Zbiór Orzeczeń

WYROK TRYBUNAŁU (druga izba)

z dnia 19 października 2016 r.*

Odesłanie prejudycjalne — Przetwarzanie danych osobowych — Dyrektywa 95/46/WE — Artykuł 2 lit. a) — Artykuł 7 lit. f) — Pojęcie „danych osobowych" — Adresy protokołów internetowych — Przechowywanie przez dostawcę usług medialnych online — Uregulowanie krajowe uniemożliwiające uwzględnienie uzasadnionego interesu administratora danych

W sprawie C-582/14

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez Bundesgerichtshof (federalny trybunał sprawiedliwości, Niemcy) postanowieniem z dnia 28 października 2014 r., które wpłynęło do Trybunału w dniu 17 grudnia 2014 r., w postępowaniu:

Patrick Breyer

przeciwko

Bundesrepublik Deutschland,

TRYBUNAŁ (druga izba),

w składzie: M. Ilešič, prezes izby, A. Prechal, A. Rosas (sprawozdawca), C. Toader i E. Jarašiūnas, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: V. Giacobbo-Peyronnel, administrator,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 25 lutego 2016 r.,

rozważywszy uwagi przedstawione:

— w imieniu P. Breyera przez M. Starostika, Rechtsanwalt,

— w imieniu rządu niemieckiego przez A. Lippstreua oraz T. Henzego, działających w charakterze pełnomocników,

— w imieniu rządu austriackiego przez G. Eberharda, działającego w charakterze pełnomocnika,

— w imieniu rządu portugalskiego przez L. Ineza Fernandesa oraz C. Vieirę Guerrę, działających w charakterze pełnomocników,

* Język postępowania: niemiecki.

— w imieniu Komisji Europejskiej przez P.J.O. Van Nuffela, H. Krämera, P. Costę de Oliveirę oraz J. Vondung, działających w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 12 maja 2016 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni art. 2 lit. a) i art. 7 lit. f) dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31).

2 Powyższy wniosek został przedstawiony w ramach sporu między Patrickiem Breyerem a Bundesrepublik Deutschland (Republiką Federalną Niemiec) w przedmiocie rejestrowania i przechowywania przez nią adresu protokołu internetowego (zwanego dalej „adresem IP") P. Breyera podczas przeglądania przez niego wielu stron internetowych niemieckich służb federalnych.

Ramy prawne

Prawo Unii

3 Motyw 26 dyrektywy 95/46 ma następujące brzmienie:

„Zasady ochrony danych muszą odnosić się do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób; w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby; zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w taki sposób, że podmiot danych nie będzie mógł być zidentyfikowany; zasady postępowania w rozumieniu art. 27 mogą być przydatnym instrumentem w udzielaniu wskazówek co do sposobów nadawania danym charakteru anonimowego oraz zachowania w formie, w której identyfikacja osoby, której dane dotyczą, nie jest dłużej możliwa".

4 Artykuł 1 wspomnianej dyrektywy stanowi:

„1. Zgodnie z przepisami niniejszej dyrektywy, państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.

2. Państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych między państwami członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1".

5 Artykuł 2 omawianej dyrektywy stanowi:

„Do celów niniejszej dyrektywy:

a) »dane osobowe« oznacza[ją] wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio,

szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

b) »przetwarzanie danych osobowych« (»przetwarzanie«) oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie;

[…]

d) »administrator danych« oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe;

[…]

f) »osoba trzecia« oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych;

[…]”.

6 Artykuł 3 dyrektywy 95/46, zatytułowany „Zakres obowiązywania”, przewiduje:

„1. Niniejsza dyrektywa stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

— w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

[…]”.

7 Artykuł 5 rzeczonej dyrektywy stanowi:

„Państwa członkowskie określą, w granicach przepisów zawartych w niniejszym rozdziale, bardziej szczegółowe warunki ustalania legalności przetwarzania danych osobowych”.

8 Artykuł 7 tej samej dyrektywy brzmi następująco:

„Państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas gdy:

a) osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę;

lub

b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy;

lub

c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega;

lub

d) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą;

lub

e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane [której dane są ujawniane];

lub

f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom [osób trzecich], którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1 [gdy pierwszeństwo mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony zgodnie z art. 1 ust. 1]”.

9 Artykuł 13 ust. 1 dyrektywy 95/46 stanowi:

„Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzian[ych] w art. 6 ust. 1, art. 10, art. 11 ust. 1, art. 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia:

[…]

d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji;

[…]”.

Prawo niemieckie

10 Paragraf 12 Telemediengesetz [ustawy o usługach medialnych online (telemediach)] z dnia 26 lutego 2007 r. (BGBl. 2007 I, s. 179, zwanej dalej „TMG”) stanowi:

„1) Usługodawca może gromadzić i wykorzystywać dane osobowe w celu udostępniania telemediów, o ile zezwala na to niniejsza ustawa lub inny przepis prawny, który odnosi się wyraźnie do telemediów, lub gdy użytkownik wyraził na to zgodę.

2) Usługodawca może wykorzystywać dane osobowe, które zostały zgromadzone w celu udostępniania telemediów, do innych celów tylko wtedy, gdy zezwala na to niniejsza ustawa lub inny przepis prawny, który odnosi się wyraźnie do telemediów, lub gdy użytkownik wyraził na to zgodę.

3) O ile prawo nie stanowi inaczej, należy stosować przepisy obowiązujące w odniesieniu do ochrony danych osobowych, nawet jeżeli dane nie są przetwarzane w zautomatyzowany sposób".

11 Paragraf 15 TMG przewiduje:

„1) Usługodawca może gromadzić i wykorzystywać dane osobowe użytkownika tylko wtedy, gdy jest to konieczne do umożliwienia korzystania z telemediów i zafakturowania kosztów takiego korzystania (dane o korzystaniu). Danymi o korzystaniu są w szczególności:

1. kryteria umożliwiające identyfikację użytkownika,

2. dane na temat rozpoczęcia i zakończenia oraz zakresu danego korzystania,

3. dane na temat telemediów, z których korzystał użytkownik.

2) Usługodawca może łączyć dane użytkownika o korzystaniu z różnych telemediów, o ile jest to konieczne w celu zafakturowania w stosunku do użytkownika.

[…]

4) Usługodawca może wykorzystywać dane o korzystaniu po zakończeniu danej sesji, jeżeli są one konieczne do celów wystawienia faktury użytkownikowi (dane do faktury). Usługodawca może zablokować dane w celu dochowania istniejących ustawowych, statutowych lub umownych terminów przechowywania. […]".

12 Zgodnie z § 3 ust. 1 Bundesdatenschutzgesetz (federalnej ustawy o ochronie danych) z dnia 20 grudnia 1990 r. (BGBl. 1990 I, s. 2954, zwanej dalej „BDSG") „[d]anymi osobowymi są szczegółowe dane dotyczące sytuacji osobistej lub rzeczowej zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą) […]".

Postępowanie główne i pytania prejudycjalne

13 Patrick Breyer przeglądał wiele stron internetowych niemieckich służb federalnych. Na tych dostępnych publicznie stronach wspomniane służby dostarczają zaktualizowanych informacji.

14 Aby chronić się przed atakami i umożliwić ściganie na drodze karnej „piratów", w przypadku większości tych portali każde wejście na stronę jest rejestrowane w pliku logów. Po zakończeniu danej sesji w danych tych przechowuje się nazwę konsultowanych danych lub strony, pojęcia wpisane w polach wyszukiwania, dzień i godzinę konsultacji, ilość przesłanych danych, informację, czy konsultacja się powiodła, oraz adres IP komputera, za pomocą którego przeglądano określone dane lub strony.

15 Adresy IP stanowią ciągi liczb, które są przypisywane komputerom podłączonym do Internetu, aby umożliwić ich komunikację za pomocą tej sieci. Przy konsultowaniu strony internetowej adres IP komputera wykorzystywanego do konsultacji danej strony jest przesyłany do serwera, na którym jest zarejestrowana konsultowana strona. Jest to konieczne, by konsultowane dane można było przesłać odpowiedniemu odbiorcy.

16 Ponadto z postanowienia odsyłającego oraz z akt sprawy, którymi dysponuje Trybunał, wynika, że dostawcy dostępu do Internetu przyznają użytkownikom Internetu bądź „statyczny" adres IP, bądź „dynamiczny" adres IP, który zmienia się przy okazji każdego nowego połączenia z Internetem. W odróżnieniu od statycznych adresów IP, dynamiczne adresy IP nie umożliwiają powiązania – za pomocą publicznie dostępnych plików – danego komputera i fizycznego podłączenia do sieci wykorzystywanego przez dostawcę dostępu do Internetu.

17 Patrick Breyer wytoczył przed niemiecki sąd administracyjny powództwo, które miało na celu zakazanie Republice Federalnej Niemiec przechowywania – lub zlecania przechowywania przez osoby trzecie – adresu IP systemu hostingowego P. Breyera po zakończeniu przeglądania dostępnych publicznie stron mediów online niemieckich służb federalnych, o ile rejestracja tego adresu nie jest konieczna do przywrócenia dostępności tych mediów w przypadku awarii.

18 Jako że powództwo P. Breyera zostało oddalone w pierwszej instancji, wniósł on apelację od orzeczenia oddalającego powództwo.

19 Sąd apelacyjny zmienił częściowo owo orzeczenie. Nakazał on Republice Federalnej Niemiec zaniechać przechowywania lub zlecania przechowywania przez osoby trzecie – po zakończeniu każdego przeglądania – adresu IP systemu hostingowego P. Breyera, przekazanego w trakcie przeglądania przez niego dostępnych publicznie stron mediów online niemieckich służb federalnych, w przypadku gdy adres ten jest przechowywany w powiązaniu z datą sesji, do której on się odnosi, i gdy P. Breyer ujawnił swoją tożsamość w trakcie tej sesji, także w formie adresu e-mail wskazującego na jego tożsamość, o ile to przechowywanie nie jest konieczne do przywrócenia dostępności mediów online w przypadku awarii.

20 Zdaniem tegoż sądu apelacyjnego dynamiczny adres IP w połączeniu z datą sesji, do której się on odnosi, stanowi, w sytuacji gdy dany użytkownik strony internetowej ujawnił swoją tożsamość w trakcie tej sesji, dane osobowe, ponieważ operator tej strony może zidentyfikować tego użytkownika poprzez zestawienie jego nazwiska z adresem IP jego komputera.

21 Wspomniany sąd apelacyjny uznał, że nie należy jednak uwzględnić powództwa P. Breyera w innych przypadkach. W przypadku bowiem, gdy P. Breyer nie podaje swojej tożsamości w trakcie przeglądania strony, jedynie dostawca dostępu do Internetu może powiązać adres IP ze zidentyfikowanym abonentem. Natomiast w rękach Republiki Federalnej Niemiec, jako dostawcy usług medialnych online, adres IP nie stanowi jednej z danych osobowych, nawet w połączeniu z datą przeglądania strony, do której się on odnosi, zważywszy, że użytkownik rozpatrywanych stron internetowych nie może zostać zidentyfikowany przez to państwo członkowskie.

22 Zarówno P. Breyer, jak i Republika Federalna Niemiec wnieśli skargę rewizyjną („Revision") do Bundesgerichtshof (federalnego trybunału sprawiedliwości, Niemcy) na orzeczenie sądu apelacyjnego. Patrick Breyer wnosi o uwzględnienie w całości jego wniosku o zakazanie czynności, o których mowa powyżej. Republika Federalna Niemiec wnosi o oddalenie tego wniosku.

23 Sąd odsyłający wyjaśnia, że dynamiczne adresy IP komputera P. Breyera, przechowywane przez Republikę Federalną Niemiec, działającą w charakterze dostawcy usług medialnych online, stanowią – przynajmniej w kontekście innych danych przechowywanych w plikach logów – szczegółowe dane dotyczące sytuacji rzeczowej P. Breyera, jako że dostarczają wskazówek co do przeglądania przez niego określonych stron lub określonych plików w Internecie w określonych datach.

24 Niemniej przechowywane w ten sposób dane nie pozwalają ustalić bezpośrednio tożsamości P. Breyera. Operatorzy stron internetowych będących przedmiotem sporu w postępowaniu głównym mogliby bowiem zidentyfikować P. Breyera wyłącznie wtedy, gdyby jego dostawca dostępu do Internetu przekazał im informacje na temat tożsamości tego użytkownika. Uznanie tych danych za „osobowe" zależy w konsekwencji od tego, czy P. Breyer mógł zostać zidentyfikowany.

25 Bundesgerichtshof (federalny trybunał sprawiedliwości) wskazuje na doktrynalną kontrowersję dotyczącą kwestii, czy w celu ustalenia, czy osoba może zostać zidentyfikowana, należy oprzeć się na kryterium „obiektywnym" bądź na kryterium „względnym". Zastosowanie kryterium „obiektywnego" skutkowałoby tym, że dane takie jak adresy IP będące przedmiotem sporu w postępowaniu głównym mogłyby być uznawane, po zakończeniu przeglądania rozpatrywanych stron internetowych, za dane osobowe, nawet jeśli tylko osoba trzecia jest w stanie ustalić tożsamość osoby, której dane dotyczą, przy czym tą osobą trzecią jest w niniejszym przypadku dostawca dostępu do Internetu dla P. Breyera, który to dostawca przechowywał dodatkowe dane umożliwiające zidentyfikowanie P. Breyera za pomocą wspomnianych adresów IP. Zgodnie z kryterium „względnym" takie dane mogłyby być uznawane za dane osobowe wobec podmiotu takiego jak dostawca dostępu do Internetu dla P. Breyera, ponieważ pozwalają one na precyzyjną identyfikację użytkownika (zob. w tym względzie wyrok z dnia 24 listopada 2011 r., Scarlet Extended, C-70/10, EU:C:2011:771, pkt 51), lecz nie mogłyby być uznawane za dane osobowe wobec innego podmiotu, takiego jak operator stron internetowych przeglądanych przez P. Breyera, jako że operator ten nie dysponuje – w przypadku gdy P. Breyer nie ujawnił swojej tożsamości w trakcie przeglądania tych stron – informacjami koniecznymi do jego identyfikacji bez nadmiernego wysiłku.

26 W przypadku gdyby dynamiczne adresy IP komputera P. Breyera należało uznać – w połączeniu z datą przeglądania stron, do której się one odnoszą – za stanowiące dane osobowe, sąd odsyłający chciałby się dowiedzieć, czy przechowywanie tych adresów IP po zakończeniu przeglądania danych stron jest dozwolone na podstawie art. 7 lit. f) tej samej dyrektywy.

27 W powyższym względzie Bundesgerichtshof (federalny trybunał sprawiedliwości) precyzuje, po pierwsze, że zgodnie z § 15 ust. 1 TMG dostawcy usług medialnych online mogą gromadzić i wykorzystywać dane osobowe użytkownika tylko wtedy, gdy jest to konieczne do umożliwienia korzystania z danych mediów i zafakturowania kosztów takiego korzystania. Po drugie, sąd odsyłający wskazuje, że według Republiki Federalnej Niemiec przechowywanie wspomnianych danych jest konieczne do zapewnienia bezpieczeństwa i ciągłości sprawnego funkcjonowania stron w ramach usług medialnych online, które to strony udostępnia ona publicznie, pozwalając w szczególności rozpoznać ataki informatyczne zwane „atakami w postaci odmowy usługi" (denial of service), mające na celu sparaliżowanie funkcjonowania tych stron poprzez celowe i skoordynowane zalanie określonych serwerów internetowych dużą ilością zapytań, jak również zwalczać te ataki.

28 Zdaniem sądu odsyłającego, jeżeli dostawca usług medialnych online podjął środki w celu zwalczania takich ataków – oraz w zakresie w jakim konieczne jest, by je podjął – środki te mogłyby zostać uznane za konieczne do „umożliwienia korzystania z telemediów" na podstawie § 15 TMG. W doktrynie przeważa jednak pogląd, że gromadzenie i wykorzystywanie danych osobowych użytkownika strony internetowej jest dozwolone tylko po to, aby umożliwić konkretne korzystanie z tej strony, zaś dane te, o ile nie są one konieczne do wystawienia faktury, powinny zostać wymazane w momencie zakończenia danego przeglądania. Taka restrykcyjna interpretacja § 15 ust. 1 TMG stałaby jednak na przeszkodzie temu, by przechowywanie adresów IP było dozwolone w celu zapewnienia bezpieczeństwa i ciągłości sprawnego funkcjonowania mediów online.

29 Sąd odsyłający zastanawia się, czy ta ostatnia interpretacja, za którą właśnie opowiada się sąd apelacyjny, jest zgodna z art. 7 lit. f) dyrektywy 95/46 w świetle między innymi kryteriów wypracowanych przez Trybunał w pkt 29 i nast. wyroku z dnia 24 listopada 2011 r., ASNEF i FECEMD (C-468/10 i C-469/10, EU:C:2011:777).

30 W takich okolicznościach Bundesgerichtshof (federalny trybunał sprawiedliwości) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy art. 2 lit. a) dyrektywy 95/46 powinien być interpretowany w ten sposób, że adres protokołu internetowego (adres IP), który usługodawca [dostawca usług medialnych online] rejestruje w związku z wejściem na jego stronę internetową, stanowi dla niego dane osobowe już wtedy, gdy osoba trzecia (tu: dostawca dostępu) dysponuje dodatkową wiedzą wymaganą do identyfikacji danej osoby?

2) Czy art. 7 lit. f) [tej dyrektywy] stoi na przeszkodzie przepisowi prawa krajowego, zgodnie z którym usługodawca [dostawca usług medialnych online] może gromadzić i wykorzystywać dane osobowe użytkownika bez jego zgody tylko wtedy, gdy jest to konieczne do umożliwienia i zafakturowania konkretnego skorzystania z mediów online przez danego użytkownika, i zgodnie z którym cel polegający na zapewnieniu ogólnego funkcjonowania mediów online nie może uzasadniać korzystania z tych danych po zakończeniu danej sesji [przeglądania danej strony]?”.

W przedmiocie pytań prejudycjalnych

W przedmiocie pytania pierwszego

31 W swoim pytaniu pierwszym sąd odsyłający zastanawia się zasadniczo, czy art. 2 lit. a) dyrektywy 95/46 należy interpretować w ten sposób, że dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu tego przepisu, w sytuacji gdy tylko osoba trzecia, w niniejszym przypadku dostawca dostępu do Internetu dla tej osoby, dysponuje dodatkowymi informacjami koniecznymi do identyfikacji tejże osoby.

32 Zgodnie ze wskazanym powyżej przepisem „dane osobowe” oznaczają „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«)”. W myśl tego przepisu osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

33 Tytułem wstępu należy zauważyć, że w pkt 51 wyroku z dnia 24 listopada 2011 r., Scarlet Extended (C-70/10, EU:C:2011:771), który dotyczył między innymi wykładni tej samej dyrektywy, Trybunał uznał zasadniczo, że adresy IP użytkowników Internetu stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników.

34 Niemniej powyższe twierdzenie Trybunału odnosiło się do przypadku, w którym gromadzenie i identyfikacja adresów IP użytkowników Internetu są dokonywane przez dostawców dostępu do Internetu.

35 Natomiast w niniejszym przypadku pytanie pierwsze dotyczy przypadku, w którym to dostawca usług medialnych online, czyli Republika Federalna Niemiec, rejestruje adresy IP użytkowników strony internetowej, którą ten usługodawca udostępnia publicznie, nie dysponując dodatkowymi informacjami koniecznymi do zidentyfikowania tych użytkowników.

36 Ponadto bezsporne jest, że adresy IP, do których odnosi się sąd odsyłający, są „dynamicznymi” adresami IP, czyli tymczasowymi adresami, przydzielanymi każdemu połączeniu z Internetem i zastępowanymi podczas kolejnych połączeń, a nie „statycznymi” adresami IP, które są niezmienne i umożliwiają stałą identyfikację urządzenia podłączonego do sieci.

37 Zadane przez sąd odsyłający pytanie pierwsze opiera się zatem na założeniu, zgodnie z którym z jednej strony dane obejmujące dynamiczny adres IP oraz datę i godzinę przeglądania strony internetowej z tego adresu IP, zarejestrowane przez dostawcę usług medialnych online, nie dają same w sobie temu dostawcy możliwości zidentyfikowania użytkownika, który przeglądał tę stronę internetową w trakcie danej sesji, a z drugiej strony dostawca dostępu do Internetu dysponuje dodatkowymi informacjami, które w połączeniu z tym adresem IP umożliwiają identyfikację danego użytkownika.

38 W powyższym względzie należy najpierw zwrócić uwagę, że bezsporne jest, iż dynamiczny adres IP nie stanowi informacji odnoszącej się do „zidentyfikowanej osoby fizycznej", jako że taki adres nie ujawnia bezpośrednio tożsamości osoby fizycznej będącej właścicielem komputera, z którego była przeglądana strona internetowa, ani tożsamości innej osoby, która mogłaby korzystać z tego komputera.

39 Następnie, w celu ustalenia, czy dynamiczny adres IP stanowi, w przypadku przedstawionym w pkt 37 niniejszego wyroku, dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 96/45 wobec dostawcy usług medialnych online, należy sprawdzić, czy taki adres IP, zarejestrowany przez takiego dostawcę, może zostać uznany za informację odnoszącą się do „możliwej do zidentyfikowania osoby fizycznej", w sytuacji gdy dodatkowe informacje konieczne do identyfikacji użytkownika strony internetowej, którą ten usługodawca udostępnia publicznie, znajdują się w posiadaniu dostawcy dostępu do Internetu dla tego użytkownika.

40 W powyższym względzie z treści art. 2 lit. a) dyrektywy 95/46 wynika, że za możliwą do zidentyfikowania uznaje się osobę, która może zostać zidentyfikowana nie tylko bezpośrednio, lecz także pośrednio.

41 Użycie przez prawodawcę Unii terminu „pośrednio" służy wskazaniu, że aby móc uznać informację za dane osobowe, nie jest konieczne, by informacja ta umożliwiała sama w sobie zidentyfikowanie osoby, której dane dotyczą.

42 Ponadto w motywie 26 dyrektywy 95/46 wskazano, że w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może, racjonalnie rzecz biorąc, posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby.

43 W zakresie, w jakim wskazany wyżej motyw odnosi się do sposobów, jakimi mogą, racjonalnie rzecz biorąc, posłużyć się zarówno administrator danych, jak i „inna osoba", brzmienie tego motywu sugeruje, że aby dane mogły zostać uznane za „dane osobowe" w rozumieniu art. 2 lit. a) wspomnianej dyrektywy, nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby.

44 Nie wydaje się zatem, by okoliczność, że dodatkowe informacje konieczne do identyfikacji użytkownika strony internetowej są w posiadaniu nie dostawcy usług medialnych online, lecz dostawcy dostępu do Internetu dla tego użytkownika, mogła wykluczać to, iż dynamiczne adresy IP zarejestrowane przez dostawcę usług medialnych online stanowią dla niego dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46.

45 Należy jednak ustalić, czy możliwość połączenia dynamicznego adresu IP z owymi dodatkowymi informacjami będącymi w posiadaniu tego dostawcy dostępu do Internetu stanowi sposób, który może, racjonalnie rzecz biorąc, zostać zastosowany w celu zidentyfikowania osoby, której dane dotyczą.

46 Jak zauważył zasadniczo rzecznik generalny w pkt 68 opinii, nie miałoby to miejsca w przypadku, gdyby identyfikacja osoby, której dane dotyczą, była zakazana prawem lub niewykonalna w praktyce, przykładowo z powodu okoliczności, że wiąże się ona z nadmiernym nakładem czasu, kosztów i pracy ludzkiej, tak że ryzyko identyfikacji wydaje się w rzeczywistości znikome.

47 Otóż jakkolwiek sąd odsyłający wyjaśnia w swoim postanowieniu odsyłającym, że prawo niemieckie nie pozwala dostawcy dostępu do Internetu przekazywać bezpośrednio dostawcy usług medialnych online dodatkowych informacji koniecznych do identyfikacji osoby, której dane dotyczą, wydaje się jednak – z zastrzeżeniem konieczności zweryfikowania tego przez ten sąd – że istnieją środki prawne umożliwiające dostawcy usług medialnych online zwrócenie się do właściwego organu, aby podjął on konieczne działania w celu uzyskania tych informacji od dostawcy dostępu do Internetu oraz w celu wszczęcia ścigania karnego.

48 Wydaje się zatem, że dostawca usług medialnych online dysponuje środkami, którymi może, racjonalnie rzecz biorąc, posłużyć się w celu zidentyfikowania – z pomocą innych osób, czyli właściwego organu i dostawcy dostępu do Internetu – osoby, której dane dotyczą, na podstawie przechowywanych adresów IP.

49 W świetle całości powyższych rozważań na pytanie pierwsze należy odpowiedzieć, iż art. 2 lit. a) dyrektywy 95/46 należy interpretować w ten sposób, że dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu tego przepisu, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby.

W przedmiocie pytania drugiego

50 W drodze pytania drugiego sąd odsyłający chciałby się zasadniczo dowiedzieć, czy art. 7 lit. f) dyrektywy 95/46 należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu państwa członkowskiego, na podstawie którego dostawca usług medialnych online może gromadzić i wykorzystywać dane osobowe użytkownika tych usług – w braku jego zgody – tylko wtedy, gdy takie gromadzenie i wykorzystywanie są konieczne do umożliwienia konkretnego skorzystania ze wspomnianych usług przez tego użytkownika i zafakturowania kosztów takiego korzystania, przy czym cel polegający na zapewnieniu ogólnej funkcjonalności tychże usług nie może uzasadniać korzystania z tych danych po zakończeniu przeglądania danych mediów.

51 Przed udzieleniem odpowiedzi na powyższe pytanie należy ustalić, czy przetwarzanie danych osobowych będących przedmiotem sporu w postępowaniu głównym, czyli dynamicznych adresów IP użytkowników określonych stron internetowych federalnych służb niemieckich, nie jest wykluczone z zakresu stosowania dyrektywy 95/46 na podstawie art. 3 ust. 2 tiret pierwsze tej dyrektywy, zgodnie z którym owa dyrektywa nie ma zastosowania do przetwarzania danych osobowych w ramach działalności państwa w obszarach prawa karnego.

52 W powyższym względzie należy przypomnieć, że rodzaje działalności wymienione tytułem przykładu we wskazanym przepisie stanowią w każdym razie działalność właściwą państwom lub władzom państwowym, odmienną od dziedzin działalności podmiotów prywatnych (zob. wyroki: z dnia 6 listopada 2003 r., Lindqvist, C-101/01, EU:C:2003:596, pkt 43; z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia, C-73/07, EU:C:2008:727, pkt 41).

53 W sprawie zawisłej w postępowaniu głównym – z zastrzeżeniem konieczności zweryfikowania tego przez sąd odsyłający – wydaje się, że federalne służby niemieckie, które świadczą usługi medialne online i które są odpowiedzialne za przetwarzanie dynamicznych adresów IP, działają, mimo przysługującego im statusu władz publicznych, w charakterze podmiotów prywatnych poza ramami działalności państwa w obszarach prawa karnego.

54 Należy zatem ustalić, czy uregulowanie państwa członkowskiego takie jak uregulowanie będące przedmiotem sporu w postępowaniu głównym jest zgodne z art. 7 lit. f) dyrektywy 95/46.

55 W tym celu należy przypomnieć, że uregulowanie krajowe będące przedmiotem sporu w postępowaniu głównym, w restrykcyjnej wykładni przytoczonej przez sąd odsyłający, zezwala na gromadzenie i wykorzystywanie danych osobowych użytkownika wspomnianych usług – w braku jego zgody – wyłącznie wtedy, gdy jest to konieczne do umożliwienia konkretnego skorzystania z mediów online przez danego użytkownika i zafakturowania kosztów takiego korzystania, przy czym cel polegający na zapewnieniu ogólnej funkcjonalności mediów online nie może uzasadniać korzystania z tych danych po zakończeniu przeglądania danych mediów.

56 W myśl art. 7 lit. f) dyrektywy 95/46 przetwarzanie danych osobowych jest zgodne z prawem, gdy „jest [ono] konieczne dla [realizacji] potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom [osób trzecich], którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1 [gdy pierwszeństwo mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony zgodnie z art. 1 ust. 1]” tej dyrektywy.

57 Należy przypomnieć, że Trybunał orzekł, iż art. 7 owej dyrektywy przewiduje zamknięty i wyczerpujący wykaz przypadków, w których przetwarzanie danych osobowych może zostać uznane za legalne, oraz iż państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych względem kryteriów ustanowionych w tym artykule ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu jednego z sześciu kryteriów przewidzianych w tymże artykule (zob. podobnie wyrok z dnia 24 listopada 2011 r., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, pkt 30, 32).

58 O ile art. 5 dyrektywy 95/46 zezwala państwom członkowskim doprecyzować – w granicach rozdziału II tej dyrektywy i tym samym art. 7 tejże dyrektywy – warunki, w jakich przetwarzanie danych osobowych jest legalne, o tyle zakres uznania, jakim na podstawie owego art. 5 dysponują państwa członkowskie, może zostać wykorzystany jedynie zgodnie z celem przyświecającym wspomnianej dyrektywie, polegającym na zachowaniu równowagi między swobodnym przepływem danych osobowych a ochroną życia prywatnego. Państwa członkowskie nie mogą na podstawie art. 5 tej samej dyrektywy wprowadzać innych kryteriów legalności przetwarzania danych osobowych niż kryteria ustanowione w art. 7 dyrektywy ani też modyfikować, za pomocą dodatkowych wymogów, zakresu sześciu kryteriów przewidzianych we wspomnianym art. 7 (zob. podobnie wyrok z dnia 24 listopada 2011 r., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, pkt 33, 34, 36).

59 W niniejszym przypadku okazuje się, że § 15 TMG, gdyby był interpretowany w ścisły sposób wspomniany w pkt 55 niniejszego wyroku, byłby ujęty bardziej wąsko niż zasada przewidziana w art. 7 lit. f) dyrektywy 95/46.

60 Podczas bowiem gdy art. 7 lit. f) wspomnianej dyrektywy odnosi się w sposób ogólny do „[realizacji] potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom [osób trzecich], którym dane są ujawniane”, § 15 TMG zezwala dostawcy usług na gromadzenie i wykorzystywanie danych osobowych użytkownika wyłącznie w zakresie, w jakim jest to konieczne do umożliwienia konkretnego korzystania z mediów elektronicznych i zafakturowania kosztów takiego korzystania. Paragraf 15 TMG stoi zatem na przeszkodzie, ogólnie rzecz biorąc, przechowywaniu danych osobowych po zakończeniu przeglądania mediów online w celu zagwarantowania korzystania z tych mediów. Niemieckie służby federalne, które świadczą usługi medialne online, mogłyby także mieć uzasadniony interes w zagwarantowaniu, poza każdym konkretnym skorzystaniem z ich dostępnych publicznie stron internetowych, ciągłości funkcjonowania wspomnianych stron.

61 Jak zauważył rzecznik generalny w pkt 100 i 101 opinii, takie uregulowanie krajowe nie ogranicza się do uszczegółowienia zgodnie z art. 5 dyrektywy 95/46 pojęcia „uzasadnionego interesu” występującego w art. 7 lit. f) tej dyrektywy.

62 W powyższym względzie należy także przypomnieć, że art. 7 lit. f) wspomnianej dyrektywy stoi na przeszkodzie temu, by państwo członkowskie wykluczyło w sposób kategoryczny i ogólny w odniesieniu do określonych kategorii danych osobowych możliwość ich przetwarzania, nie dopuszczając do ważenia przeciwstawnych praw i interesów występujących w indywidualnym przypadku. Państwo członkowskie nie może zatem określić w stosunku do tych kategorii w sposób ostateczny rezultatu ważenia przeciwstawnych praw i interesów, nie dopuszczając do innego rezultatu będącego wynikiem szczególnych okoliczności konkretnego przypadku (zob. podobnie wyrok z dnia 24 listopada 2011 r., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, pkt 47, 48).

63 Uregulowanie takie jak uregulowanie będące przedmiotem sporu w postępowaniu głównym ogranicza – w odniesieniu do przetwarzania danych osobowych użytkowników stron internetowych mediów online – zakres zasady przewidzianej w art. 7 lit. f) dyrektywy 95/46, wykluczając możliwość ważenia celu polegającego na zagwarantowaniu ogólnej funkcjonalności mediów online z interesem lub podstawowymi prawami i wolnościami tych użytkowników, które wymagają zgodnie z tym przepisem ochrony na podstawie art. 1 ust. 1 tej dyrektywy.

64 Z całości powyższych rozważań wynika, że na pytanie drugie należy odpowiedzieć, iż art. 7 lit. f) dyrektywy 95/46 należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu państwa członkowskiego, na podstawie którego dostawca usług medialnych online może gromadzić i wykorzystywać dane osobowe użytkownika tych usług – w braku jego zgody – tylko wtedy, gdy takie gromadzenie i wykorzystywanie są konieczne do umożliwienia konkretnego skorzystania ze wspomnianych usług przez tego użytkownika i zafakturowania kosztów takiego korzystania, przy czym cel polegający na zapewnieniu ogólnej funkcjonalności tychże usług nie może uzasadniać korzystania z tych danych po zakończeniu przeglądania danych mediów.

W przedmiocie kosztów

65 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (druga izba) orzeka, co następuje:

1) **Artykuł 2 lit. a) dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych należy interpretować w ten sposób, że dynamiczny adres protokołu internetowego zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu tego przepisu, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby.**

2) **Artykuł 7 lit. f) dyrektywy 95/46 należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu państwa członkowskiego, na podstawie którego dostawca usług medialnych online może gromadzić i wykorzystywać dane osobowe użytkownika tych usług – w braku jego zgody – tylko wtedy, gdy takie gromadzenie i wykorzystywanie są konieczne do umożliwienia konkretnego skorzystania ze wspomnianych usług przez tego użytkownika i zafakturowania kosztów takiego korzystania, przy czym cel polegający na zapewnieniu ogólnej funkcjonalności tychże usług nie może uzasadniać korzystania z tych danych po zakończeniu przeglądania danych mediów.**

Podpisy