Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
M. CAMPOSA SÁNCHEZA-BORDONY
przedstawiona w dniu 12 maja 2016 r.*

Sprawa C-582/14

Patrick Breyer
przeciwko
Bundesrepublik Deutschland

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Bundesgerichtshof (federalny trybunał sprawiedliwości, Niemcy)]

Przetwarzanie danych osobowych — Dyrektywa 95/46 — Artykuł 2 lit. a) i art. 7 lit. f) — Pojęcie „danych osobowych" — Adresy IP — Przechowywanie przez dostawcę usług mediów elektronicznych — Prawo krajowe, które nie pozwala na uwzględnienie uzasadnionego interesu administratora danych

1. Adres protokołu internetowego (zwany dalej „adresem IP") to ciąg liczb binarnych, przydzielany urządzeniu (komputerowi, tabletowi, smartfonowi), które go identyfikuje i umożliwia dostęp do sieci łączności elektronicznej. Urządzenie służące do połączenia z Internetem musi posłużyć się sekwencją liczb dostarczoną przez dostawców dostępu do sieci. Adres IP przesyłany jest do serwera, na którym jest zarejestrowana wyświetlana strona internetowa.

2. W szczególności dostawcy dostępu do sieci (co do zasady firmy telekomunikacyjne) przyznają swoim klientom przy każdym połączeniu z Internetem tymczasowe tzw. dynamiczne adresy IP i zmieniają je przy każdym późniejszym połączeniu. Spółki te prowadzą rejestr, w którym widnieje informacja, jaki adres IP został przyznany w danej chwili określonemu urządzeniu**.

3. Również właściciele stron internetowych, do których uzyskuje się dostęp za pomocą dynamicznych adresów IP, prowadzą zwykle rejestry, w których widnieje informacja o stronach, jakie były wyświetlane, a także o tym kiedy to nastąpiło i przy użyciu jakiego dynamicznego adresu IP. Z technicznego punktu widzenia po zakończeniu połączenia internetowego użytkownika rejestry te mogą być przechowywane bez ograniczeń czasowych.

4. Dynamiczny adres IP nie wystarcza sam w sobie do tego, aby usługodawca zidentyfikował użytkownika swojej strony internetowej. Jednakże może uczynić to łącząc ten dynamiczny adres IP z innymi dodatkowymi danymi znajdującymi się w rękach dostawcy dostępu do sieci.

* Język oryginału: hiszpański.

** Artykuł 5 dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54) nakładał m.in. obowiązek zatrzymania w celu dochodzenia, wykrywania i ścigania poważnych naruszeń „daty i godziny zalogowania i wylogowywania sesji internetowej […] włącznie z adresem protokołu komunikacyjnego dynamicznego lub statycznego (IP), przydzielonym przez dostawcę usług internetowych dla danej komunikacji oraz identyfikatorem użytkownika abonenta lub zarejestrowanego użytkownika".

5. W niniejszej sprawie kwestią sporną jest to, czy dynamiczne adresy IP stanowią dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE***. Aby udzielić odpowiedzi na to pytanie, należy najpierw ustalić znaczenie, jakie ma w tym względzie fakt, że dodatkowe dane konieczne do identyfikacji użytkownika nie znajdują się w posiadaniu właściciela strony internetowej, lecz osoby trzeciej (tj. dostawcy usługi dostępu do sieci).

6. Kwestią tą Trybunał się jeszcze nie zajmował, gdyż w pkt 51 wyroku Scarlet Extended**** co prawda stwierdził, że adresy IP „stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników", lecz uczynił to w kontekście, w którym zbieranie i identyfikacja adresów IP były dokonywane przez dostawcę dostępu do sieci*****, a nie – jak w niniejszym przypadku – dostawcę treści.

7. Jeśli dynamiczne adresy IP stanowią w przypadku dostawcy usług internetowych dane osobowe, należy wówczas zbadać, czy przetwarzanie ich jest objęte zakresem stosowania dyrektywy 95/46.

8. Możliwe jest, że nawet jeżeli adresy te stanowią dane osobowe, to nie muszą one być objęte ochroną wynikającą z dyrektywy 95/46; sytuacja taka miałaby miejsce np. wówczas, gdy celem ich przetwarzania byłoby wykonywanie czynności w sprawach karnych przeciwko pomiotom mogącym przeprowadzić atak na stronę internetową. W takim przypadku dyrektywa 95/46 nie znajdzie zastosowania, zgodnie z jej art. 3 ust. 2 tiret pierwsze.

9. Należy dodatkowo wyjaśnić to, czy usługodawca, który rejestruje dynamiczne adresy IP w momencie, gdy użytkownik uzyskuje dostęp do strony internetowej (w tym przypadku Republika Federalna Niemiec), działa jako władza publiczna, czy też może jako osoba prywatna.

10. Jeżeli zastosowanie znajdzie tu dyrektywa 95/46, należałoby określić wreszcie, do jakiego stopnia jej art. 7 lit. f) stoi na przeszkodzie stosowaniu przepisów krajowych, które ograniczają zakres jednej z ustanowionych w nim przesłanek uzasadniających przetwarzanie danych osobowych.

I – Ramy prawne

A – *Prawo Unii*

11. Motyw 26 dyrektywy 95/46 ma następujące brzmienie:

„(26) 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 [racjonalnie rzecz biorąc] 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".

*** Dyrektywa 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, wyd. spec. w jęz. polskim rozdz. 13, t. 13, s. 355).

**** Wyrok z dnia 24 listopada 2011 r. (C-70/10, EU:C:2011:771), pkt 51.

***** Podobnie jak w wyroku z dnia 19 kwietnia 2012 r. Bonnier Audio i in. (C-461/10, EU:C:2012:219), pkt 51 i 52.

12. Zgodnie z art. 1 dyrektywy 95/46:

„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".

13. Zgodnie z art. 2 dyrektywy 95/46:

„Na użytek niniejszej dyrektywy stosuje się następujące definicje:

a) »dane osobowe« oznacza 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« oznacza dowolną operację lub zestaw operacji dokonywanych na danych osobowych w sposób zautomatyzowany lub inny, takich jak gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie.;

[…]

d) »administrator danych« oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny organ, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych; 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;

[…]".

14. Artykuł 3 dyrektywy 95/46, zatytułowany „Zakres obowiązywania" stanowi:

„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 gospodarcza państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego;

[…]".

15. Rozdział II dyrektywy 95/46, zatytułowany „Ogólne zasady legalności przetwarzania danych osobowych" otwiera art. 5, zgodnie z którym „[p]aństwa członkowskie określą, w granicach przepisów zawartych w niniejszym rozdziale, bardziej szczegółowe warunki ustalania legalności przetwarzania danych osobowych".

16. Na mocy art. 6 dyrektywy 95/46:

„1. Państwa członkowskie zapewniają, aby dane osobowe były:

a) przetwarzane rzetelnie i legalnie;

b) gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami pod warunkiem ustanowienia przez państwa członkowskie odpowiednich środków zabezpieczających;

c) prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone i/lub przetwarzane dalej;

d) prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane;

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane. Państwa członkowskie ustanowią odpowiednie środki zabezpieczające dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych.

2. Na administratorze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1".

17. Zgodnie z art. 7 dyrektywy 95/46:

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

a) podmiot danych jednoznacznie wyraził na to zgodę; lub

b) przetwarzanie jest konieczne dla realizacji umowy, której stroną jest podmiot danych, lub w celu podjęcia działań na życzenie podmiotu danych 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; lub

f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, 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"

18. Zgodnie z art. 13 dyrektywy 95/46:

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

a) bezpieczeństwa narodowego;

b) obronności;

c) bezpieczeństwa publicznego;

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

e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi;

f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c)–e);

g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób.

[…]".

B – *Prawo krajowe*

19. Paragraf 12 Telemediengesetz (TMG) [ustawy o elektronicznych usługach informacyjnych i komunikacyjnych, 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, jeżeli zezwala na to niniejsza ustawa lub inny przepis prawny, który odnosi się wyraźnie do telemediów lub jeżeli użytkownik wyraził na to zgodę.

****** Ustawa z dnia 26 lutego 2007 r. (BGBl. 2007 I, s. 179).

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".

20. Zgodnie z § 15 TMG:

„(1) Usługodawca może gromadzić i wykorzystywać dane osobowe użytkownika tylko wtedy, jeżeli 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 i

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 […]".

21. Zgodnie z § 3 ust. 1 Bundesdatenschutzgesetz (federalnej ustawy o ochronie danych; zwanej dalej „BDSG")******* „danymi osobowymi są szczegółowe dane dotyczące sytuacji osobistej lub rzeczowej zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą)".

II – Okoliczności faktyczne

22. Patrick Breyer skierował przeciwko Republice Federalnej Niemiec powództwo o zaniechanie rejestracji adresów IP.

23. Liczne niemieckie instytucje publiczne prowadzą ogólnodostępne portale internetowe, na których udostępniają aktualne informacje. Aby chronić się przed atakami i umożliwić ściganie na drodze prawnej podmiotów, które dopuściły się takich ataków, 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.

24. Patrick Breyer w przeszłości przeglądał różne tego rodzaju strony internetowe. W swoim powództwie domaga się, by nałożyć na Republikę Federalną Niemiec obowiązek zaniechania rejestrowania – lub zlecania rejestrowania przez osoby trzecie – adresu IP systemu nadrzędnego swego komputera, o ile rejestracja tego adresu nie jest konieczna do przywrócenia dostępności telemediów w przypadku awarii.

******* Ustawa z dnia 20 grudnia 1990 r. (BGBl 1990 I, s. 2954).

25. Powództwo P. Breyera zostało oddalone w pierwszej instancji. Jego apelacja została jednak uwzględniona w części, a Republice Federalnej Niemiec nakazano zaniechać przechowywania adresu IP po zakończeniu danej sesji. Zaniechanie to zostało nakazane pod warunkiem, że powód poda w trakcie dostępu swoje dane osobowe, także w formie adresu e-mail, i jeżeli rejestracja nie jest konieczna do przywrócenia dostępności usługi telekomunikacyjnej.

III – Wniesione pytanie

26. Po wniesieniu rewizji przez obie strony VI izba Bundesgerichtshof (federalny trybunał sprawiedliwości, Niemcy) sformułowała następujące pytania prejudycjalne, wniesione do Trybunału Sprawiedliwości w dniu 17 grudnia 2014 r.:

„1) Czy art. 2 lit. a) dyrektywy 95/46/WE powinien być interpretowany w ten sposób, że adres protokołu internetowego (adres IP), który usługodawca 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) dyrektywy o ochronie danych stoi na przeszkodzie przepisowi prawa krajowego, zgodnie z którym usługodawca może gromadzić i wykorzystywać dane osobowe użytkownika bez jego zgody tylko wtedy, gdy jest to konieczne do umożliwienia i zafakturowania konkretnego skorzystania z telemediów [usług telekomunikacyjnych] przez danego użytkownika, i zgodnie z którym cel polegający na zapewnieniu ogólnego funkcjonowania telemediów [usług telekomunikacyjnych] nie może uzasadniać korzystania z tych danych po zakończeniu danej sesji?”.

27. Jak wyjaśnia sąd odsyłający, powód mógłby domagać się zgodnie z prawem niemieckim zaniechania rejestracji adresów IP, jeżeli ich przechowywanie stanowiłoby, w świetle prawa ochrony danych osobowych, ogólnie rzecz biorąc bezprawne naruszenie jego dóbr osobistych, a mówiąc dokładniej – prawa do „informacyjnego samostanowienia” [§ 1004 ust. 1, § 823 ust. 1 Bürgerliches Gesetzbuch (niemieckiego kodeksu cywilnego) w związku z art. 1 i 2 Grundgesetz (niemieckiej Ustawy Zasadniczej)].

28. Taka sytuacja miałaby miejsce a) gdyby adres IP – w każdym razie w powiązaniu z datą dostępu do strony internetowej – zaliczał się do „danych osobowych” w rozumieniu art. 2 lit. a) w związku z motywem 26 zdanie drugie dyrektywy o ochronie danych lub § 12 ust. 1 i 3 TMG w związku z § 3 ust. 1 BDSG b) i gdyby nie istniały podstawy do zezwolenia na określone działanie w rozumieniu art. 7 lit. f) dyrektywy o ochronie danych lub § 12 ust. 1 i 3, § 15 ust. 1 i 4 TMG.

29. Zdaniem Bundesgerichtshof (federalnego trybunału sprawiedliwości) w celu dokonania wykładni prawa krajowego (§ 12 ust. 1 TMG) konieczne jest ustalenie tego, jak należy rozumieć osobowy charakter danych, o których mowa w art. 2 lit. a) dyrektywy 95/46.

30. Dodatkowo sąd a quo wskazuje, że skoro zgodnie z § 15 ust. 1 TMG usługodawca może gromadzić i wykorzystywać dane osobowe użytkownika tylko wtedy, jeżeli jest to konieczne do umożliwienia korzystania z usług telekomunikacyjnych i zafakturowania kosztów takiego korzystania (dane o korzystaniu) ********, to wykładnia tego przepisu wewnętrznego jest związana z wykładnią art. 7 lit. f) dyrektywy 95/46.

******** Zdaniem Bundesgerichtshof (federalnego trybunału sprawiedliwości) danymi o korzystaniu są dane umożliwiające identyfikację użytkownika, dane na temat rozpoczęcia i zakończenia oraz zakresu danego korzystania oraz dane na temat usług telekomunikacyjnych, z których korzystał użytkownik.

IV – Postępowanie przez Trybunałem. Twierdzenia stron

31. Uwagi na piśmie złożyły rządy niemiecki, austriacki i portugalski oraz Komisja. Jedynie ta ostatnia instytucja, jak również P. Breyer wzięli udział w rozprawie, która odbyła się w dniu 25 lutego 2016 r., a z udziału w której zrezygnował rząd niemiecki.

A – *Twierdzenia stron w związku z pierwszym pytanie prejudycjalnym*

32. Zdaniem P. Breyera stanowią dane osobowe również te dane, których połączenie jest wyłącznie możliwe z teoretycznego punktu widzenia, tj. jeżeli wyjść z założenia o potencjalnym abstrakcyjnym niebezpieczeństwie, niezależenie od tego czy w praktyce dojdzie to takiego połączenia. Jego zdaniem fakt, iż organ może być względnie niezdolny do zidentyfikowania osoby posługując się adresem IP nie oznacza, że należy wykluczyć istnienie takiego zagrożenia w przypadku tej osoby. Dodatkowo, jak twierdzi, istotne znaczenie ma okoliczność, że Niemcy przechowują jego dane dotyczące IP, aby w razie czego dokonać identyfikacji ewentualnych ataków lub wszcząć postępowanie karne, co jest możliwe na gruncie § 113 TMG i miało miejsce w licznych przypadkach.

33. Zdaniem rządu niemieckiego na pierwsze pytanie należy odpowiedzieć przecząco. Według niego dynamiczne adresy IP nie ujawniają jeszcze osoby „zidentyfikowanej” w rozumieniu art. 2 lit. a) dyrektywy 95/46. W celu stwierdzenia tego, czy dostarczają one informacji o osobie „możliwej do zidentyfikowania” w rozumieniu tego przepisu, badanie możliwości zidentyfikowania powinno zostać przeprowadzone przy pomocy kryteriów „względnych”. Tak jego zdaniem wynika z motywu 26 dyrektywy 95/46, zgodnie z którym należy wziąć pod uwagę jedynie środki, „jakimi może [racjonalnie rzecz biorąc] posłużyć się administrator danych” lub osoba trzecia do zidentyfikowania danej osoby. Zdaniem rządu niemieckiego sformułowanie to wskazuje na to, że prawodawca Unii nie zamierzał uwzględnić w zakresie zastosowania dyrektywy 95/46 tych sytuacji, w których istnieje obiektywna możliwość identyfikacji przez jakąkolwiek osobę trzecią.

34. Rząd niemiecki przyjmuje również, że pojęcie „danych osobowych” w rozumieniu art. 2 lit. a) dyrektywy 95/46 należy interpretować w świetle celu tej dyrektywy, tj. przestrzegania praw podstawowych. Konieczność ochrony osób fizycznych może być różnie postrzegana w zależności od tego, kto posiada te dane i czy podmiot ten dysponuje środkami, które może zastosować w celu użycia ich do identyfikacji.

35. Rząd niemiecki uważa, że P. Breyer nie może zostać zidentyfikowany za pomocą adresów IP w połączeniu z innymi danymi, które przechowują dostawcy treści. W tym celu konieczne byłoby skorzystanie z informacji, jakimi dysponują dostawcy dostępu do Internetu, którzy w braku podstawy prawnej nie mogą udostępnić ich dostawcom treści.

36. Natomiast zdaniem rządu austriackiego odpowiedź powinna być twierdząca. Zgodnie z motywem 26 dyrektywy 95/46 do tego, aby jakaś osoba była uznana za możliwą do zidentyfikowania nie jest konieczne, aby wszystkie dane identyfikacyjne znajdowały się w rękach jednego podmiotu. Zatem adres IP może stanowić dane osobowe, jeżeli osoba trzecia (jak np. dostawca dostępu do Internetu) dysponuje środkami służącymi identyfikacji właściciela adresu, a identyfikacja może być przeprowadzona bez przezwyciężania nadmiernych trudności.

37. Rząd portugalski skłania się również do udzielenia odpowiedzi twierdzącej, uznając, że adres IP w połączeniu z datą dostępu do strony stanowi dane osobowe ze względu na to, że może prowadzić do identyfikacji użytkownika przez podmiot inny niż ten, który zachował adres IP.

38. Komisja również proponuje udzielenie odpowiedzi twierdzącej, odwołując się do stanowiska Trybunału w sprawie Scarlet Extended********. Zdaniem Komisji z uwagi na to, że gromadzenie adresów IP służy właśnie identyfikacji użytkowników w przypadku cyberataków, skorzystanie z danych dodatkowych, które rejestrowane są przez dostawców dostępu do Internetu, stanowi środek, który „można [racjonalnie rzecz biorąc]" zastosować w rozumieniu motywu 26 dyrektywy 95/46. Wreszcie zdaniem Komisji zarówno cel dyrektywy jak i art. 7 i 8 Karty praw podstawowych UE (zwanej dalej, „kartą") przemawiają za przyjęciem szerokiej wykładni art. 2 lit a) dyrektywy 95/46.

B – *Twierdzenia stron w związku z drugim pytaniem*

39. Patrick Breyer twierdzi, że art. 7 lit. f) dyrektywy 95/46 stanowi klauzulę generalną, której zastosowanie w praktyce wymaga skonkretyzowania. Zgodnie z orzecznictwem Trybunału należy zatem ocenić okoliczności konkretnego przypadku i ustalić, czy istnieją grupy posiadające uzasadniony interes w rozumieniu tego przepisu, skoro w celu zastosowania tego przepisu dozwolone – a nawet niezbędne – jest ustanowienie przepisów szczególnych dla takich grup. W podobnym przypadku, również dla P. Breyera, przepisy krajowe byłyby zgodne z art. 7 lit. f) dyrektywy 95/46, ponieważ nie istnieje interes publicznego portalu w przechowywaniu danych osobowych czy też większą wagę należy przypisać do interesu polegającego na ochronie anonimowości. Jego zdaniem systematyczne przechowywanie danych osobowych nie jest ani dopuszczalne w społeczeństwie demokratycznym, ani konieczne czy też proporcjonalne do osiągnięcia celu polegającego na zapewnieniu funkcjonowania mediów elektronicznych, które jest niewątpliwie możliwe bez rejestrowania tych danych osobowych, co zresztą potwierdzają strony internetowe niektórych ministerstw federalnych.

40. Rząd niemiecki utrzymuje, że nie ma potrzeby udzielać odpowiedzi na drugie pytanie, które zadano jedynie na wypadek, gdyby na pierwsze pytanie udzielono odpowiedzi twierdzącej, co jego zdaniem nie powinno nastąpić z wyżej wymienionych powodów.

41. Rząd austriacki proponuje udzielić odpowiedzi, zgodnie z którą dyrektywa 95/46 nie wyklucza co do zasady przechowywania danych takich jak te sporne w postępowaniu głównym, jeżeli jest to konieczne dla zabezpieczenia prawidłowego funkcjonowania mediów elektronicznych. Zdaniem tego rządu ograniczone w czasie przechowywanie adresu IP trwające dłużej niż konsultowanie strony internetowej może być zgodne z prawem, jeżeli administrator danych osobowych będzie przestrzegał obowiązków spoczywających na nim w zakresie stosowania środków ochrony tych danych zgodnie z art. 17 ust. 1 dyrektywy 95/46. Walka z cyberatakami może uzasadniać przeprowadzanie analizy danych dotyczących wcześniejszych ataków oraz odmowę dostępu do strony internetowej z niektórych adresów IP. To czy przechowywanie danych takich jak te sporne w postępowaniu głównym jest proporcjonalne do celu polegającego na zapewnieniu prawidłowego funkcjonowania mediów elektronicznych, powinno zostać ocenione w każdym przypadku indywidualnie, biorąc pod uwagę zasady określone w art. 6 ust. 1 dyrektywy 95/46.

42. Rząd portugalski broni tezy, że art. 7 lit. f) dyrektywy 95/46 nie sprzeciwia się przepisom krajowym takim jak te stosowane w postępowaniu głównym, ponieważ prawodawca niemiecki dokonał już w tym przepisie wyważenia pomiędzy, z jednej strony, uzasadnionymi interesami administratora danych osobowych, oraz, z drugiej strony, prawami i wolnościami osób, których te dane dotyczą.

43. Zdaniem Komisji przepisy krajowe, za pomocą których dokonywana jest transpozycja art. 7 lit. f) dyrektywy, 95/46 muszą określać cele przetwarzania danych osobowych w taki sposób, aby były przewidywalne dla osoby zainteresowanej. Jej zdaniem niemieckie przepisy nie czynią zadość temu wymogowi, gdyż zgodnie z § 15 ust. 1 TMG przechowywanie adresów IP jest dopuszczalne „jeżeli jest to konieczne do umożliwienia korzystania z telemediów".

******** Wyrok z dnia 24 listopada 2011 r. (C-70/10, EU:C:2011:771), pkt 51.

44. Komisja proponuje zatem odpowiedzieć na drugie pytanie w ten sposób, że przepis ten sprzeciwia się takiej wykładni przepisu prawa krajowego, zgodnie z którą władza publiczna działająca jako usługodawca może gromadzić i korzystać z danych osobowych użytkownika bez jego zgody, nawet jeżeli realizowany w ten sposób cel polega na zapewnieniu prawidłowego funkcjonowania mediów elektronicznych – jeżeli tylko ten przepis prawa krajowego nie wyraża tego celu w sposób wystarczająco jasny i precyzyjny.

V – Ocena

A – *Pierwsze pytanie*

1. Wyznaczenie granic przedstawionego pytania prejudycjalnego

45. Zgodnie z brzmieniem nadanym mu przez Bundesgerichtshof (federalny trybunał sprawiedliwości) za pomocą pierwszego z pytań prejudycjalnych sąd ten zmierza do wyjaśnienia, czy adres IP, za pomocą którego uzyskuje się dostęp do strony internetowej, stanowi dla podmiotu publicznego będącego właścicielem strony dane osobowe [w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE] w przypadku, gdy dostawca dostępu do sieci posiadał dane dodatkowe, pozwalające na identyfikację zainteresowanego.

46. Sformułowane w ten sposób pytanie jest wystarczająco precyzyjne, aby odrzucić na wstępie inne kwestie, jakie mogą powstać *in abstracto* co do charakteru prawnego adresów IP w kontekście ochrony danych osobowych.

47. Po pierwsze, Bundesgerichtshof (federalny trybunał sprawiedliwości) odnosi się wyłącznie do „dynamicznych adresów IP", tj. przyznawanych w sposób tymczasowy dla każdego połączenia do sieci i zmienianych w przypadku następnych połączeń. Nie są to zatem „statyczne adresy IP" charakteryzujące się tym, że są niezmienne i pozwalają na identyfikowanie urządzenia podłączonego do sieci w sposób ciągły.

48. Po drugie sąd odsyłający wychodzi z założenia, że dostawca strony internetowej nie jest w sprawie będącej przedmiotem postępowania głównego w stanie zidentyfikować za pomocą dynamicznego adresu IP osób, które odwiedzają jego strony oraz nie dysponuje również danymi dodatkowym, które w połączeniu z adresem IP umożliwiałyby identyfikację. Bundesgerichtshof (federalny trybunał sprawiedliwości) zdaje się przyjmować, że w tym kontekście dynamiczny adres IP nie stanowi danych osobowych w rozumieniu art. 2 lit. a) dyrektywy 95/46 dla dostawcy strony internetowej.

49. Wątpliwość sądu odsyłającego dotyczy tego, czy dynamiczny adres IP może zostać z punktu widzenia dostawcy strony internetowej zakwalifikowany jako dane osobowe, jeżeli to osoba trzecia dysponuje dodatkowymi danymi, które łącznie z tym adresem identyfikują osoby, które konsultowały dane strony. Dodatkowo, co jest tu szczególnie istotne, Bundesgerichtshof (federalny trybunał sprawiedliwości) nie odnosi się tu do dowolnej osoby trzeciej posiadającej dane dodatkowe, lecz do usługodawcy dostępu do sieci (wyklucza zatem inne osoby posiadające tego typu dane).

50. Poza przedmiotem sporu pozostają zatem, oprócz innych, następujące aspekty: a) czy statyczne adresy IP stanowią dane osobowe zgodnie z dyrektywą 95/46*********; b) czy dynamiczne adresy IP stanowią, zawsze i w każdych okolicznościach, dane osobowe w rozumieniu tej dyrektywy i wreszcie, c) czy zaliczenie dynamicznych adresów IP do danych osobowych jest nieuniknione w sytuacji, gdy istnieje jakakolwiek osoba trzecia zdolna do skorzystania z tych adresów w celu zidentyfikowania użytkowników sieci.

51. Należy zatem wyłącznie rozstrzygnąć, czy dynamiczny adres IP stanowi dla dostawcy usług internetowych dane osobowe w sytuacji, gdy firma telekomunikacyjna oferująca dostęp do sieci (dostawca dostępu) korzysta z danych dodatkowych, które w połączeniu z tym adresem pozwalają zidentyfikować osobę, która uzyskuje dostęp do strony internetowej prowadzonej przez ten pierwszy podmiot.

2. Co do istoty sprawy

52. Kwestia leżąca u podstaw niniejszego odesłania jest przedmiotem intensywnej debaty prowadzonej w doktrynie oraz orzecznictwie niemieckim, w ramach której można wyodrębnić dwa nurty**********. | W ramach pierwszego z nich (opowiadającego się za przyjęciem kryterium „obiektywnego” lub „absolutnego”) użytkownik może zostać zidentyfikowany – i z tego względu adres IP zalicza się do danych osobowych podlegających ochronie – jeżeli, niezależnie od możliwości oraz środków dostawcy usług internetowych, do dokonania identyfikacji wystarczy połączenie dynamicznego adresu IP z danymi dostarczonymi przez osobę trzecią (np. dostawcę dostępu do sieci).

53. Dla zwolenników drugiego nurtu (broniących kryterium tzw. względnego) możliwość skorzystania przy ostatecznej identyfikacji użytkownika z pomocy osoby trzeciej nie wystarcza do nadania dynamicznemu adresowi IP osobowego charakteru. Istotne jest to, czy podmiot mający dostęp do danych ma możliwość posłużenia się nimi w ramach własnych środków w celu identyfikacji danej osoby.

54. Niezależnie od tego, jak brzmią główne tezy tej dyskusji w ramach prawa krajowego, odpowiedź Trybunału winna ograniczyć się do wykładni dwóch przepisów dyrektywy 95/46, do których odwoływał się zarówno sąd a quo jak również strony postępowania, tj. art. 2 lit a)********** i jej motywu 26**********.

********* Problem ten został rozstrzygnięty przez Trybunał w wyrokach: z dnia 24 listopada 2011 r. Scarlet Extended (C-70/10, EU:C:2011:771), pkt 51; z dnia 19 kwietnia 2012 r., Bonnier Audio i in. (C-461/10, EU:C:2012:219). W pkt 51 i 52 tego ostatniego wyroku Trybunał stwierdził, że przekazanie, „w celu ujawnienia nazwy i adresu abonenta Internetu lub użytkownika Internetu korzystającego z adresu IP, z którego, jak się przypuszcza, dokonano nielegalnej wymiany plików zawierających dzieła podlegające ochronie […] stanowi przetwarzanie danych osobowych w rozumieniu art. 2 akapit pierwszy, dyrektywy 2002/58 w związku z art. 2 lit. b) dyrektywy 95/46”.

********** Co do obu nurtów w doktrynie zob. np. M. Schreibauer, w: *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, M. Esser, P. Kramer, K.von Lewinski (red.), Carl Heymanns Verlag/Wolters Kluwer, Kolonia, 2014, 4 wyd., § 11 Telemediengesetz (4–10). J. Nink i J. Pohle: Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze, w: *Multimedia und Recht*, 9/2015, s. 563–567. J. Heidrich, C. Wegener, Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging, w: *Multimedia und Recht*, 8/2015, s. 487–492. H.Leisterer Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr, w: *Computer und Recht*, 10/2015, s. 665–670.

********** Przytoczony w pkt 13.

********** Przytoczony w pkt 11.

55. Dynamiczne adresy IP dostarczają jedynie informacji co do daty i godziny, kiedy miał miejsce dostęp do strony internetowej za pomocą komputera (lub innego urządzenia) oraz odzwierciedlają pewien profil zachowania użytkowników Internetu i z tego względu wiążą się z potencjalną ingerencją w prawo do poszanowania życie prywatnego********** zagwarantowane przez art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności i art. 7 karty, w której świetle, jak również w świetle jej art. 8 należy interpretować dyrektywę 95/46**********. W rzeczywistości strony postępowania nie poddają tego założenia w wątpliwość, które zresztą nie jest jako takie przedmiotem pytania prejudycjalnego.

56. Osoba, do której te szczegóły się odnoszą nie jest „zidentyfikowaną osoba fizyczną". Data i godzina połączenia, jak również źródło numeryczne, nie ujawniają ani bezpośrednio ani natychmiast tożsamości osoby fizycznej będącej właścicielem urządzenia, z którego doszło do uzyskania dostępu do strony internetowej, ani tożsamości użytkownika, który się nim posługuje (może to być jakakolwiek osoba fizyczna).

57. Jednakże w zakresie, w jakim dynamiczny adres IP pomaga określić – albo sam, albo łącznie z innymi danymi – kto jest właścicielem urządzenia użytego w celu uzyskania dostępu do strony internetowej, może zostać uznany za informację o „możliwej do zidentyfikowania osobie"**********.

58. Zgodnie ze stanowiskiem Bundesgerichtshof (federalnego trybunału sprawiedliwości) dynamiczny adres IP nie wystarcza sam w sobie do identyfikacji użytkownika, który, korzystając z niego, uzyskał dostęp do strony internetowej. Przeciwnie, gdyby dostawca usług internetowych mógł zidentyfikować za pomocą dynamicznego adresu IP użytkownika, chodziłoby w sposób niewątpliwy o dane osobowe w rozumieniu dyrektywy 95/46. Nie wydaje się jednak, aby taki był sens pytania prejudycjalnego, z którego wynika, że będący stroną sporu w sprawie głównej dostawcy usług internetowych nie są w stanie zidentyfikować użytkownika wyłącznie na podstawie dynamicznego adresu IP.

59. Strony tego sporu są zgodne co do tego, że ten dynamiczny adres IP umożliwia w połączeniu z innymi danym „pośrednią" identyfikacją użytkownika. Czy potencjalnie istnienie takich danych dodatkowych, możliwych do skojarzenia z dynamicznym adres IP, zezwala, bez ustanawiania żadnych dodatkowych warunków, na zaliczenie go do danych osobowych w rozumieniu dyrektywy? Nasuwa się konieczność rozstrzygnięcia, czy wystarczające jest tu istnienie samej abstrakcyjnej możliwości zapoznania się z tymi danymi, czy też, przeciwnie, koniecznym jest, aby były dostępne dla osoby, która zna już dynamiczny adres IP, lub dla osoby trzeciej.

********** Jak wskazuje rzecznik generalny P. Cruz Villalón w opinii przedstawionej w sprawie Scarlet Extended (C-70/10, EU:C:2011:255), pkt 76, i tak też przyjmuje Europejski Inspektor Ochrony Danych w opinii z dnia 22 lutego 2010 r., na temat bieżących negocjacji Unii Europejskiej w sprawie Umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi (ACTA) (Dz.U. 2010, C 147, s. 1, pkt 24) oraz z dnia 10 maja 2010 r. na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylającej decyzję ramową 2004/68/WSiSW (Dz.U. 2010, C 323, s. 6, pkt 11).

********** Zobacz podobnie wyrok z dnia 23 maja 2003 r. Österreichischer Rundfunk (C-465/00, C-138/01 i C-139/01, EU:C:2003:294), pkt 68, oraz opinia rzecznik generalnej J. Kokott przedstawiona w sprawie Promusicae (C-275/06, EU:C:2007:454), pkt 51 i nast.

********** Należy zakładać – o ile nie zostanie udowodniona teza przeciwna – że osoba ta jest tą, która „surfowała" po Internecie i konsultowała odpowiednią stroną internetową. Mimo wszystko, nawet mimo tego ostatniego założenia, informacje dotyczące daty, godziny oraz numerycznego źródła dostępu do strony internetowej, pozwalają połączyć ten dostęp z właścicielem urządzenia i skojarzyć go pośrednio z wzorem jego zachowania w sieci. Możliwym do wyobrażenia wyjątkiem są adresy IP nadawane lokalnym komputerom jak w przypadku *kafejek internetowych*, których anonimowi użytkownicy są nie do zidentyfikowania, a w przypadku których właścicieli ruch po sieci w lokalu nie dostarcza żadnej istotnej informacji osobowej, z której można by wnioskować co do profilu zachowania w sieci klientów. Jest to poza tym jedyny wyjątek od zasady, że adresy IP to dane osobowe, który został dopuszczony przez grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, utworzoną na mocy dyrektywy 95/46 (tzw. „Grupę Roboczą Artykułu 29"). Zobacz opinia 4/2007 z dnia 20 czerwca 2007 r. w sprawie pojęcia danych osobowych, WP 136, dostępna na stronie internetowej: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

60. Strony skoncentrowały swoje uwagi na interpretacji motywu 26 dyrektywy 95/46, w ramach którego podkreślają sformułowanie „jakimi może [racjonalnie rzecz biorąc] posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby". Pytanie sądu odsyłającego nie się odnosi do danych dodatkowych znajdujących się w posiadaniu usługodawców występujących w postępowaniu głównym. Również nie odnosi się do jakiejkolwiek osoby trzeciej, w której posiadaniu znajdują się te dane dodatkowe (których połączenie z dynamicznym adresem IP umożliwia identyfikację użytkownika), lecz do dostawcy dostępu do sieci.

61. Nie jest zatem koniecznie, aby w tym przypadku Trybunał analizował wszystkie środki, których „może [racjonalnie rzecz biorąc]" użyć strona pozwana w sprawie głównej, aby dynamiczne adresy IP, którymi dysponuje, zostały zaliczone do danych osobowych. Skoro Bundesgerichtshof (federalny trybunał sprawiedliwości) odnosi się wyłącznie do danych dodatkowych znajdujących się rękach osoby trzeciej, to można wywnioskować: a) że albo pozwana nie posiada własnych danych dodatkowych, które pozwalałyby jej na identyfikację użytkownika, b) albo, jeżeli ma dostęp do tych danych, nie jest w stanie racjonalnie rzecz biorąc skorzystać z nich w tym celu jako ich administrator zgodnie z motywem 26 dyrektywy 95/46.

62. To, którą tezę należy przyjąć, zależy od ustaleń faktycznych, których dokonanie należy do wyłącznej kompetencji sądu odsyłającego. Trybunał mógłby dostarczyć mu ogólnych kryteriów mogących posłużyć do dokonania wykładni sformułowania: „sposoby, jakimi może posłużyć się administrator danych", jeżeli Bundesgerichtshof (federalny trybunał sprawiedliwości) miałby jakąś wątpliwość co do możliwości skorzystania przez strony pozwanej w racjonalny sposób z własnych danych dodatkowych. Ponieważ tak nie jest, nie ma moim zdaniem tu miejsca na to, aby Trybunał wprowadzał kryteria interpretacji, które ani nie są niezbędne dla sądu odsyłającego, ani o które sąd ten się nie zwracał.

63. Centralna kwestia pytania prejudycjalnego ogranicza się bowiem do tego, czy dla celów zaliczenia dynamicznego adresu IP do danych osobowych istotna jest okoliczność polegająca na tym, że bardzo określona osoba trzecia – dostawca dostępu do Internetu – dysponuje danymi dodatkowymi, które w połączeniu z tymi adresami pozwalają na zidentyfikowanie użytkownika, który odwiedzał określoną stronę internetową.

64. Ponownie warto odwołać się do motywu 26 dyrektywy 95/46. Zwrot „może [racjonalnie rzecz biorąc] posłużyć się […] inna osoba"********** może prowadzić do przyjęcia interpretacji, zgodnie z którą to, że jakaś osoba trzecia może uzyskać dane dodatkowe (które mogą zostać połączone z dynamicznym adresem IP w celu zidentyfikowania określonej osoby), wystarcza do tego, aby uznać, że adres ten stanowi *eo ipso* dane osobowe.

65. Ta maksymalistyczna interpretacja prowadziłaby w praktyce do uznawania za dane osobowe wszelkiego rodzaju informacji, niezależnie od tego jak bardzo byłyby one same w sobie niewystarczające do identyfikacji użytkownika. Nigdy nie można określić z całą pewnością tego, że nie istnieje osoba trzecia, która posiadałaby dane dodatkowe, jakie można by połączyć z tymi informacjami i które pozwalałby w rezultacie na ujawnienie tożsamości danej osoby.

********** Wyróżnienie moje.

66. Moim zdaniem możliwość polegająca na tym, że postęp w zakresie środków technicznych znacząco utoruje w bliższej lub dalszej przyszłości drogę do coraz bardziej skomplikowanych instrumentów umożliwiających uzyskiwanie i przetwarzanie informacji, uzasadnia przyjmowanie środków ostrożności mających na celu ochronę prywatności. Podjęte zostały starania, aby przy definiowaniu odpowiednich kategorii prawnych w obszarze ochrony danych uwzględnić rodzaje zachowania w sposób wystarczająco szeroki i elastyczny, aby osiągnąć cel polegający na zapewnieniu ochrony w każdym możliwym przypadku**********.

67. Uważam jednak, że ta troska – skądinąd bardzo uzasadniona – nie może prowadzić do zignorowania woli prawodawcy, a wykładnia systemowa motywu 26 dyrektywy 95/46 ogranicza się do „sposobów, jakimi mogą [racjonalnie rzecz biorąc] posłużyć się" *określone osoby trzecie*.

68. Podobnie jak motyw 26 nie odwołuje się do dowolnych środków, które może zastosować administrator danych (w tym przypadku dostawca usług internetowych), lecz jedynie do tych, którymi „może się [racjonalnie rzecz biorąc] posłużyć", należy również rozumieć, że prawodawca odnosi się do „osób trzecich", do których, również racjonalnie rzecz biorąc, może odwołać się administrator danych starający się uzyskać dane dodatkowe w celu identyfikacji. Nie miałoby to miejsca w przypadku, gdyby kontakt z tymi osobami trzecimi byłyby bardzo kosztowny w kategoriach ludzkich oraz gospodarczych czy też praktycznie niewykonalny albo zakazany prawem. W przeciwnym razie, jak wskazywałem wcześniej, praktycznie niemożliwe byłoby dokonanie rozróżnienia pomiędzy jednymi i drugimi środkami, skoro zawsze należałoby dopuścić możliwość istnienia osoby trzeciej, która, niezależnie od tego jak bardzo jest niedostępna z punktu widzenia dostawcy usług internetowych, może dysponować – teraz lub w przyszłości – danymi dodatkowymi odpowiednimi do tego, aby pomóc w identyfikacji użytkownika.

69. Jak wcześniej wskazałem, osobą trzecią, do której odnosi się Bundesgerichtshof (federalny trybunał sprawiedliwości) jest dostawca dostępu do sieci. Z punktu widzenia usługodawcy to do tej właśnie osoby trzeciej jest najlepiej zwrócić się po szczegółowe dane dodatkowe, jeżeli pragnie on zidentyfikować w sposób bardziej efektywny, praktyczny i bezpośredni użytkownika, który miał dostęp do jego strony internetowej przy użyciu dynamicznego adresu IP. Nie chodzi tu bynajmniej o hipotetyczną osobę trzecią, nieznaną i niedostępną, lecz główne ogniwo połączenia z Internetem, o którym wiadomo, że z pewnością jest w posiadaniu danych, jakich potrzebuje usługodawca do identyfikacji użytkownika. Jak bowiem wskazuje sąd odsyłający, chodzi tu o konkretną osobą trzecią, do której ma zamiar zwrócić się pozwana w sprawie głównej w celu uzyskania potrzebnych jej danych dodatkowych.

70. Dostawca dostępu do Internetu to przeważnie osoba trzecia, do której odnosi się motyw 26 dyrektywy 95/46, a do której „może [racjonalnie rzecz biorąc]" zwrócić się usługodawca w postępowaniu a quo. Trzeba jednak wyjaśnić, czy uzyskanie tych posiadanych przez tę osobę trzecią danych dodatkowych, należy uznać za „racjonalnie rzecz biorąc" możliwe w sensie praktycznym.

71. Rząd niemiecki utrzymuje, że skoro informacja znajdującą się w posiadaniu dostawcy dostępu do Internetu stanowi dane osobowe, nie można dostarczyć jej tak po prostu, lecz musi być to dokonane zgodnie z przepisami regulującymi przetwarzanie tych danych**********.

********** Podobne ostrożne i zapobiegawcze podejście stanowi podstawę stanowiska przyjętego przez grupę art. 29, zdaniem której, jak wskazywałem, należy wyjść z założenia, że adresy IP stanowią dane osobowe, uznając za jedyny wyjątek przypadek, w którym usługodawca jest w stanie określić z całą pewnością, które adresy odpowiadają osobom niemożliwym do identyfikacji, jak może być w przypadku klientów *kafejki internetowej*. Zobacz przypis 16, in fine.

********** Punkt 40 i 45 uwag przedstawionych na piśmie.

72. Jest tak niewątpliwie, ponieważ, aby skorzystać z tych informacji, należy postępować zgodnie z ustawodawstwem dotyczącym danych osobowych. Określona informacja „może [racjonalnie rzecz biorąc]" być uzyskana, jeżeli zostaną spełnione warunki, które regulują dostęp do tego typu danych, i z których pierwszym jest możliwość ich zgodnego z prawem przechowywania i przekazywania innym osobom. Prawdą jest, że dostawca dostępu do Internetu jest uprawniony do odrzucenia wniosku o dostarczenie danych zainteresowanych, lecz możliwe jest również rezultat przeciwny. Możliwość przekazania danych – całkowicie „racjonalna" – sprawia sama w sobie, że dynamiczny adres IP, zgodnie z motywem 26 dyrektywy 95/46, staje się z punktu widzenia dostawcy usług internetowych danymi osobowymi.

73. Chodzi tu o środek dopuszczalny w ramach prawa i przez to – „racjonalny". Możliwe do wykorzystania „racjonalnie rzecz biorąc" środki dostępu, o których wspomina dyrektywa 95/46, muszą być z definicji zgodne z prawem**********. Z takiego założenia wychodzi naturalnie sąd odsyłający, na co wskazuje rząd niemiecki**********. Zatem dochodzi tutaj do istotnego ograniczenia dróg dostępu, które są relewantne z prawnego punktu widzenia, skoro muszą to być wyłącznie te zgodne z prawem. Jednak jeżeli takowe istnieją, niezależnie od tego jak bardzo ograniczony jest praktyczny zakres ich stosowania, stanowią one „racjonalny środek" w rozumieniu dyrektywy 95/46.

74. W rezultacie uważam, że na pierwsze pytanie sformułowane przez Bundesgerichtshof (federalny trybunał sprawiedliwości) należy udzielić odpowiedzi twierdzącej. Dynamiczny adres IP powinien zostać uznany w przypadku dostawcy usług internetowych za dane osobowe, a to ze względu na istnienie osoby trzeciej (dostawcy dostępu do sieci), do której można się zwrócić w celu uzyskania innych danych dodatkowych umożliwiających w połączeniu tym z adresem identyfikację użytkownika.

75. Uważam, że za przyjęciem takiego wniosku przemawiają też skutki, do których prowadziłoby zastosowanie rozwiązania przeciwnego. Gdyby dynamiczne adresy IP nie stanowiły w przypadku dostawcy dostępu do Internetu danych osobowych, mogłyby być przechowywane na zawsze i w jakimkolwiek momencie można by było zwrócić się do dostawcy dostępu do Internetu o dane dodatkowe w celu połączenia ich z adresem i doprowadzić do zidentyfikowania użytkownika. W tych okolicznościach, jak przyznaje rząd niemiecki**********, dynamiczny adres IP staje się danymi osobowymi każdorazowo, gdy istnieją już odpowiednie dane dodatkowe służące identyfikacji użytkownika, przy poszanowaniu ustawodawstwa w zakresie ochrony danych.

76. Niemniej jednak chodziłoby tu o dane, których przechowywanie byłoby jedynie możliwe z uwagi na to, że nie były uważane do tej pory za dane osobowe dla usługodawcy. Zatem w rękach tego ostatniego pozostawałaby klasyfikacja prawna dynamicznego adresu IP jako danych osobowych w zależności od tego, czy w przyszłości postanowi on użyć ich w celu identyfikacji użytkownika poprzez ich połączenie z danymi dodatkowymi pochodzącymi od osoby trzeciej. Jednak moim zdaniem decydująca, zgodnie z brzmieniem dyrektywy 95/46, jest możliwość (racjonalna) istnienia „dostępnej" osoby trzeciej, która posiada konieczne środki do identyfikacji osoby, a nie realizacja tej możliwości odwołania się do tego podmiotu trzeciego.

77. Można twierdzić nawet, jak wskazuje rząd niemiecki, że dynamiczny adres IP staje się danymi osobowymi po uzyskaniu go przez dostawcę usługi dostępu do Internetu. Jednak należałoby wówczas uznać, że podobne sklasyfikowanie działałoby w sposób wsteczny, jeżeli chodzi o termin przechowywania adresu IP i w rezultacie trzeba by uznać go za nieistniejący, gdyby doszło do przekroczenia okresu, w trakcie którego można zachowywać dane, które uznano by od samego początku za dane osobowe. Takie podejście doprowadziłoby do rezultatu sprzecznego z duchem

********** Bez znaczenia jest tu okoliczność polegająca na tym, że w tym kontekście dostęp do danych osobowych jest możliwy *de facto* jedynie w ramach działań sprzecznych z ustawą o ochronie danych.

********** Punkt 47 i 48 uwag przedstawionych na piśmie.

********** Punkt 36 uwag przedstawionych na piśmie.

przepisów dotyczących ochrony danych osobowych. Przyczyna uzasadniająca jedynie czasowe przechowywanie tych danych straciłaby na znaczeniu w przypadku zwłoki w uznaniu za istotną cechy charakteryzującej te dane od samego początku, a mianowicie możliwości posłużenia się nimi jako środkiem identyfikacji – jako takimi lub w związku z innymi danymi – osoby fizycznej. Również z tej praktycznej przyczyny bardziej rozsądne wydaje się nadanie odpowiedniego statusu od samego początku.

78. Z tego względu w pierwszej kolejności wyciągam wniosek, że art. 2 lit. a) dyrektywy 95/46 należy interpretować w ten sposób, że adres IP przechowywany przez usługodawcę w związku z dostępem do jego strony internetowej stanowi dla niego dane osobowe w zakresie, w jakim dostawca dostępu do sieci (Internetu) dysponuje danymi dodatkowymi, które pozwalają zidentyfikować osobę, której te dane dotyczą.

B – *Drugie pytanie*

79. W ramach drugiego pytania prejudycjalnego Bundesgerichtshof (federalny trybunał sprawiedliwości) pragnie ustalić, czy art. 7 lit. f) dyrektywy 95/46 stoi na przeszkodzie stosowaniu przepisów krajowych, które dopuszczają gromadzenie i korzystanie z danych osobowych użytkownika bez jego zgody jedynie wówczas, gdy jest to konieczne do umożliwienia i zafakturowania konkretnego skorzystania z usług telekomunikacyjnych przez danego użytkownika, a cel polegający na zapewnieniu funkcjonowania usługi nie może uzasadniać korzystania z tych danych po zakończeniu danej operacji korzystania.

80. Udzielenie odpowiedzi na to pytanie należy poprzedzić szczegółowym omówieniem informacji dostarczonych przez Bundesgerichtshof (federalny trybunał sprawiedliwości), który wskazuje, że sporne dane są przechowywane w celu zapewnienia prawidłowego funkcjonowania stron internetowych takich jak te rozpatrywane w postępowaniu głównym, co ma umożliwiać prawnokarne ściganie cyberataków, których mogą być one obiektem.

81. Należy zatem zadać sobie przede wszystkim pytanie, czy przetwarzanie adresów IP, o którym mowa w postanowieniu odsyłającym, jest objęte wyjątkiem przewidzianym w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46**********.

1. Co do zastosowania dyrektywy 95/46 do przetwarzania spornych danych

82. Republika Federalna Niemiec występuje w postępowaniu w sprawie głównej, jak się wydaje, jako zwykły dostawca usług internetowych, tj. jako podmiot prywatny (i z tego względu *sine imperio*). Wynika z tego, że co do zasady przetwarzanie spornych w sprawie danych nie jest wyłączone z zakresu zastosowania dyrektywy 95/46.

83. Jak stwierdził Trybunał w wyroku Lindqvist**********, działania prowadzone na podstawie art. 3 ust. 2 dyrektywy 95/46 „stanowią w każdym razie działania właściwe państwom i władzom państwowym, obce dziedzinom działalności jednostek”**********. W zakresie, w jakim za przetwarzanie spornych danych odpowiedzialny jest ten, kto – mimo swojego statusu władzy publicznej – działa w rzeczywistości jako podmiot prywatny, zastosowanie znajdzie dyrektywa 95/46.

********** Nie wchodzi w zakres zastosowania dyrektywy 95/46 „przetwarzanie danych osobowych (…) w ramach działalności (…) na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa […] oraz *działalności państwa w obszarach prawa karnego*” (podkreślenie moje).

********** Wyrok z dnia 6 listopada 2003 r. (C-101/01, EU:C:2003:596), pkt 43.

********** Tak samo wyrok z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727), pkt 41.

84. Sąd odsyłający, wskazując na podstawowy cel, jaki administracja niemiecka chce osiągnąć poprzez rejestrowanie dynamicznych adresów IP, podkreśla, iż jest to konieczne do „zapewnienia i utrzymania bezpieczeństwa oraz prawidłowego funkcjonowania jej telemediów". Odnosi się to w szczególności do »rozpoznawania często występujących ataków „odmowy usługi" („denial-of-service") i ochrony przed tymi atakami, w przypadku których infrastruktura telekomunikacyjna zostaje sparaliżowana wskutek celowego i skoordynowanego zalania poszczególnych serwerów dużą ilością zapytań«**********. Przechowywanie w tym celu dynamicznych adresów IP jest powszechne w przypadku właścicieli mających pewne znaczenie stron internetowych i nie stanowi, ani pośrednio, ani bezpośrednio, wykonywania władzy publicznej, efektem czego objęcie tego przechowywania zakresem zastosowania dyrektywy 95/46 nie przysparza zbytnich trudności.

85. Bundesgerichtshof (federalny trybunał sprawiedliwości) stwierdza jednak, że przechowywanie dynamicznych adresów IP przez usługodawców w sprawie głównej związane jest również z zamiarem podejmowania w stosownym momencie przeciwko autorom ewentualnych ataków cybernetycznych działań w obszarze prawa karnego. Czy zamiar ten stanowi przesłankę wystarczającą do wykluczenia przetwarzania tych danych z zakresu stosowania dyrektywy 95/46?

86. Moim zdaniem jeżeli za „działalność w obszarze prawa karnego" uznać korzystanie z ius puniendi państwa przez usługodawców pozwanych w sprawie głównej, mielibyśmy do czynienia z „działalnością państwa w obszarach prawa karnego" i, wobec tego, jednym z wyjątków przewidzianych w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46.

87. W tych okolicznościach zgodnie z orzeczeniem Trybunału w sprawie Huber********** przetwarzanie danych osobowych przez usługodawców z uwagi na względy bezpieczeństwa oraz funkcjonowania technicznego usług telekomunikacyjnych jest objęte zakresem zastosowania dyrektywy 95/46, podczas gdy przetwarzanie danych ukierunkowane na działalność państwa w obszarach prawa karnego pozostawałoby poza jej marginesem.

88. Podobnie, nawet jeżeli Republika Federalna Niemiec, działając jedynie jako usługodawca pozbawiony władzy publicznej nie prowadziłaby działalności w obszarze prawa karnego sensu stricte, lecz, jedynie tak jak ma to miejsce w przypadku każdego innego podmiotu, ograniczałaby się do przekazania spornych adresów IP do organu państwowego w celu podjęcia działań represyjnych, przetwarzanie dynamicznych adresów IP również miałoby za przedmiot działania wykluczone z zakresu stosowania dyrektywy 95/46.

89. Tak wynika z utrwalonego orzecznictwa zawartego w wyroku sprawie Parlament/Rada i Komisja**********, w którym Trybunał potwierdził, że fakt, iż określone dane osobowe „gromadzone są przez podmioty prywatne do celów działalności gospodarczej i że to te podmioty przekazują dane do państwa trzeciego" nie oznacza, iż to przekazanie „nie wchodziło w zakres zastosowania" art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, skoro celem tego przekazania jest prowadzenie przez państwo działań w obszarze prawa karnego, w tym przypadku „następuje bowiem w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego"**********.

********** Punkt 36 wniosku odsyłającego.

********** Wyrok z dnia 16 grudnia 2008 r. (C-524/06, EU:C:2008:725), pkt 45.

********** Wyrok z dnia 30 maja 2006 r. (C-317/04 i C-318/04, EU:C:2006:346), pkt 54–59.

********** *Ibidem*, pkt 59. Dotyczyło to danych osobowych, których przetwarzanie nie było konieczne do świadczenia usług stanowiącego działalność gospodarczą zainteresowanych prywatnych podmiotów (firm lotniczych), lecz które musiały być przekazywane przez te podmioty władzom amerykańskim w celu zapobiegania i zwalczania terroryzmu.

90. Z drugiej strony jeżeli, jak przyjmuję, przez „działalność w obszarze prawa karnego” należy rozumieć, jak wynika to z postanowienia odsyłającego, działalność właściwą jednostce jako podmiotowi uprawnionemu do wszczęcia poprzez odpowiednią czynność działań z zakresu *ius puniendi* państwa, to nie można twierdzić, iż przetwarzanie dynamicznych adresów IP ma na celu działalność państwa w obszarach prawa karnego, wykluczoną z zakresu stosowania dyrektywy 95/46.

91. Przechowywanie i rejestrowanie tych danych służyłoby bowiem bardziej jako środek dowodowy, za pomocą którego właściciel strony internetowej zwraca się do państwa o ściganie, na wniosek strony, zachowania niezgodnego z prawem. Byłby to wreszcie instrument służący obronie na drodze karnej praw przyznanych podmiotowi w ramach danego porządku prawnego (w tym przypadku podmiotowi publicznemu, który działa w ramach prawa prywatnego). Nie różniłby się z tego punktu widzenia od skierowanego przez jakiegokolwiek innego dostawcę usług internetowych wniosku o ochronę państwa zgodnie z przyjętymi w danym porządku prawnym zasadami postępowania w sprawach karnych.

92. Tak więc w zakresie, w jakim władze niemieckie działają jako pozbawiony władzy publicznej dostawca usług internetowych – czego ocenę powinien przeprowadzić sąd odsyłający – przetwarzanie dynamicznych adresów IP jako danych osobowych zawiera się w zakresie zastosowania dyrektywy 95/46.

2. Co do istoty sprawy

93. Paragraf 15 ust. 1 TMG dopuszcza jedynie gromadzenie i korzystanie z danych osobowych użytkownika wówczas, gdy jest to konieczne dla zapewnienia i zafakturowania konkretnego korzystania z usług telekomunikacyjnych. Dokładniej rzecz ujmując, usługodawca może gromadzić i wykorzystywać tzw. „dane o korzystaniu”, tj. dane osobowe użytkownika, jedynie wówczas, gdy jest to konieczne do umożliwienia „korzystania z telemediów i zafakturowania kosztów takiego korzystania”. Dane te należy usunąć po zakończeniu operacji (tj. gdy zakończy się konkretne korzystanie z usług telekomunikacyjnych) – chyba, że muszą zostać zachowane „w celu zafakturowania”, jak stanowi § 15 ust. 4 TMG.

94. Przepis ten zdaje się odrzucać możliwość, aby po zakończeniu połączenia dane o korzystaniu były gromadzone z innych powodów – tj. również w celu zapewnienia ogólnie rozumianego „korzystania z telemediów”. Przyjmując jako punkt odniesienia wyłącznie cel polegający na fakturowaniu jako przyczynę uzasadniającą przechowywanie tych danych, wskazany przepis TMG mógłby zostać odczytany (chociaż ostateczna interpretacja należy do sądu odsyłającego) w ten sposób, że ustanawia on wymóg, aby dane o korzystaniu były wykorzystywane jedynie w celu umożliwienia konkretnego połączenia i po jego zakończeniu były następnie usuwane.

95. Artykuł 7 lit. f) dyrektywy 95/46********** dopuszcza przetwarzanie danych osobowych w szerszym zakresie niż ten przewidziany (dla administratora danych) w § 15 TMG. Przepis niemiecki można uznać zatem za bardziej restrykcyjny niż ten unijny, skoro nie uwzględnia on co do zasady uzasadnionych interesów innych niż ten związany z fakturowaniem usługi, choć dostawca usług internetowych, tj. Republika Federalna Niemiec może mieć również uzasadniony interes w zapewnieniu prawidłowego funkcjonowania jej stron internetowych w zakresie szerszym niż każdy indywidualny przypadek użytkowania**********.

********** Przytoczony w pkt 17.

********** Zobacz pkt 84. Z pewnością właściciele stron internetowych mają uzasadniony interes w tym, aby zapobiegać przypadkom odmowy świadczenia usługi („denials of service”), o której wspomina sąd odsyłający, tj. masowym atakom, jakie czasem przeprowadza się w sposób skoncentrowany przeciwko określonym stronom internetowym w celu ich przesycenia i sprawienia, aby przestały prawidłowo działać.

96. Stanowisko Trybunału zawarte w wyroku ASNEF i FECEMD********** dostarcza wskazówek pomocnych do tego, aby udzielić odpowiedzi na drugie pytanie. Trybunał stwierdził bowiem, iż z celu dyrektywy 95/46 „wynika, że art. 7 dyrektywy 95/46 przewiduje zamknięty i wyczerpujący wykaz przypadków, w których przetwarzanie danych osobowych może zostać uznane za legalne”**********. Zatem „państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych względem kryteriów ustanowionych w art. 7 dyrektywy 95/46, ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu jednego z sześciu kryteriów przewidzianych we wspomnianym artykule”**********.

97. Paragraf 15 TMG nie zawiera dodatkowej, w porównaniu do art. 7 dyrektywy 95/46, przesłanki jeżeli chodzi o zgodne z prawem przetwarzanie danych – jak miało to miejsce w sprawach ASNEF i FECEMD********** – jeżeli jednak dokonuje się wykładni ścisłej, do której odwołuje się sąd a quo, ogranicza on treść przesłanki zawartej w lit. f) tego przepisu: tam gdzie prawodawca Unii odnosi się w sposób generalny do uwzględnienia „[…] uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane”, § 15 TMG odwołuje się jedynie do konieczności „umożliwienia korzystania z telemediów i zafakturowania kosztów takiego korzystania”.

98. Podobnie jak miało to miejsce w sprawie ASNEF i FECEMD**********, również w niniejszej środek krajowy – również w przypadku zinterpretowania go we wcześniej wyjaśniony ścisły sposób – raczej zmienia zakres zastosowania zasady wynikającej z art. 7 dyrektywy 95/46, niż ogranicza się do określenia bardziej szczegółowych warunków tego stosowania, co jest jedynym elementem, w przypadku którego władze każdego państwa członkowskiego dysponują, zgodnie z art. 5 dyrektywy 95/46, pewnym zakresem swobodnego uznania.

99. Zgodnie bowiem z tym ostatnim przepisem: „[p]aństwa członkowskie określą, w granicach przepisów zawartych w niniejszym rozdziale[**********], bardziej szczegółowe warunki ustalania legalności przetwarzania danych osobowych”. Jednakże, jak wskazano w sprawach ASNEF i FECEMD**********, „państwa członkowskie nie mogą również 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 artykule”.

100. Paragraf 15 TMG ogranicza znacznie, w porównaniu z art. 7 lit. f) dyrektywy 95/46, zakres uzasadnionego interesu usprawiedliwiającego przetwarzanie danych, i bynajmniej nie sprowadza się do jego uszczegółowienia lub wejścia w jego istotę w dozwolonych przez art. 5 dyrektywy ramach. Czyni to dodatkowo w sposób kategoryczny i absolutny, nie biorąc pod uwagę tego, że interes polegający na ochronie i zabezpieczaniu powszechnego korzystania z usług telekomunikacyjnych może podlegać wyważeniu z „interes[ami] związanym[i] z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1” dyrektywy 95/46, jak stanowi jej art. 7 lit. f).

********** Wyrok z dnia 24 listopada 2011 r. (C-468/10 i C-469/10, EU:C:2011:777).

********** Ibidem, pkt 30.

********** Wyrok z dnia 24 listopada 2011 r. ASNEF i FECEMD (C-468/10 i C-469/10, EU:C:2011:777), pkt 32.

********** Przypadek, w którym prawo krajowe dodaje do przesłanek z art. 7 lit. f) dyrektywy 95/46 wymóg, aby przetwarzane dane widniały w źródłach dostępnych publicznie.

********** Wyrok z dnia 24 listopada 2011 r. (C-468/10 i C-469/10, EU:C:2011:777).

********** Zawierający art. 5–21 rozdział II dyrektywy 95/46, zatytułowany „Ogólne zasady legalności przetwarzania danych osobowych”.

********** Wyrok z dnia 24 listopada 2011 r. (C-468/10 i C-469/10, EU:C:2011:777), pkt 36.

101. Wreszcie, podobnie jak w sprawach ASNEF i FECEMD**********, ustawodawca niemiecki określa „w stosunku do nich [określonych kategorii danych osobowych] w sposób ostateczny rezultat ważenia przeciwstawnych praw i interesów, tym samym nie dopuszczając do innego rezultatu będącego wynikiem szczególnych okoliczności konkretnego przypadku", efektem czego „nie chodzi już o uszczegółowienie w rozumieniu […] art. 5" dyrektywy 95/46.

102. W tych okolicznościach uważam, że Bundesgerichtshof (federalny trybunał sprawiedliwości) jest zobowiązany interpretować prawo krajowe zgodnie z dyrektywą 95/46, co oznacza, że: a) można uwzględnić, jako jedną z przyczyn uzasadniających przetwarzanie tzw. „danych o korzystaniu", uzasadniony interes dostawcy usług telekomunikacyjnych polegający na chronieniu ich powszechnego użycia i b) można dokonać wyważenia w każdym indywidualnym przypadku interesu usługodawcy z interesem lub podstawowymi prawami i wolnościami użytkownika w celu ustalenia, który z nich zasługuje na ochronę zgodnie art. 1 ust. 1 dyrektywy 95/46**********.

103. Moim zdaniem, jeżeli chodzi o sposób dokonania tego wyważenia w okolicznościach sprawy, w której skierowano postanowienie odsyłające, nie ma potrzeby dodawać niczego więcej. Zresztą zadający pytania prejudycjalne Bundesgerichtshof (federalny trybunał sprawiedliwości) skoncentrował się wyłącznie na kwestii, którą należy rozwiązać przed przeprowadzeniem takiego ważenia, tj. kwestii tego, czy takie ważenie może w ogóle zostać przeprowadzone.

104. Wreszcie wydaje mi się, iż nie ma potrzeby wskazywać, że sąd a quo może wziąć pod uwagę ewentualne przepisy przyjęte przez państwo członkowskie w ramach pozwolenia zawartego w art. 13 ust. 1 lit. d) dyrektywy 95/46 w celu ograniczenia zakresu obowiązków oraz praw przewidzianych w art. 6 dyrektywy, gdy jest to konieczne dla zabezpieczenia m.in. „[…] działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych […]". Do okoliczności tej nie odnosi się również sąd odsyłający, zdając sobie niewątpliwie sprawę z istnienia obu przepisów.

105. W rezultacie proponuję udzielić na drugie pytanie prejudycjalne odpowiedzi, że niezgodny z art. 7 lit. f) dyrektywy 95/46 jest przepis prawa krajowego, zgodnie z którego wykładnią usługodawca nie może, w celu zagwarantowania funkcjonowania usług telekomunikacyjnych, zbierać i przetwarzać bez zgody użytkownika jego danych osobowych po zakończeniu danej operacji użytkowania.

VI – Wnioski

106. Mając na uwadze powyższe, sugeruję, aby Trybunał w następujący sposób odpowiedział na skierowane do niego pytania:

„1) Na mocy art. 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 dynamiczny adres IP, za pomocą którego użytkownik uzyskuje dostęp do strony internetowej dostawcy usług telekomunikacyjnych stanowi dla tego ostatniego „dane osobowe" w zakresie, w jakim dostawca dostępu do sieci posiada inne dane dodatkowe, które w połączeniu z tym dynamicznym adresem IP, umożliwiają identyfikację użytkownika.

********** Wyrok z dnia 24 listopada 2011 r. (C-468/10 i C-469/10, EU:C:2011:777), pkt 47.

********** W trakcie rozprawy P. Breyer bronił się, odrzucając tezę jakoby rejestr dynamicznych adresów IP był konieczny dla zapewnienia prawidłowego funkcjonowania usług internetowych w obliczu ataków. Uważam, że udzielenie uniwersalnej odpowiedzi nie jest możliwe w przypadku tej kwestii, której rozwiązanie powinno właśnie być poprzedzone w każdym poszczególnym przypadku zestawieniem interesu właściciela strony internetowej z prawami i interesami użytkowników.

2) Artykuł 7 lit. f) dyrektywy 95/46 należy interpretować w ten sposób, że cel, jakim jest zapewnienie funkcjonowania usług telekomunikacyjnych, może co do zasady zostać uznany za uzasadniony interes, którego ochrona pozwala na przetwarzanie tych danych osobowych w przypadku, gdy przeważy on nad interesem lub prawami podstawowymi podmiotu, którego te dane dotyczą. Przepis prawa krajowego, który uniemożliwia uwzględnienie tego uzasadnionego interesu, jest niezgodny z wyżej wymienionym przepisem".