Przetwarzanie danych osobowych przez dostawców usług online.

Glosa do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 r., sygn. C-582/14

Spis treści

I. Przedmiot wniosku o wydanie orzeczenia w trybie prejudycjalnym

Wniosek o wydanie orzeczenia w trybie prejudycjalnym został złożony przez niemiecki Federalny Trybunał Sprawiedliwości (dalej: Bundesgerichtshof) i 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) (dalej: dyrektywa).

Problem powstał na tle sporu pomiędzy Patrickiem Breyerem a Republiką Federalną Niemiec w przedmiocie rejestrowania i przechowywania przez państwo adresu protokołu internetowego (dalej: adres IP) Patricka Breyera (dalej: użytkownik) podczas przeglądania przez niego wielu stron internetowych niemieckich służb federalnych.

Podczas każdego z takich połączeń dostawcy usług przyznają użytkownikom bądź statyczny adres IP, bądź dynamiczny adres IP. Ten ostatni zmienia się wraz z każdym połączeniem użytkownika z Internetem. W odróżnieniu od statycznych adresów IP, dynamiczne adresy IP nie dają możliwości utworzenia powiązania (linku) – za pomocą publicznie dostępnych danych – komputera, z którego nastąpiło połączenie i fizycznego podłączenia do sieci, wykorzystywanego przez dostawcę dostępu do Internetu.

Powództwo, jakie użytkownik wytoczył przed niemieckim sądem administracyjnym, miało na celu zakazanie przechowywania (lub zlecania przechowywania przez osoby trzecie) adresu IP systemu hostingowego użytkownika po zakończeniu przeglądania dostępnych publicznie mediów online stron niemieckich służb federalnych, o ile rejestracja adresu IP nie jest konieczna do przywrócenia dostępności mediów online w przypadku awarii.

W pierwszej instancji powództwo zostało oddalone. Sąd apelacyjny częściowo uwzględnił żądanie użytkownika. Nakazał zaniechać przechowywania (lub zlecania przechowywania przez osoby trzecie) adresu IP systemu hostingowego użytkownika po zakończeniu każdej sesji na stronach niemieckich służb federalnych dostępnych publicznie online, przekazanego w trakcie

przeglądania tych stron. Nakaz ten odnosi się do przypadku, gdy ten adres IP jest przechowywany w powiązaniu z datą sesji, do której adres IP się odnosi i gdy użytkownik ujawnił swoją tożsamość w trakcie takiej sesji, także w formie adresu e-mail, wskazującego na tożsamość użytkownika – o ile to przechowywanie nie jest konieczne do przywrócenia dostępności mediów online w przypadku awarii. Zdaniem sądu apelacyjnego, dynamiczny adres IP stanowi dane osobowe użytkownika, jeżeli użytkownik ujawnił swoją tożsamość w trakcie sesji, ponieważ operator strony internetowej może zidentyfikować tego użytkownika poprzez zestawienie jego nazwiska z adresem IP jego komputera. W przypadku, gdy użytkownik nie podaje swojej tożsamości w trakcie przeglądania strony, jedynie dostawca Internetu może powiązać adres IP ze zidentyfikowanym użytkownikiem. Natomiast dla dostawcy usług medialnych online (w tym wypadku: Republiki Federalnej Niemiec) adres IP nie stanowi jednej z danych osobowych, nawet w połączeniu z datą przeglądania strony, do której się on odnosi, zważywszy że użytkownik przedmiotowych stron internetowych nie może zostać zidentyfikowany przez tegoż dostawcę usług medialnych.

II. Stanowiska przed skierowaniem sprawy do Trybunału

Obydwie strony wniosły skargę od orzeczenia sądu apelacyjnego do Federalnego Trybunału Sprawiedliwości. Użytkownik domagał się uwzględnienia żądania o zakazanie przechowywania adresu IP w pełnym zakresie, Republika Federalna Niemiec domagała się zaś nieuwzględnienia wniosku użytkownika w całości. Bundesgerichtshof przyjął, że sporne zapatrywania stron w przedmiotowej sprawie dotyczą dynamicznych adresów IP użytkownika, przechowywanych przez państwo, które działa w charakterze dostawcy usług medialnych online. W zestawieniu z innymi przechowywanymi danymi mają one charakter szczegółowych danych o okolicznościach faktycznych dotyczących użytkownika, ponieważ dostarczają informacji na temat przeglądania przez niego określonych stron lub określonych plików w Internecie w określonym czasie. Dane te nie są wystarczające do ustalenia w sposób bezpośredni tożsamości użytkownika. Operator stron internetowych może zidentyfikować użytkownika jedynie wówczas, gdy dostawca dostępu do Internetu udostępni mu dane o tożsamości użytkownika. W związku z tym, uznanie przechowywanych danych, o których mowa powyżej, za „dane osobowe" zależy od tego czy użytkownik może zostać zidentyfikowany.

Bundesgerichtshof oczekiwał stanowiska Trybunału co do tego czy gdyby uznać dynamiczne adresy IP użytkownika (w połączeniu z datą przeglądania stron) za adresy internetowe, to przechowywanie tych adresów po zakończeniu przeglądania przedmiotowych stron jest dozwolone na podstawie art. 7 lit. f dyrektywy 95/46.

Sąd odsyłający wskazał, że (i) zgodnie z § 15 ust. 1 niemieckiej ustawy o usługach medialnych online (Telemediengesetz – dalej: TMG) dostawcy usług medialnych online mogą gromadzić i wykorzystywać dane osobowe użytkowników tylko wtedy, gdy jest to konieczne do umożliwienia korzystania z danych mediów i rozliczenia kosztów takiego korzystania. Ponadto (ii) według Republiki Federalnej Niemiec przechowywanie przedmiotowych danych jest konieczne do zapewnienia bezpieczeństwa i ciągłości sprawnego funkcjonowania stron serwisów medialnych online, dzięki którym są publicznie udostępniane, w szczególności w celu umożliwienia rozpoznania i zwalczania cyberataków, znanych jako „ataki w postaci odmowy usługi". Zdaniem sądu odsyłającego, w zakresie, w jakim jest konieczne podjęcie przez dostawcę usług medialnych online środków mających na celu zwalczanie takich ataków, środki te mogą zostać uznane za niezbędne

do „umożliwiania korzystania z telemediów" zgodnie z § 15 ust. 1 TMG. Jednakże w doktrynie przeważa bardziej restrykcyjny pogląd, iż gromadzenie i wykorzystywanie danych osobowych użytkownika strony internetowej jest dozwolone jedynie w celu umożliwienia konkretnego korzystania z tej strony, dane te powinny zaś zostać usunięte po zakończeniu korzystania ze strony, o ile dane te nie są konieczne do wystawienia faktury. Taka restrykcyjna interpretacja § 15 ust. 1 TMG stała by na przeszkodzie temu, by przechowywanie adresów IP było generalnie dozwolone w celu zapewnienia bezpieczeństwa i ciągłości należytego funkcjonowania mediów online.

III. Pytania prejudycjalne

Sąd odsyłający miał wątpliwości czy restrykcyjna interpretacja przyjęta przez sąd apelacyjny jest zgodna z art. 7 lit. f dyrektywy w świetle m. in. kryteriów wypracowanych przez Trybunał w pkt 29 i nast. wyroku z dnia 24 listopada 2011 r., ASNF i FECEMD (C-468/10 i C-469/10, EU:C:2011:777).

W związku z tym Bundesgerichtshof zwrócił się do Trybunału z następującymi pytaniami prejudycjalnymi:

1) Czy art. 2 lit. a dyrektywy[1] powinien być interpretowany w ten sposób, że 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 jedynie osoba trzecia (dostawca dostępu do Internetu) dysponuje dodatkową wiedzą, wymaganą do identyfikacji danej osoby?
2) Czy art. 7 lit. f dyrektywy[2] stoi na przeszkodzie przepisowi prawa krajowego, zgodnie z którym dostawca usług medialnych online może gromadzić dane osobowe użytkownika bez jego zgody tylko wtedy, gdy jest to konieczne do umożliwienia skorzystania z tych usług przez użytkownika i zafakturowania przez dostawcę, w związku z czym cel polegający na zapewnieniu ogólnej funkcjonalności mediów online nie może uzasadniać korzystania z tych danych po zakończeniu określonej sesji (dostępu do strony)?

IV. Rozważania Trybunału dotyczące pytania 1

W odniesieniu do pytania pierwszego, kluczowe jest ustalenie, czy sam adres IP mieści się w pojęciu „dane osobowe" także wówczas, gdy inny podmiot (lub podmioty) dysponuje narzędziami niezbędnymi do ustalenia tożsamości osoby użytkownika, a bez tych narzędzi dostawca usług medialnych online nie jest w stanie ustalić tej tożsamości.

Na wstępie Trybunał wskazał, że rozpatrywany stan faktyczny różni się zasadniczo od stanu faktycznego, jaki był rozważany w sprawie *Scarlet Extended* (C-70/10, EU:C:2011:771), w której Trybunał uznał, że adresy IP użytkowników Internetu stanowią chronione dane osobowe, ponieważ pozwalają na precyzyjną identyfikację osoby użytkownika. Powyższe stanowisko Trybunału dotyczyło przypadku, gdy zarówno rejestracja adresów IP, jak i identyfikacja użytkowników jest dokonywana przez dostawcę dostępu do Internetu. Z tego powodu stanowisko to nie może zostać

[1] Art. 2 lit. a dyrektywy określa dane osobowe jako „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".

[2] Art. 7 lit. f dyrektywy przewiduje, że „Państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas, gdy (…) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej lub osób trzecich, którym te dane są ujawniane, o ile interesy takie nie są podporządkowane interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, a które wymagają ochrony na podstawie art. 1 ust. 1".

uznane za adekwatne dla stanu faktycznego i wątpliwości powstałych w sprawie przedstawionej przez Bundesgerichtshof. We wcześniejszej sprawie chodziło o rejestrowanie „statycznych" adresów IP, podczas gdy w rozważanej sprawie występowały „dynamiczne" adresy IP, co jednak nie wydaje się być okolicznością o pierwszorzędnym znaczeniu.

Trybunał zwraca uwagę, że dynamiczny adres IP nie stanowi informacji odnoszącej się do „zidentyfikowanej osoby fizycznej", ponieważ 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. Trybunał wskazuje na konieczność sprawdzenia czy w okolicznościach zaistniałych w analizowanym przypadku adres IP zarejestrowany przez dostawcę treści medialnych online 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 posiadaniu dostawcy dostępu do Internetu tego użytkownika. Z treści art. 2 lit a dyrektywy 95/46 wynika, że osoba możliwa do zidentyfikowania, to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio. Użycie słowa „pośrednio" wskazuje, że aby móc uznać informację za dane osobowe, nie jest konieczne, by ta informacja sama w sobie umożliwiała zidentyfikowanie osoby, której dane dotyczą.

Trybunał wskazał również na motyw 26 dyrektywy 95/46, zgodnie z którym zasady ochrony 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. W ocenie Trybunału, brzmienie motywu 26 wskazuje przy tym, że nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, znajdowały się w rękach jednej tylko osoby. Jednakże dostawca usług treści medialnych online nie zawsze ma możliwość uzyskania od osób trzecich dodatkowych informacji koniecznych do zidentyfikowania osoby, której dane dotyczą. Co do zasady, dostawca treści medialnych nie ma nieograniczonej możliwości uzyskania takowych informacji od innych podmiotów, w tym podmiotów zapewniających dostęp do Internetu. Podmioty te są związane ograniczeniami, jakie z zasady nakłada na nie prawo (np. dotyczące ochrony danych osobowych, dotyczące komunikacji elektronicznej).

W celu uzyskania informacji koniecznych do zidentyfikowania osoby, której dane dotyczą, dostawca dysponuje środkami prawnymi umożliwiającymi zwrócenie się do uprawnionego organu, aby podjął konieczne działania w celu uzyskania tych informacji od dostawcy dostępu do Internetu. Dotyczy to jednak tylko przypadków, określonych przez prawo, np. w celu wszczęcia lub prowadzenia postępowania karnego.

Mając powyższe na uwadze, Trybunał uznał, że 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 ten dostawca 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 dodatkowy informacjom, jakimi dysponuje dostawca dostępu do Internetu tej osoby.

Z praktycznego punktu widzenia powyższe stanowisko dotyczy bardzo ważnej kwestii. Uprawnienia i obowiązki dostawców Internetu związane z przetwarzaniem danych, jakie zostawiają

„ślad" osoby użytkownika jest jasno określony w przepisach i doktrynie. Natomiast uprawnienia i obowiązki dostawców treści medialnych budzą istotne wątpliwości. Znaczenie omawianego wyroku Trybunału jest tym bardziej istotne, że został on wydany na kanwie stanu faktycznego dotyczącego danych tworzących dynamiczny adres IP użytkownika. Powstaje on w trakcie chwilowego kontaktu z usługą medialną, niekiedy być może nawet przypadkowego. Ze względu na szerokie wykorzystanie dynamicznych adresów IP w praktyce, omawiane stanowisko Trybunału powinno mieć istotny wpływ na działalność dostawców treści i usług internetowych.

Wyrok Trybunału ma duże znaczenie praktyczne, rosnące wraz z rozwojem wolumenu usług świadczonych online i wzrostem liczby podmiotów świadczących te usługi.

V. Rozważania Trybunału dotyczące pytania 2

W drugim pytaniu Bundesgerichtshof zawarte są w istocie dwie kwestie.

Po pierwsze, wątpliwość wstępna – czy przetwarzanie danych osobowych będących przedmiotem postępowania głównego, czyli dynamicznych adresów IP użytkowników stron internetowych federalnych służb niemieckich, nie jest wykluczone z zakresu stosowania dyrektywy 95/46 na podstawie art. 3 ust. 2 tiret pierwsze tej dyrektywy[3]; zgodnie z tym przepisem dyrektywa 95/46 nie ma zastosowania do przetwarzania danych w ramach działalności państwa w obszarze prawa karnego. Przepis ten wskazuje przykładowo rodzaje działalności właściwej państwom i władzom państwowym, odmiennych od działalności podmiotów prywatnych. Trybunał uznał co do zasady, że federalne służby niemieckie, które świadczą usługi medialne online i które są odpowiedzialne za przetwarzanie dynamicznych adresów IP, mimo przysługującego im statusu władz publicznych, prowadzą w takim przypadku działalność w charakterze podmiotu prywatnego, poza ramami uzasadniającymi wyłączenie zastosowania dyrektywy. Konieczne jest jednak, by w każdym przypadku sąd krajowy weryfikował okoliczności faktyczne w celu dokonania konkretnego ustalenia.

Po drugie, po przesądzeniu kwestii wstępnej, Trybunał mógł rozważyć czy art. 7 (f) dyrektywy należy interpretować w sposób, który stoi na przeszkodzie uregulowaniu państwa członkowskiego, na podstawie którego dostawca usług medialnych online może gromadzić i wykorzystywać dane osobowe użytkownika tych usług – przy 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. Zagadnienie to jest związane z weryfikacją prawidłowości rozwiązań prawnych zawartych w niemieckim prawie krajowym, czyli w ustawie TMG. Trybunał przypomniał, że wykaz przypadków, w których przetwarzanie danych osobowych może zostać uznane za legalne (bez uzyskania zgody użytkownika usług) jest zamknięty i wyczerpujący. Państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu kryteriów przewidzianych w artykule 7 dyrektywy WE.

[3] Art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 stanowi: „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".

Jednocześnie Trybunał stwierdził, że państwa członkowskie nie mogą wprowadzać innych kryteriów legalności przetwarzania danych osobowych niż kryteria ustanowione w art. 7 dyrektywy, jak również nie mogą modyfikować za pomocą dodatkowych wymogów zakresu sześciu kryteriów przewidzianych w tym artykule 7. W szczególności zasada powyższa nie może zostać zakwestionowana w oparciu o art. 5 dyrektywy[4], z którego nie można wyprowadzać uprawnienia państw członkowskich do wprowadzania innych kryteriów legalności lub modyfikowania za pomocą dodatkowych wymogów, zakresu sześciu kryteriów zawartych w artykule 7 dyrektywy[5].

Gdyby więc zastosować ścisłą wykładnię § 15 TMG, na kanwie którego powstał omawiany wniosek prejudycjalny, przepis ten miałby węższy zakres niż określony w art. 7 (f) dyrektywy, a więc stanowiłby naruszenie przepisu dyrektywy. Zgodnie ze wskazanym powyżej stanowiskiem Trybunału, art. 7f dyrektywy stoi na przeszkodzie wykluczeniu przez państwo członkowskie możliwości przetwarzania określonych kategorii danych, nie dopuszczając do ważenia przeciwstawnych praw i interesów występujących w indywidualnym przypadku.

Z rozważań Trybunału wynika, że zamknięty i wyczerpujący charakter wykazu przypadków, w których przetwarzanie danych osobowych może zostać uznane za legalne bez uzyskania zgody użytkownika usług oznacza, że państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu kryteriów przewidzianych w artykule 7 dyrektywy 95/46 WE. Nie mogą także zawężać w prawie krajowym możliwości przetwarzania danych, jakie zostały przewidziane w dyrektywie. Dotyczy to również art. 7 lit. f dyrektywy.

VI. Orzeczenie Trybunału

1) Artykuł 2 lit. a dyrektywy 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 ten dostawca 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 Internetu dla tej osoby.

2) Artykuł 7 lit. f dyrektywy 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, jeżeli 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.

Tadeusz Piątek
radca prawny
e-mail: Tadeusz.Piatek@dzp.pl

[4] Artykuł 5 dyrektywy stanowi: „Państwa Członkowskie określą, w granicach przepisów zawartych w niniejszym rozdziale, bardziej szczegółowe warunki ustalania legalności przetwarzania danych osobowych".

[5] Trybunał powołuje się na podobne stanowisko w wyr. z dn. 24.11.2011 r., ASNEF i FECEMD, C-468/10 i C-469/10, EU:C:2011:777, pkt 33,34,36.