posjeta] u tijeku?”

O prethodnim pitanjima

Prvo pitanje

31 Svojim prvim pitanjem sud koji je uputio zahtjev u biti pita treba li članak 2. točku (a) Direktive 95/46 tumačiti na način da dinamična IP adresa koju pohrani pružatelj usluga informatičkih medija prilikom posjeta osobe internetskoj stranici koju taj pružatelj čini dostupnom javnosti predstavlja, u odnosu na tog pružatelja, osobni podatak u smislu te odredbe, ako jedino treća osoba, u ovom slučaju pružatelj internetskog pristupa te osobe, raspolaže dodatnim informacijama potrebnima za njezinu identifikaciju.

32 U skladu s tom odredbom, „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’)”. U skladu s tom odredbom, 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 njezin fizički, fiziološki, mentalni, gospodarski, kulturni ili socijalni identitet.

33 Uvodno valja navesti da je u točki 51. presude od 24. studenoga 2011., Scarlet Extended (C-70/10, EU:C:2011:771), koja se odnosila, među ostalim, na tumačenje iste direktive, Sud u biti smatrao da su IP adrese korisnika interneta zaštićeni osobni podaci jer omogućuju preciznu identifikaciju tih korisnika.

34 Međutim, ta se tvrdnja Suda odnosila na slučaj u kojem prikupljanje i identifikaciju IP adresa korisnika interneta provode pružatelji internetskog pristupa.

35 Ipak, u ovom slučaju prvo pitanje odnosi se na slučaj u kojem je pružatelj usluga internetskih medija, tj. Savezna Republika Njemačka, taj koji pohranjuje IP adrese korisnika internetske stranice koju taj pružatelj usluga čini dostupnom javnosti a da ne raspolaže dodatnim informacijama potrebnima za identifikaciju tih korisnika.

36 Nadalje, nije sporno da su IP adrese na koje upućuje sud koji je uputio zahtjev „dinamične" IP adrese, tj. privremene adrese koje se dodjeljuju prilikom svakog povezivanja na internet i zamjenjuju prilikom kasnijih povezivanja, a ne „statične" IP adrese, koje su nepromjenjive i koje omogućuju trajnu identifikaciju uređaja povezanog na mrežu.

37 Prvo pitanje koje je postavio sud koji je uputio zahtjev stoga se temelji na premisi prema kojoj, s jedne strane, podaci koji se sastoje od dinamične IP adrese te datuma i vremena sesije posjeta internetskoj stranici s te IP adrese, koje pohranjuje pružatelj usluga internetskih medija, same po sebi tom pružatelju ne daju mogućnost identifikacije korisnika koji je posjetio tu internetsku stranicu tijekom te sesije i, s druge strane, pružatelj internetskog pristupa raspolaže dodatnim informacijama koje, ako se povežu s tom IP adresom, omogućuju identifikaciju tog korisnika.

38 U tom smislu najprije valja navesti da nije sporno da dinamična IP adresa nije informacija koja se odnosi na „utvrđenu fizičku osobu" jer takva adresa ne otkriva izravno identitet fizičke osobe koja je vlasnik računala s kojega je obavljen posjet internetskoj stranici ni identitet druge osobe koja bi se mogla koristiti tim računalom.

39 Nadalje, kako bi se utvrdilo je li dinamična IP adresa, u slučaju navedenom u točki 37. ove presude, osobni podatak u smislu članka 2. točke (a) Direktive 96/45 u odnosu na pružatelja usluga internetskih medija, valja provjeriti može li se takva IP adresa, koju pohranjuje taj pružatelj, kvalificirati kao informacija koja se odnosi na „fizičku osobu koju se može utvrditi", ako dodatne informacije potrebne za identifikaciju korisnika internetske stranice koju taj pružatelj usluga čini dostupnom javnosti posjeduje pružatelj internetskog pristupa tog korisnika.

40 U tom smislu iz teksta članka 2. točke (a) Direktive 96/45 proizlazi da je osoba koju se može utvrditi ona čiji je identitet moguće utvrditi ne samo izravno nego i neizravno.

41 Upotrebna pojma „neizravno" od strane zakonodavca Unije ima za cilj istaknuti da za kvalifikaciju informacije kao osobnog podatka nije potrebno da ta informacija sama po sebi omogućuje identifikaciju osobe o kojoj je riječ.

42 Nadalje, uvodna izjava 26. Direktive 96/45 navodi 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 koristiti da utvrdi navedenu osobu.

43 Budući da ta uvodna izjava spominje sredstva koja nadzornik ili „bilo koja druga osoba" može opravdano koristiti, njezin tekst upućuje na to da, kako bi se podatak mogao kvalificirati kao „osobni podatak" u smislu članka 2. točke (a) te direktive, nije potrebno da se sve informacije koje omogućuju identifikaciju osobe o kojoj je riječ moraju nalaziti u posjedu samo jedne osobe.

44 Činjenica da dodatne informacije potrebne za identifikaciju korisnika internetske stranice ne posjeduje pružatelj usluga internetskih medija, nego pružatelj internetskog pristupa tog korisnika, nije stoga takva da isključuje da su dinamične IP adrese koje pohranjuje pružatelj usluga internetskih medija za njega osobni podaci u smislu članka 2. točke (a) Direktive 96/45.

45 Ipak, valja utvrditi je li mogućnost povezivanja dinamične IP adrese s tim dodatnim informacijama koje posjeduje taj pružatelj internetskog pristupa sredstvo koje se može opravdano koristiti za utvrđivanje navedene osobe.

46 Kao što je to u biti naveo nezavisni odvjetnik u točki 68. svojeg mišljenja, to nije slučaj ako je identifikacija osobe o kojoj je riječ zabranjena zakonom ili neostvariva u praksi, primjerice, zbog toga što bi značila nerazmjerne napore u pogledu vremena, troškova i rada, tako da se rizik identifikacije u stvarnosti čini neznatnim.

47 Međutim, iako sud koji je uputio zahtjev u svojoj odluci kojom se upućuje prethodno pitanje pojašnjava da njemačko pravo ne dopušta pružatelju internetskog pristupa da pružatelju usluga internetskih medija izravno proslijedi dodatne informacije potrebne za identifikaciju osobe o kojoj je riječ, ipak se čini, ne dovodeći u pitanje provjere koje treba u tom smislu provesti taj sud, da postoje pravni putevi koji pružatelju usluga internetskih medija omogućuju da se obrati, osobito u slučaju kibernetskih napada, nadležnom tijelu kako bi ono poduzelo potrebne korake za dobivanje tih informacija od pružatelja internetskog pristupa i za pokretanje kaznenih postupaka.

48 Stoga se čini da pružatelj usluga internetskih medija raspolaže sredstvima koja se mogu opravdano koristiti za utvrđivanje, uz pomoć drugih osoba, tj. nadležnog tijela i pružatelja internetskog pristupa, identiteta navedene osobe na temelju pohranjenih IP adresa.

49 S obzirom na sve prethodno navedeno, na prvo pitanje valja odgovoriti tako da članak 2. točku (a) Direktive 95/46 treba tumačiti na način da dinamična IP adresa koju pohrani pružatelj usluga informatičkih medija prilikom posjeta osobe internetskoj stranici koju taj pružatelj čini dostupnom javnosti predstavlja, u odnosu na tog pružatelja, osobni podatak u smislu te odredbe, ako raspolaže pravnim sredstvima koji mu omogućuju identifikaciju navedene osobe pomoću dodatnih informacija kojima raspolaže pružatelj internetskog pristupa te osobe.

Drugo pitanje

50 Svojim drugim pitanjem sud koji je uputio zahtjev u biti pita treba li članak 7. točku (f) Direktive 96/45 tumačiti na način da mu se protivi propis države članice prema kojem pružatelj usluga internetskih medija može prikupljati i koristiti osobne podatke korisnika tih usluga bez njegove dozvole samo u dijelu u kojem su to prikupljanje i to korištenje potrebni kako bi omogućio i obračunao konkretno korištenje tih usluga od tog korisnika a da cilj osiguranja općeg funkcioniranja tih usluga ne može opravdati korištenje tim podacima nakon sesije njegova posjeta.

51 Prije odgovora na to pitanje valja utvrditi nije li obrada osobnih podataka u glavnom postupku, tj. dinamičnih IP adresa korisnika određenih internetskih stranica njemačkih saveznih službi, isključena iz područja primjene Direktive 96/45 na temelju njezina članka 3. stavka 2. prve alineje, u skladu s kojim se ta direktiva ne primjenjuje na postupke obrade koji se odnose na, među ostalim, aktivnosti države u području kaznenog prava.

52 U tom smislu valja podsjetiti na to da su aktivnosti koje ta odredba spominje kao primjere u svakom slučaju aktivnosti države i državnih tijela, koje ne ulaze u područje aktivnosti pojedinaca (vidjeti presude od 6. studenoga 2003., Lindqvist, C-101/01, EU:C:2003:596, t. 43. i od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, t. 41.).

53 Međutim, u glavnom se postupku, ne dovodeći u pitanje provjere koje u tom smislu treba provesti sud koji je uputio zahtjev, čini da njemačke savezne službe, koje pružaju usluge internetskih medija i koje su odgovorne za postupanje s dinamičnim IP adresama, djeluju, unatoč svojem svojstvu javnih tijela, u svojstvu pojedinaca i izvan okvira aktivnosti države u području kaznenog prava.

54 Stoga valja utvrditi je li propis države članice, poput onoga iz glavnog postupka, u skladu s člankom 7. točkom (f) Direktive 96/45.

55 U tu svrhu valja podsjetiti na to da nacionalni propis u glavnom postupku, tumačen usko na način kako to čini sud koji je uputio zahtjev, dopušta prikupljanje i korištenje osobnih podataka korisnika tih usluga 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 sesije posjeta pritom ne može opravdati svrhom osiguranja funkcioniranja usluge.

56 U skladu s člankom 7. točkom (f) Direktive 96/45, obrada osobnih podataka zakonita je ako „je obrada potrebna u svrhe zakonitog interesa koji ima nadzornik ili treća stranka ili stranke 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.” te direktive.

57 Valja podsjetiti na to da je Sud presudio da članak 7. te direktive predviđa iscrpan i taksativan popis slučajeva u kojima se obrada osobnih podataka može smatrati zakonitom te da države članice ne mogu ni dodati nova načela tom članku u pogledu legitimacije obrade osobnih podataka ni predvidjeti dodatne zahtjeve koji bi značili izmjenu dosega nekog od šest načela predviđenih u tom članku (vidjeti u tom smislu presudu od 24. studenoga 2011., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, t. 30. i 32.).

58 Iako članak 5. Direktive 96/45, doduše, dopušta državama članicama da, u granicama poglavlja II. te direktive i, prema tome, njezina članka 7., podrobnije utvrde uvjete pod kojima je obrada osobnih podataka zakonita, margina prosudbe kojom u skladu s tim člankom 5. raspolažu države članice može se koristiti samo u skladu s ciljem koji postavlja ta direktiva, tj. održavanja ravnoteže između slobodnog kretanja osobnih podataka i zaštite privatnog života. Države članice ne mogu uvesti, u skladu s člankom 5. te direktive, neka druga načela u pogledu legitimacije obrade osobnih podataka koja nisu ona navedena u njezinu članku 7. ni izmijeniti, dodatnim zahtjevima, doseg šest načela predviđenih u članku 7. (vidjeti u tom smislu presudu od 24. studenoga 2011., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, t. 33., 34. i 36.).

59 U ovom slučaju razvidno je da bi članak 15. TMG-a, ako bi se tumačio usko, kako je spomenuto u točki 55. ove presude, imao uži doseg od dosega načela predviđenog člankom 7. točkom (f) Direktive 96/45.

60 Naime, iako članak 7. točka (f) te direktive općenito navodi „svrhe zakonitog interesa kojeg ima nadzornik ili treća stranka ili stranke kojima se podaci otkrivaju”, članak 15. TMG-a pružatelju usluga dopušta prikupljanje i korištenje osobnih podataka korisnika samo u dijelu u kojem je to potrebno kako bi se omogućilo i obračunalo konkretno korištenje elektroničkim medijima. Članak 15. TMG-a stoga se općenito protivi pohranjivanju, nakon sesije posjeta internetskim medijima, osobnih podataka radi osiguranja korištenja tim medijima. Međutim, njemačke savezne službe koje pružaju usluge internetskih medija mogle bi također imati zakoniti interes za jamčenje, nakon svakog konkretnog korištenja njihovim internetskim stranicama dostupnima javnosti, nastavka funkcioniranja tih stranica.

61 Kao što je to naveo nezavisni odvjetnik u točkama 100. i 101. svojeg mišljenja, takav nacionalni propis ne ograničava se na to da samo precizira, u skladu s člankom 5. Direktive 96/45, pojam „zakoniti interes” iz članka 7. točke (f) te direktive.

62 U tom smislu također valja podsjetiti na to da se članak 7. točka (f) te direktive protivi tomu da država članica kategorički i općenito isključi mogućnost obrade za određene kategorije osobnih podataka bez omogućavanja odvagivanja suprotstavljenih prava i interesa o kojima je riječ u konkretnom slučaju. Država članica stoga ne može za te kategorije definitivno propisati rezultat odvagivanja suprotstavljenih prava i interesa bez omogućivanja različitog rezultata ovisno o pojedinim okolnostima konkretnog slučaja (vidjeti u tom smislu presudu od 24. studenoga 2011., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, t. 47. i 48.).

63 Međutim, propis poput onoga u glavnom postupku sužava, u pogledu obrade osobnih podataka korisnika stranica internetskih medija, doseg načela predviđenog člankom 7. točkom (f) Direktive 96/45 isključujući mogućnost da cilj osiguranja općeg funkcioniranja tog internetskog medija bude predmet odvagivanja s interesom ili temeljnim pravima i slobodama tog korisnika koji uživaju zaštitu u skladu s člankom 1. stavkom 1. te direktive.

64 Iz svega prethodno navedenog proizlazi da na drugo pitanje valja odgovoriti tako da članak 7. točku (f) Direktive 96/45 treba tumačiti na način da mu se protivi propis države članice prema kojem pružatelj usluga internetskih medija može prikupljati i koristiti osobne podatke korisnika tih usluga bez njegove dozvole samo u dijelu u kojem su to prikupljanje i to korištenje potrebni kako bi omogućio i obračunao konkretno korištenje tih usluga od tog korisnika a da cilj osiguranja općeg funkcioniranja tih usluga ne može opravdati korištenje tim podacima nakon sesije njegova posjeta.

Troškovi

65 Budući da ovaj postupak ima značaj prethodnog pitanja za stranke glavnog postupka pred sudom koji je uputio zahtjev, na tom je sudu da odluči o troškovima postupka. Troškovi podnošenja očitovanja Sudu, koji nisu troškovi spomenutih stranaka, ne nadoknađuju se.

Slijedom navedenoga, Sud (drugo vijeće) odlučuje:

1. **Članak 2. točku (a) Direktive 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka treba tumačiti na način da dinamična IP adresa koju pohrani pružatelj usluga informatičkih medija prilikom posjeta osobe internetskoj stranici koju taj pružatelj čini dostupnom javnosti predstavlja, u odnosu na tog pružatelja, osobni podatak u smislu te odredbe, ako raspolaže pravnim sredstvima koji mu omogućuju identifikaciju navedene osobe pomoću dodatnih informacija kojima raspolaže pružatelj internetskog pristupa te osobe.**

2. **Članak 7. točku (f) Direktive 96/45 treba tumačiti na način da mu se protivi propis države članice prema kojem pružatelj usluga internetskih medija može prikupljati i koristiti osobne podatke korisnika tih usluga bez njegove dozvole samo u dijelu u kojem su to prikupljanje i to korištenje potrebni kako bi omogućio i obračunao konkretno korištenje tih usluga od tog korisnika a da cilj osiguranja općeg funkcioniranja tih usluga ne može opravdati korištenje tim podacima nakon sesije njegova posjeta.**

Potpisi