TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ | DYREKCJA BADAŃ I DOKUMENTACJI

Fiszka tematyczna

OCHRONA DANYCH OSOBOWYCH

Prawo do ochrony danych osobowych jest prawem podstawowym, którego przestrzeganie stanowi istotny cel Unii Europejskiej.

Prawo to zostało uznane w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „kartą"), która w art. 8 stanowi:

„1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.

3. Przestrzeganie tych zasad podlega kontroli niezależnego organu".

To prawo podstawowe jest ściśle związane z prawem do poszanowania życia prywatnego i rodzinnego uznanego w art. 7 karty.

Prawo do ochrony danych osobowych jest przewidziane także w art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), który zastąpił w tym względzie art. 286 WE.

W odniesieniu do prawa wtórnego należy wskazać, że od połowy lat 90. Wspólnota Europejska wprowadza różne instrumenty mające na celu zagwarantowanie ochrony danych osobowych. Dyrektywa 95/46 WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[1], przyjęta na podstawie art. 100 A WE, stanowi podstawowy akt prawny Unii w tej dziedzinie. Dyrektywa ta ustanawia ogólne warunki zgodności z prawem przetwarzania tych danych, a także prawa osób, których te dane dotyczą, i przewiduje w szczególności ustanowienie w państwach członkowskich niezależnych organów nadzorczych.

1 Dyrektywa 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. L 281 z 23.11.1995, s. 31), wersja skonsolidowana z 20.11.2003, uchylona w dniu 25 maja 2018 r. (zob. przypis 5).

Następnie dyrektywę 95/46/WE uzupełniła dyrektywa 2002/58/WE[2], harmonizując przepisy ustawowe państw członkowskich dotyczące ochrony prawa do poszanowania życia prywatnego w odniesieniu w szczególności do przetwarzania danych osobowych w szczególności w sektorze łączności elektronicznej[3].

Poza tym w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (dawne art. 30 i 31 TUE) decyzja ramowa 2008/977/WSiSW[4] reguluje (do maja 2018 r.) ochronę danych osobowych w dziedzinach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych.

Ostatnio Unia Europejska ustanowiła nowe kompleksowe ramy prawne w omawianej dziedzinie. W tym celu w 2016 r. przyjęła rozporządzenie (UE) 2016/679[5] w sprawie ochrony danych, które uchyla dyrektywę 95/46/WE i które będzie bezpośrednio stosowane od dnia 25 maja 2018 r., a także dyrektywę (UE) 2016/680[6] dotyczącą ochrony wspomnianych danych w sprawach karnych, która uchyla decyzję ramową 2008/977/WSiSW i której termin transpozycji przez państwa członkowskie został wyznaczony na 6 maja 2018 r.

Wreszcie w ramach przetwarzania danych osobowych przez instytucje i organy Unii ochrona tych danych jest zapewniana przez rozporządzenie (WE) nr 45/2001[7]. Rozporządzenie to w szczególności umożliwiło utworzenie w 2004 r. organu o nazwie Europejski Inspektor Ochrony Danych. W styczniu 2017 r. Komisja przedstawiła wniosek[8] dotyczący nowego rozporządzenia uchylającego rozporządzenie nr 45/2001 i decyzję nr 1247/2002/WE mające na celu unowocześnienie przepisów w tej dziedzinie i dostosowanie ich do nowego reżimu ustanowionego w rozporządzeniu (UE) 2016/679.

2 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej (dyrektywa dotycząca prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37), wersja skonsolidowana z 19.12.2009.

3 Dyrektywa 2002/58/WE została zmieniona dyrektywą 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 zmieniająca dyrektywę 2002/58/WE (Dz.U. L 105 z 13.4.2006, s. 54). Trybunał stwierdził nieważność tej dyrektywy w wyroku z dnia 8 kwietnia 2014 r., Digital Rights Ireland i Seitlinger i in. (C-293/12 i C-594/12, EU:C:2014:238) z tego względu, że prowadziła ona do poważnego naruszenia praw do poszanowania życia prywatnego i do ochrony danych osobowych (zob. część I.1., zatytułowana „Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych" niniejszej broszury).

4 Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60), uchylona w dniu 6 maja 2018 r. (zob. przypis 6)

5 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. L 119 z 4.5.2016, s. 1), obowiązująca od dnia 25 maja 2018 r.

6 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

7 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

8 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylającego rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE [COM(2017) 8 wersja ostateczna].

I. Prawo do ochrony danych osobowych uznane w Karcie praw podstawowych Unii Europejskiej

1. Zgodność prawa wtórnego Unii z prawem do ochrony danych osobowych

Wyrok z dnia 9 listopada 2010 r. (wielka izba), Volker und Markus Schecke i Eifert (C-92/09 i C-93/09, EU:C:2010:662)[9]

W tej sprawie w postępowaniach głównych przedsiębiorcy rolni weszli w spór z krajem związkowym Hesja w przedmiocie publikacji na stronie internetowej Bundesanstalt für Landwirtschaft und Ernährung (federalnego instytutu rolnictwa i wyżywienia) danych osobowych dotyczących ich jako beneficjentów środków pochodzących z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW). Wspomniani przedsiębiorcy sprzeciwili się tej publikacji, podnosząc w szczególności, że nie była ona uzasadniona nadrzędnym interesem publicznym. Natomiast kraj związkowy Hesja twierdził, że publikacja wspomnianych danych wynikała z rozporządzeń (WE) nr 1290/2005[10] i 259/2008[11], które ustanawiały przepisy dotyczące finansowania wspólnej polityki rolnej i nakładały obowiązek publikowania informacji dotyczących osób fizycznych będących beneficjentami EFRG i EFRROW.

W tym kontekście Verwaltungsgericht Wiesbaden (sąd administracyjny w Wiesbaden, Niemcy) skierował do Trybunału Sprawiedliwości szereg pytań dotyczących ważności niektórych przepisów rozporządzenia (WE) nr 1290/2005 i rozporządzenia (WE) nr 259/2008, które nakładają obowiązek udostępnienia do publicznej wiadomości takich informacji, w szczególności za pośrednictwem stron internetowych prowadzonych przez urzędy krajowe.

W odniesieniu do relacji między uznanym przez kartę prawem do ochrony danych osobowych a obowiązkiem przejrzystości w odniesieniu do funduszy europejskich Trybunał stwierdził, że publikacja na stronie internetowej imiennych danych dotyczących beneficjentów funduszy i kwot przez nich otrzymanych stanowi, ze względu na swobodny dostęp do strony osób trzecich, ingerencję w prawo zainteresowanych beneficjentów do poszanowania ich życia prywatnego w ogólności, a do ochrony danych osobowych, które ich dotyczą, w szczególności (pkt 56–64).

Aby tego rodzaju ingerencja mogła być uzasadniona, powinna ona być przewidziana ustawowo, z poszanowaniem istoty omawianych praw oraz, zgodnie z zasadą proporcjonalności, być niezbędna i rzeczywiście odpowiadać uznanym przez Unię celom interesu ogólnego, a odstępstwa od tych praw i ich ograniczenia powinny sprowadzać się do tego, co ściśle niezbędne" (pkt 65). W tym kontekście Trybunał stwierdził, że wprawdzie w demokratycznym społeczeństwie podatnicy mają prawo do informacji o wykorzystaniu środków publicznych, niemniej Rada i Komisja powinny były znaleźć właściwą równowagę między poszczególnymi wchodzącymi w grę interesami, co wymagało zweryfikowania, zanim przepisy zostały wydane, czy publikacja danych na pojedynczej stronie internetowej w każdym

9 Wyrok ten został omówiony w sprawozdaniu rocznym 2010, s. 11.

10 Rozporządzenia Rady (WE) nr 1290/2005 z dnia 21 czerwca 2005 r. w sprawie finansowania wspólnej polityki rolnej (Dz.U. L 209 z 11.8.2005, s. 1), uchylone rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1306/2013 z dnia 17 grudnia 2013 r. w sprawie finansowania wspólnej polityki rolnej (Dz.U. L 347 z 20.12.2013, s. 549).

11 Rozporządzenie Komisji (WE) nr 259/2008 z dnia 18 marca 2008 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie publikowania informacji na temat beneficjentów środków pochodzących z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW) (Dz.U. L 76 z 19.3.2008, s. 28), uchylone rozporządzeniem wykonawczym Komisji (UE) nr 908/2014 z dnia 6 sierpnia 2014 r. ustanawiającym zasady dotyczące stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1306/2013 w odniesieniu do agencji płatniczych i innych organów, zarządzania finansami, rozliczania rachunków, przepisów dotyczących kontroli, zabezpieczeń i przejrzystości (Dz.U. L 255 z 28.8.2014, s. 59).

państwie członkowskim nie wykracza poza to, co jest niezbędne dla realizacji zamierzonych uzasadnionych celów (pkt 77, 79, 85, 86).

Trybunał stwierdził więc nieważność określonych przepisów rozporządzenia (WE) nr 1290/2005, a także rozporządzenia (WE) nr 259/2008 w całości, w zakresie, w jakim w odniesieniu do osób fizycznych będących beneficjentami pomocy z EFRG i EFRROW przepisy te wymagają publikacji danych osobowych dotyczących każdego beneficjenta, bez wprowadzenia rozróżnienia według odpowiednich kryteriów, takich jak okresy, w których otrzymali tę pomoc, jej częstość czy też rodzaj i wysokość (pkt 92, pkt 1 sentencji). Jednakże Trybunał nie zakwestionował skutków publikacji wykazów beneficjentów takiej pomocy, dokonanej przez organy krajowe na podstawie tych przepisów w okresie przed dniem wydania wyroku (pkt 94, pkt 2 sentencji).

Wyrok z dnia 17 października 2013 r., Schwarz (C-291/12, EU:C:2013:670)

Michael Schwarz zwrócił się do miasta Bochum (Niemcy) o wydanie mu paszportu, nie zgadzając się jednak na to, by przy tej okazji zostały od niego pobrane odciski palców. Władze miasta Bochum oddaliły jego wniosek, w związku z czym M. Schwarz wniósł do Verwaltungsgericht Gelsenkirchen (sądu administracyjnego w Gelsenkirchen, Niemcy) skargę, w której domagał się zobowiązania władz miasta do wydania mu paszportu bez pobierania od niego odcisków palców. Przed wspomnianym sądem M. Schwarz kwestionował ważność rozporządzenia (WE) nr 2252/2004[12], które wprowadziło obowiązek pobierania odcisków palców osób ubiegających się o paszport i podniósł między innymi, że rozporządzenie to narusza prawo do ochrony danych osobowych i prawo do poszanowania życia prywatnego.

W tym kontekście Verwaltungsgericht Gelsenkirchen zwrócił się od Trybunału Sprawiedliwości w trybie prejudycjalnym w celu ustalenia, czy wspomniane rozporządzenie w zakresie, w jakim zobowiązuje osobę występującą o wydanie paszportu do pozostawienia odcisków palców i przewiduje ich zachowanie w paszporcie, jest ważne, w szczególności w świetle karty.

Trybunał odpowiedział twierdząco, orzekając, że o ile pobieranie i przechowywanie odcisków palców przez organy krajowe, przewidziane w art. 1 ust. 2 rozporządzenia (WE) nr 2252/2004, stanowią naruszenie praw do poszanowania życia prywatnego oraz do ochrony danych osobowych, o tyle naruszenie to jest uzasadnione celem polegającym na ochronie paszportów przed ich bezprawnym użyciem.

Przede wszystkim takie ograniczenie, przewidziane w ustawie, realizuje cel interesu ogólnego uznanego przez Unię w zakresie, w jakim zmierza w do uniemożliwienia między innymi nielegalnego wjazdu osób na terytorium Unii (pkt 35–38). Następnie pobieranie i przechowywanie odcisków palców jest właściwe do osiągnięcia tego celu. Po pierwsze bowiem, chociaż metoda weryfikacji tożsamości za pomocą odcisków palców nie jest w pełni wiarygodna, to w sposób znaczący zmniejsza ryzyko wpuszczenia osób nieuprawnionych. Po drugie, brak zgodności odcisków palców posiadacza paszportu z danymi umieszczonymi w tym dokumencie nie oznacza, że danej osobie automatycznie odmówi się wjazdu na terytorium Unii, gdyż jedyną konsekwencją takiej niezgodności jest przeprowadzenie dokładniejszej kontroli w celu definitywnego ustalenia jej tożsamości (pkt 42–45).

Wreszcie, co do koniecznego charakteru takiego przetwarzania, nie podano do wiadomości Trybunału, by istniały środki mogące w wystarczająco skuteczny sposób przyczynić się do celu związanego z ochroną paszportów przed bezprawnym użyciem i jednocześnie naruszające prawa uznane w art. 7 i 8 karty

12 Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie (Dz.U. L 385 z 29.12.2004, s. 1), zmienione rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 6 maja 2009 r. (Dz.U. L 142 z 6.6.2009, s. 1).

w stopniu mniejszym niż metoda związana z odciskami palców (pkt 53). Artykuł 1 ust. 2 rozporządzenia (WE) nr 2252/2004 nie skutkuje przetwarzaniem pobranych odcisków palców wykraczającym poza to, co jest konieczne dla osiągnięcia zamierzonego celu. We wspomnianym rozporządzeniu wyraźnie bowiem stwierdzono, iż odciski palców mogą być wykorzystywane wyłącznie w celu sprawdzenia autentyczności paszportu i tożsamości jego posiadacza. Ponadto art. 1 ust. 2 rozporządzenia zapewnia ochronę przed ryzykiem odczytania danych zawierających odciski palców przez osoby nieupoważnione i przewiduje przechowywanie odcisków palców wyłącznie w samym paszporcie, który znajduje się w wyłącznym posiadaniu osoby, na którą został wystawiony (pkt 54–57, 60, 63).

Wyrok z dnia 8 kwietnia 2014 r. (wielka izba), Digital Rights Ireland i Seitlinger i in. (sprawy połączone C-293/12 i C-594/12, EU:C:2014:238)[13]

U podstaw tego wyroku leżą wnioski o przeprowadzenie oceny ważności dyrektywy 2006/24/WE w sprawie zatrzymywania danych w świetle praw podstawowych do ochrony życia prywatnego i ochrony danych osobowych, przedłożone w ramach sporów krajowych przed sądami irlandzkim i austriackim. W sprawie C-293/12 przed High Court (wysokim trybunałem, Irlandia) zwisł spór pomiędzy spółką Digital Rights a organami irlandzkimi w przedmiocie zgodności z prawem środków krajowych dotyczących zatrzymywania danych dotyczących łączności elektronicznej. W sprawie C-594/12 Verfassungsgerichtshof (trybunał konstytucyjny, Austria) rozpatrywał szereg skarg konstytucyjnych mających na celu stwierdzenie nieważności przepisów krajowych transponujących do prawa austriackiego dyrektywę 2006/24/WE.

We wnioskach o wydanie orzeczenia w trybie prejudycjalnym sądy irlandzki i austriacki zwróciły się do Trybunału Sprawiedliwości z zapytaniem o ważność dyrektywy 2006/24/WE w świetle art. 7, 8 i 11 karty. W szczególności wspomniane sądy zwróciły się do Trybunału o ustalenie, czy ciążący na mocy wspomnianej dyrektywy na dostawcach ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązek zatrzymywania przez określony czas danych związanych z życiem prywatnym danej osoby i jej komunikacją oraz udostępniania ich właściwym organom krajowym stanowi nieuzasadnioną ingerencję we wspomniane prawa podstawowe. Danymi, do których zatrzymywania zobowiązani są wspomniani dostawcy, są w szczególności dane niezbędne do ustalenia źródła oraz odbiorcy połączenia, do określenia daty, godziny i czasu trwania połączenia oraz jego rodzaju, do określenia narzędzia komunikacji i do lokalizacji urządzenia komunikacji ruchomej, w tym między innymi nazwiska i adresu abonenta lub zarejestrowanego użytkownika, numeru nadawcy i odbiorcy połączenia, a także adresu IP w przypadku usług internetowych. Dane te pozwalają w szczególności ustalić, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, a także – czas połączenia oraz miejsce, z którego zostało ono nawiązane. Dzięki nim można też ustalić także częstotliwości komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie.

Trybunał wskazał przede wszystkim, że przepisy dyrektywy 2006/24/WE, które nakładają na dostawcę takie obowiązki, wprowadziły daleko posuniętą ingerencję w zagwarantowane w art. 7 i 8 karty prawa do poszanowania życia prywatnego i ochrony danych osobowych. W tym kontekście Trybunał stwierdził, że owa ingerencja może znaleźć uzasadnienie w realizacji celu interesu ogólnego, jakim jest zwalczanie zorganizowanej przestępczości. W tym zakresie Trybunał stwierdził, po pierwsze, że nałożony przez dyrektywę obowiązek zatrzymywania danych nie narusza istoty praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych, ponieważ nie pozwala na zapoznawanie się z samą treścią komunikatów elektronicznych i przewiduje, że dostawcy powinni przestrzegać pewnych zasad w zakresie ochrony i bezpieczeństwa danych. Po drugie, Trybunał zauważył, że zatrzymywanie danych w celu ich ewentualnego udostępniania właściwym organom krajowym w istocie realizuje cel interesu

13 Wyrok ten został omówiony w sprawozdaniu rocznym 2014, s. 60.

ogólnego polegający na zwalczaniu poważnej przestępczości, co w ostatecznym rozrachunku przekłada się na zapewnienie bezpieczeństwa publicznego (pkt 38–44).

Jednakże Trybunał orzekł, że przyjmując dyrektywę w sprawie zatrzymywania danych, prawodawca Unii przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności. W konsekwencji Trybunał orzekł nieważność tej dyrektywy, uznawszy, że wyjątkowo szeroko i mocno ingeruje ona we wspomniane prawa podstawowe, przy czym przepisy mające zagwarantować, by ingerencja ta rzeczywiście nie wykraczała poza to, co ściśle niezbędne, nie regulują precyzyjnie tej kwestii (pkt 65). Dyrektywa 2006/24/WE obejmuje bowiem generalnie wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, przy czym nie przewidziano w niej jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw (pkt 57–59). Dyrektywa nie przewiduje ponadto żadnego obiektywnego kryterium pozwalającego zagwarantować, że dane będą wykorzystywane wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw, które można uznać za wystarczająco poważne do celów uzasadnienia takiej ingerencji, ani też nie określa żadnych materialnych i proceduralnych przesłanek takiego dostępu lub wykorzystania (pkt 60–62). Co się tyczy wreszcie okresu zatrzymania danych, dyrektywa nałożyła wymóg co najmniej sześciomiesięcznego okresu, nie wprowadzając przy tym żadnego rozróżnienia między kategoriami danych stosownie do zainteresowanych osób lub ewentualnej przydatności danych względem realizowanego celu (pkt 63, 64).

Ponadto, w odniesieniu do wymogów ustanowionych w art. 8 ust. 3 karty Trybunał przyjął, że dyrektywa 2006/24/WE nie ustanawia gwarancji wystarczających do zapewnienia skutecznej ochrony tych danych przed ryzykiem nadużyć oraz przed dostępem do nich i wykorzystywaniem w sposób niedozwolony, a także nie wymaga zatrzymania tych danych na terytorium Unii.

Co za tym idzie, wspomniana dyrektywa nie gwarantuje w pełni kontroli poszanowania wymogów ochrony i bezpieczeństwa przez niezależny organ, do czego jednak wyraźnie zobowiązuje karta (pkt 66–68).

2. Poszanowanie prawa do ochrony danych osobowych w ramach wprowadzania w życie prawa Unii

Wyrok z dnia 21 grudnia 2016 r. (wielka izba), Tele2 Sverige (sprawy połączone C-203/15 i C-698/15, EU:C:2016:970)[14]

W związku z wydaniem wyroku Digital Rights Ireland i Seitlinger i in., stwierdzającego nieważność dyrektywy 2006/24/WE (zob. wyżej) do Trybunału Sprawiedliwości wniesiono dwie sprawy dotyczące ogólnego obowiązku nałożonego w Szwecji i w Zjednoczonym Królestwie na dostawców usług łączności elektronicznej do zatrzymywania danych dotyczących tej łączności, których zatrzymywanie było przewidziane przez unieważnioną dyrektywę.

Dzień po wydaniu wyroku Digital Rights Ireland i Seitlinger i in. przedsiębiorstwo telekomunikacyjne Tele2 Sverige zgłosiło szwedzkiemu organowi nadzoru usług pocztowych i telekomunikacji decyzję o zakończeniu zatrzymywania danych, a także zamiar usunięcia już zarejestrowanych danych (sprawa C-203/15). Prawo szwedzkie zobowiązywało bowiem dostawców usług łączności elektronicznej do zatrzymywania w sposób regularny i ciągły, i to bez żadnych wyjątków, wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej. W sprawie C-698/15 trzy osoby wniosły skargi na brytyjski system zatrzymywania danych, który zezwalał ministrowi spraw wewnętrznych na zobowiązanie publicznych

14 Wyrok ten został omówiony w sprawozdaniu rocznym 2016, s. 62.

operatorów telekomunikacyjnych do zatrzymywania wszystkich danych dotyczących połączeń przez maksymalny okres dwunastu miesięcy, przy czym wykluczone było zatrzymywanie treści tych połączeń.

Kammarrätten i Stockholm (administracyjny sąd apelacyjny w Sztokholmie, Szwecja) oraz Court of Appeal (England and Wales) (Civil Division) [sąd apelacyjny (Anglia i Walia) (izba cywilna), Zjednoczone Królestwo] skierowały do Trybunału Sprawiedliwości pytania prejudycjalne w celu uzyskania wykładni art. 15 ust. 1 dyrektywy 2002/58/WE zwanej „dyrektywą o prywatności i łączności elektronicznej", który zezwala państwom członkowskim na wprowadzenie pewnych wyjątków od przewidzianego w tej dyrektywie obowiązku zapewnienia poufności łączności elektronicznej oraz związanych z nią danych o ruchu.

W wyroku Trybunał najpierw orzekł, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty stoi na przeszkodzie uregulowaniu krajowemu, takiemu jak uregulowanie obowiązujące w Szwecji, przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych dotyczących ruchu i danych o lokalizacji wszystkich abonentów i zarejestrowanych użytkowników w odniesieniu do wszystkich środków łączności elektronicznej. Zdaniem Trybunału takie uregulowanie wykracza poza granice tego, co ściśle niezbędne i nie może zostać uznane za uzasadnione w demokratycznym społeczeństwie, jak tego wymaga wspomniany art. 15 ust. 1 w związku z przytoczonymi wyżej artykułami karty (pkt 99–105, 107, 112, pkt 1 sentencji).

Ten sam przepis, w świetle tych samych artykułów karty, stoi także na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów władz krajowych do zatrzymywania danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby dane te były zatrzymywane na obszarze Unii (pkt 118–122, 125, pkt 2 sentencji).

Trybunał natomiast stwierdził, że art. 15 ust. 1 dyrektywy 2002/58/WE nie stoi na przeszkodzie uregulowaniu, które w ramach prewencji zezwala na ukierunkowane zatrzymywanie danych tego rodzaju w celu zwalczania poważnej przestępczości, pod warunkiem że takie zatrzymywanie danych – w zakresie dotyczącym kategorii danych podlegających zatrzymywaniu, objętych tym działaniem środków łączności, osób, których dotyczy zatrzymywanie danych, oraz przyjętego okresu przechowywania danych – jest ograniczone do tego, co jest ściśle niezbędne. Aby spełniać te wymogi, rozpatrywane uregulowanie krajowe musi, w pierwszej kolejności, zawierać jasne i dokładne reguły pozwalające skutecznie chronić dane przed ryzykiem nadużyć. Uregulowanie to winno w szczególności wskazywać okoliczności i warunki, w których środek związany z zatrzymywaniem danych może zostać zastosowany tytułem prewencji, co pozwoli zagwarantować, by środek ów ograniczał się do tego, co jest ściśle niezbędne. W drugiej kolejności, jeżeli chodzi o materialne przesłanki, jakie musi spełnić uregulowanie krajowe, aby zagwarantować, że będzie ono ograniczone do tego, co jest ściśle niezbędne, zatrzymywanie danych musi zawsze spełniać obiektywne kryteria określające związek między danymi, które mają być zatrzymywane, a realizowanym celem. W szczególności przesłanki te muszą w praktyce umożliwiać określenie rzeczywistego zakresu środka, a w konsekwencji – grona objętych nim osób. Jeżeli chodzi o to ograniczenie, przepisy krajowe winny opierać się na obiektywnych elementach umożliwiających zidentyfikowanie osób, których dane mogą mieć związek, nawet pośredni, z poważną przestępczością, przyczyniać się w taki lub inny sposób do walki z ową przestępczością lub też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego (pkt 108–111).

II. Przetwarzanie danych osobowych w rozumieniu dyrektywy 95/46/WE

1. Przetwarzanie danych osobowych wykluczonych z zakresu stosowania dyrektywy nr 95/46/WE

Wyrok z dnia 30 maja 2006 r. (wielka izba), Parlament/Rada (C-317/04 i C-318/04, EU:C:2006:346)

W związku z atakami terrorystycznymi z dnia 11 września 2001 r. Stany Zjednoczone wydały przepisy zobowiązujące przewoźników lotniczych realizujących połączenia do lub ze Stanów Zjednoczonych do zapewnienia organom amerykańskim elektronicznego dostępu do danych zawartych w ich systemach rezerwacji i kontroli wylotów, określanych jako Passenger Name Records (PNR).

Komisja, uznając, że przepisy te mogą stać w sprzeczności z ustawodawstwem Unii i państw członkowskich w zakresie ochrony danych, rozpoczęła negocjacje z organami amerykańskimi. Po zakończeniu tych negocjacji Komisja w dniu 14 maja 2004 r. wydała decyzję 2004/535/WE[15] stwierdzającą, że Biuro Celne i Ochrony Granic Stanów Zjednoczonych (United States Bureau of Customs and Border Protection, zwane dalej „CBP") zapewnia odpowiedni stopień ochrony danych PNR przekazywanych ze Wspólnoty (zwaną dalej „decyzją o odpowiedniej ochronie"). Następnie, w dniu 17 maja 2004 r. Rada wydała decyzję 2004/496/WE[16] zatwierdzającą zawarcie Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych PNR przez przewoźników lotniczych mających siedziby na terytorium państw członkowskich Wspólnoty.

Parlament Europejski zwrócił się do Trybunału Sprawiedliwości o stwierdzenie nieważności obydwu wspomnianych decyzji, podnosząc w szczególności, że decyzja o odpowiedniej ochronie została wydana ultra vires, że art. 95 WE (obecnie art. 114 TFUE) nie stanowił odpowiedniej podstawy prawnej dla decyzji zatwierdzającej zawarcie porozumienia i że w obydwu przypadkach doszło do naruszenia praw podstawowych.

W odniesieniu do decyzji o odpowiedniej ochronie Trybunał zbadał przede wszystkim, czy Komisja mogła skutecznie wydać decyzję na podstawie dyrektywy 95/46/WE. W tym kontekście stwierdził, że z decyzji o odpowiedniej ochronie wynika, iż przekazywanie CBP danych PNR stanowi przetwarzanie danych w celu ochrony bezpieczeństwa publicznego oraz w ramach działalności państwa w zakresie prawa karnego. Zdaniem Trybunału, o ile rzeczywiście dane PNR są początkowo gromadzone przez przedsiębiorstwa lotnicze w ramach działalności podlegającej prawu Unii, to znaczy sprzedaży biletów lotniczych, uprawniających do korzystania z usługi transportu, o tyle przetwarzanie danych unormowane w decyzji o odpowiedniej ochronie ma zupełnie odmienny charakter. Decyzja ta nie dotyczy bowiem przetwarzania danych niezbędnego w celu świadczenia usług, ale przetwarzania uznanego za niezbędne w celu ochrony bezpieczeństwa publicznego oraz w celu zwalczania przestępczości (pkt 56, 57).

W tym zakresie Trybunał stwierdził, że fakt, iż dane PNR były gromadzone przez podmioty prywatne do celów działalności gospodarczej i że to te podmioty przekazywały je do państwa trzeciego, nie sprzeciwia

15 Decyzja Komisji 2004/535/WE z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Records (PNR) pasażerów lotniczych przekazywanych do biura celnego i ochrony granic Stanów Zjednoczonych (Dz.U. L 235 z 6.7.2004, s. 11).

16 Decyzja Rady 2004/496/WE z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do departamentu bezpieczeństwa wewnętrznego Stanów Zjednoczonych, biuraceł i ochrony granic (Dz.U. L 183 z 20.5.2004, s. 83; sprostowanie Dz.U. L 255 z 30.9.2005, s. 168).

się uznaniu tego przekazywania za przetwarzanie danych wykluczone z zakresu stosowania dyrektywy. Przekazanie to następuje bowiem w ramach ustanowionych przez organy publiczne i mających na celu ochronę bezpieczeństwa publicznego. W konsekwencji Trybunał orzekł, że decyzja o odpowiedniej ochronie nie wchodzi w zakres zastosowania dyrektywy, ponieważ dotyczy przetwarzania danych osobowych, które jest wykluczone z jej zakresu. W związku z tym Trybunał stwierdził nieważność decyzji o odpowiedniej ochronie (pkt 58, 59).

W odniesieniu do decyzji Rady Trybunał stwierdził, że art. 95 WE w związku z art. 25 dyrektywy 95/46/WE nie może stanowić podstawy kompetencji Wspólnoty do zawarcia rozpatrywanego porozumienia ze Stanami Zjednoczonymi. Porozumienie to dotyczy bowiem tego samego przekazywania danych co decyzja o odpowiedniej ochronie, czyli przetwarzania danych wyłączonego z zakresu zastosowania dyrektywy. W konsekwencji Trybunał stwierdził nieważność decyzji Rady zatwierdzającej zawarcie porozumienia (pkt 67–69).

Wyrok z dnia 11 grudnia 2014 r., Ryneš (C-212/13, EU:C:2014:2428)

W odpowiedzi na wielokrotne ataki František Ryneš zainstalował na swym domu kamerę. Po kolejnym ataku na jego dom nagrania ze wspomnianej kamery umożliwiły zidentyfikowanie dwóch podejrzanych, przeciwko którym wszczęto postępowania karne. Zgodność z prawem przetwarzania danych nagranych przez kamerę została podważona przez jednego z podejrzanych przed czeskim urzędem ds. ochrony danych osobowych, który stwierdził, że F. Ryneš naruszył przepisy z zakresu ochrony danych osobowych i wymierzył mu grzywnę.

Nejvyšší správní soud (naczelny sąd administracyjny, Republika Czeska), do którego F. Ryneš odwołał się od orzeczenia wydanego przez Městský soud v Praze (sąd miejski w Pradze), utrzymującego w mocy decyzję urzędu, zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy nagranie zarejestrowane przez F. Ryneša w celu ochrony swego życia, zdrowia i własności stanowiło przetwarzanie danych osobowych nieobjęte zakresem stosowania dyrektywy 95/46/WE z tego względu, że zostało zrealizowane przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze w rozumieniu art. 3 ust. 2 tiret drugie wspomnianej dyrektywy.

Trybunał orzekł, że wykorzystywanie systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze (pkt 35 i sentencja).

W tym względzie Trybunał przypomniał, że ochrona zagwarantowanego przez art. 7 karty prawa podstawowego do poszanowania życia prywatnego wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia były stosowane jedynie wtedy, gdy jest to ściśle niezbędne. W zakresie, w jakim przepisy dyrektywy 95/46/WE regulujące kwestię przetwarzania danych osobowych mogącego naruszyć podstawowe wolności, a w szczególności prawo do poszanowania życia prywatnego, muszą być one bezwzględnie interpretowane z punktu widzenia praw podstawowych, które zostały zawarte we wspomnianej karcie, odstępstwo przewidziane w art. 3 ust. 2 tiret drugie tej dyrektywy musi podlegać ścisłej wykładni (art. 27–29). Ponadto samo brzmienie tego przepisu wyłącza z zakresu stosowania dyrektywy 95/46/WE przetwarzanie danych wykonywane w trakcie czynności o „czysto" osobistym lub domowym charakterze. Jeśli nadzór kamer wideo rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, to nie powinien on być rozumiany jako czynność o czysto „osobistym lub domowym charakterze" w rozumieniu tego przepisu (pkt 30, 31, 33).

2. Pojęcie „danych osobowych”

Wyrok z dnia 19 października 2016 r., Breyer (C-582/14, EU:C:2016:779)[17]

Patrick Breyer wniósł do niemieckich sądów cywilnych o zakazanie Republice Federalnej Niemiec przechowywania – lub zlecania przechowywania przez osoby trzecie – danych informatycznych, które były przekazywane po zakończeniu każdego przeglądania stron internetowych niemieckich służb federalnych. Aby chronić się przed atakami i umożliwić ściganie na drodze karnej „piratów”, dostawca medialnych usług online niemieckich służb federalnych rejestrował dane obejmujące „dynamiczny” adres IP – adres IP, który zmienia się przy okazji każdego nowego połączenia z Internetem – oraz dzień i godzinę przeglądania strony internetowej. W odróżnieniu od statycznych adresów IP, dynamiczne adresy IP nie umożliwiają a priori powiązania – za pomocą publicznie dostępnych plików – danego komputera i fizycznego podłączenia do sieci wykorzystywanego przez dostawcę dostępu do Internetu. Zarejestrowane dane nie dawały same w sobie dostawcy usług medialnych online możliwości zidentyfikowania użytkownika. Natomiast dostawca dostępu do Internetu dysponował dodatkowymi informacjami, które w połączeniu z tym adresem IP umożliwiały identyfikację danego użytkownika.

W tym kontekście Bundesgerichtshof (federalny trybunał sprawiedliwości, Niemcy), do którego została wniesiona skarga rewizyjna („Revision”), zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy adres IP, który dostawca usług medialnych online rejestruje w związku z wejściem na jego stronę internetową, stanowi dla niego dane osobowe.

Trybunał przede wszystkim stwierdził, że do tego, aby dane mogły zostać uznane za „osobowe” w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE, nie jest wymagane, aby wszystkie informacje umożliwiające identyfikację danej osoby znajdowały się w rękach tylko jednego podmiotu. 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/WE (pkt 43, 44).

W konsekwencji Trybunał orzekł, 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 art. 2 lit. a) dyrektywy 95/46/WE, 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 (pkt 49, pkt 1 sentencji).

Wyrok z dnia 20 grudnia 2017 r., Nowak (C-434/16, EU:C:2017:582)

Peter Nowak, księgowy stażysta, nie zdał egzaminu organizowanego przez irlandzki instytut biegłych rewidentów. Postanowił on złożyć, na podstawie art. 4 ustawy o ochronie danych osobowych, wniosek o udostępnienie wszystkich dotyczących go danych osobowych pozostających w posiadaniu instytutu biegłych rewidentów. Instytut biegłych rewidentów przekazał do wiadomości P. Nowaka niektóre dokumenty, lecz odmówił udostępnienia jego arkusza egzaminacyjnego, uzasadniając to w ten sposób, że praca egzaminacyjna nie zawiera „dotyczących go danych osobowych” w rozumieniu ustawy o ochronie danych.

17 Wyrok ten został omówiony w sprawozdaniu rocznym 2016, s. 61.

Ponieważ komisarz ds. ochrony danych także nie uwzględnił jego wniosku o dostęp z tych samych względów, P. Nowak zwrócił się do sądów krajowych. Supreme Court (sąd najwyższy, Irlandia), do którego P. Nowak wniósł odwołanie, zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy art. 2 lit. a) dyrektywy 95/46/WE należy interpretować w ten sposób, że w okolicznościach takich jak te rozpatrywane w postępowaniu głównym pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe dotyczące osoby przystępującej do egzaminu w rozumieniu tego przepisu.

Trybunał w pierwszej kolejności orzekł, że do tego, aby dane mogły zostać uznane za „osobowe" w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE, nie jest wymagane, aby wszystkie informacje umożliwiające identyfikację danej osoby znajdowały się w rękach tylko jednego podmiotu. Ponadto, w przypadku gdy egzaminator, dokonując w ramach egzaminu oceny odpowiedzi udzielonych przez przystępującą do tego egzaminu osobę, nie zna tożsamości tej osoby, podmiot organizujący egzamin, w tym przypadku instytut biegłych rewidentów, dysponuje informacjami umożliwiającymi mu zidentyfikowanie, bez problemów i wątpliwości, osoby przystępującej do egzaminu dzięki jej numerowi identyfikacyjnemu, umieszczonemu na arkuszu egzaminacyjnym lub jego okładce, i przypisanie jej udzielonych odpowiedzi.

W drugiej kolejności Trybunał stwierdził, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego stanowią dane osobowe dotyczące tej osoby. Treść tych odpowiedzi bowiem odzwierciedla poziom wiedzy i umiejętności osoby przystępującej do egzaminu w danej dziedzinie i, w odpowiednim przypadku, sposób jej rozumowania, wnioskowania i przyjęte przez nią krytyczne podejście. Następnie odpowiedzi te są zbierane w celu dokonania oceny kwalifikacji zawodowych osoby egzaminowanej i jej zdolności do wykonywania danego zawodu. Wreszcie wykorzystanie tych informacji, wskutek którego dana osoba może w szczególności zdać egzamin, do którego przystępuje, bądź go nie zdać, może mieć wpływ na prawa i interesy tej osoby, ze względu na to, że wykorzystanie to może warunkować przykładowo szanse owej osoby na wykonywanie danego zawodu bądź zatrudnienie na danym stanowisku. Stwierdzenie, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego stanowią informacje jej dotyczące ze względu na ich treść, cel czy skutek, znajduje również zastosowanie w sytuacji, która dotyczy egzaminu, na którym można korzystać z własnych materiałów referencyjnych („open book exam").

W trzeciej kolejności, w odniesieniu do naniesionych przez egzaminatora komentarzy dotyczących tych odpowiedzi Trybunał stwierdził, że stanowią one, tak jak udzielone na egzaminie przez przystępującą do niego osobę odpowiedzi, informacje dotyczące tej właśnie osoby, zważywszy, że odzwierciedlają one wyrażoną przez egzaminatora opinię czy ocenę indywidualnych osiągnięć danej osoby na tym egzaminie, a w szczególności poziomu jej wiedzy i umiejętności w danej dziedzinie. Komentarze te mają zresztą na celu właśnie udokumentowanie dokonanej przez egzaminatora oceny wyników osiągniętych przez osobę przystępującą do egzaminu i mogą pociągnąć za sobą pewne skutki dla tej osoby.

W czwartej kolejności Trybunał orzekł, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi mogą zostać poddane weryfikacji, w szczególności pod kątem ich prawidłowości i potrzeby ich przechowywania w rozumieniu art. 6 ust. 1 lit. d) i e) dyrektywy 95/46/WE, i mogą zostać sprostowane lub usunięte na podstawie art. 12 lit. b) tej dyrektywy. Udzielenie osobie przystępującej do egzaminu prawa dostępu do tych odpowiedzi i tych komentarzy na mocy art. 12 lit. a) tej dyrektywy służy realizacji przewidzianego w niej celu polegającego na zagwarantowaniu ochrony prawa do poszanowania życia prywatnego egzaminowanego w zakresie przetwarzania dotyczących go danych i to niezależnie od tego, czy osobie przystępującej do egzaminu takie prawo dostępu przysługuje również na podstawie mających zastosowanie do procedury egzaminacyjnej przepisów krajowych. Jednakże Trybunał podkreślił, że przewidziane w art. 12 lit. a) i b) dyrektywy 95/46/WE prawa do dostępu i sprostowania nie obejmują pytań egzaminacyjnych, które nie stanowią jako takie danych osobowych egzaminowanego.

W świetle tych okoliczności Trybunał orzekł, że w okolicznościach takich jak te rozpatrywane w postępowaniu głównym pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE.

3. Pojęcie „przetwarzania danych osobowych"

Wyrok z dnia 6 listopada 2003 r. (w pełnym składzie), Lindqvist (C-101/01, EU:C:2003:596)

Bodil Lindqvist, wolontariuszka w jednej z parafii kościoła protestanckiego w Szwecji, utworzyła na swoim osobistym komputerze strony internetowe i opublikowała na nich dane osobowe dotyczące kilku osób, które pracowały tak jak ona nieodpłatnie w tej parafii. B. Lindqvist została skazana na karę grzywny za wykorzystywanie danych osobowych w ramach zautomatyzowanego przetwarzania bez uprzedniego pisemnego zgłoszenia tego faktu do szwedzkiego Datainspektion (instytucji publicznej zajmującej się ochroną danych przekazywanych drogą informatyczną), ich przekazywanie bez pozwolenia do państw trzecich, a także przetwarzanie szczególnie chronionych danych osobowych.

W ramach postępowania apelacyjnego wszczętego przez B. Lindqvist od tego orzeczenia przed Göta hovrätt (sądem apelacyjnym, Szwecja), sąd ten zwrócił się do Trybunału Sprawiedliwości w trybie prejudycjalnym z pytaniem, czy B. Lindqvist dokonywała „przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany" w rozumieniu dyrektywy 95/46/WE.

Trybunał orzekł, że operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków, np. numeru telefonu lub informacji dotyczących ich warunków pracy i sposobów spędzania przez nie wolnego czasu stanowi „przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany" w rozumieniu tej dyrektywy (pkt 27, pkt 1 sentencji). Takie przetwarzanie danych osobowych w celu wykonywania działalności niezarobkowej lub religijnej nie jest bowiem objęte żadnym z wyjątków od zakresu stosowania dyrektywy, ponieważ nie wchodzi ani w zakres kategorii działalności na rzecz bezpieczeństwa publicznego, ani w zakres kategorii działalności czynności o czysto osobistym lub domowym charakterze, które są wyłączone z zakresu stosowania dyrektywy (pkt 38, 43–48, pkt 2 sentencji).

Wyrok z dnia 13 maja 2014 r. (wielka izba), Google Spain i Google (C-131/12, EU:C:2014:317)

W 2010 r. obywatel hiszpański wniósł do Agencia Española de Protección de Datos (hiszpańskiej agencji ochrony danych, zwanej dalej „AEPD") skargę przeciwko La Vanguardia Ediciones SL, wydawcy szeroko rozpowszechnionego w Hiszpanii dziennika, a także przeciwko Google Spain i Google. Osoba ta twierdziła, że przy wprowadzeniu jej imienia i nazwiska do wyszukiwarki grupy Google pojawiały się linki do dwóch stron dziennika La Vanguardia z 1998 r., na których znajdowało się ogłoszenie w przedmiocie licytacji nieruchomości związanej z ich zajęciem wynikającym z niespłaconych należności. W skardze osoba ta zwróciła się po pierwsze o nakazanie La Vanguardii bądź usunięcia lub zmiany rozpatrywanych stron internetowych, bądź też wykorzystania przez nią narzędzi udostępnianych przez wyszukiwarki internetowe w celu ochrony tych danych. Po drugie, domagała się ona również zobowiązania Google Spain lub Google do usunięcia lub ukrycia jej danych osobowych w taki sposób, by nie były one ujawniane w wynikach wyszukiwania i powiązane z linkami do La Vanguardii.

AEPD oddaliło tę skargę w zakresie dotyczącym La Vanguardii, uznając, że rozpatrywane informacje zostały opublikowane przez wydawcę zgodnie z prawem, lecz uwzględniła ją w zakresie dotyczącym Google Spain i Google i nakazała tym dwóm spółkom podjęcie koniecznych środków w celu usunięcia danych z ich indeksów i uniemożliwienia dostępu do nich w przyszłości. Ponieważ wspomniane spółki

wniosły dwie skargi do Audiencia Nacional (Hiszpania) o stwierdzenie nieważności decyzji AEPD, sąd hiszpański skierował szereg pytań do Trybunału Sprawiedliwości.

W ten sposób Trybunał Sprawiedliwości miał sposobność wyjaśnić pojęcie „przetwarzania danych osobowych" w Internecie w świetle dyrektywy 95/46/WE.

Trybunał zatem orzekł, że prowadzoną przez wyszukiwarki internetowe działalność, która polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie udostępnianiu ich internautom w sposób uporządkowany zgodnie z określonymi preferencjami należy uznać za przetwarzanie danych osobowych, w przypadku gdy informacje te zawierają dane osobowe (pkt 1 sentencji). Trybunał ponadto przypomniał, że operacje, o których mowa w dyrektywie, należy uznać za takie przetwarzanie również w przypadku, gdy dotyczą one wyłącznie informacji opublikowanych już jako takie w mediach. Ogólne odstępstwo od stosowania dyrektywy w takim przypadku w dużej mierze pozbawiałoby tę dyrektywę sensu (pkt 29, 30).

4. Warunki zgodności z prawem przetwarzania danych osobowych w świetle art. 7 dyrektywy 95/46/WE

Wyrok z dnia 16 grudnia 2008 r. (wielka izba), Huber (C-524/06, EU:C:2008:724)[18]

Bundesamt für Migration und Flüchtlinge (federalny urząd ds. migracji i uchodźców, Niemcy) zapewniał prowadzenie scentralizowanego rejestru, w którym są gromadzone określone dane osobowe dotyczące cudzoziemców, którzy zamieszkują na terytorium niemieckim przez okres dłuższy niż trzy miesiące. Rejestr był wykorzystywany w szczególności w celach statystycznych oraz przy wykonywaniu przez służby bezpieczeństwa i policję, jak również organy sądowe przysługujących im kompetencji w zakresie zwalczania i ścigania przestępstw lub czynów zagrażających bezpieczeństwu publicznemu.

Heinz Huber, obywatel Austrii, zamieszkał w Niemczech w 1996 r. w celu prowadzenia tam działalności gospodarczej jako niezależny agent ubezpieczeniowy. H. Huber, uważając się za dyskryminowanego z uwagi na fakt przetwarzania dotyczących go danych zawartych w rozpatrywanym rejestrze, zwłaszcza w świetle tego, że taki rejestr nie jest prowadzony dla obywateli Niemiec, wniósł o wykreślenie tych danych.

W tym kontekście Oberverwaltungsgericht für das Land Nordrhein-Westfalen (wyższa izba sądu administracyjnego Nadrenii Północnej-Westfalii, Niemcy), przed którym zawisł spór, zwrócił się do Trybunału z pytaniem o zgodność z prawem Unii przetwarzania danych osobowych w rozpatrywanym rejestrze.

Trybunał najpierw przypomniał, że prawo obywatela Unii do przebywania na terytorium państwa członkowskiego, którego nie jest obywatelem, nie jest bezwarunkowe, lecz może podlegać ograniczeniom. W rezultacie wykorzystywanie rejestru w celu wspomagania organów właściwych do stosowania przepisów dotyczących prawa pobytu jest co do zasady uzasadnione i – zważywszy na jego charakter – zgodne z zakazem dyskryminacji ze względu na przynależność państwową ustanowionym w art. 12 akapit pierwszy WE (obecnie art. 18 akapit pierwszy TFUE). Jednakże taki rejestr nie może zawierać żadnych innych informacji poza tymi, które są konieczne do tego celu w rozumieniu dyrektywy o ochronie danych osobowych (pkt 54, 58, 59).

18 Wyrok ten został omówiony w sprawozdaniu rocznym 2008, s. 45.

W odniesieniu do pojęcia konieczności w rozumieniu art. 7 lit. e) dyrektywy 95/46/WE Trybunał najpierw przypomniał, że jest to autonomiczne pojęcie prawa Unii, którego wykładnia winna w pełni odpowiadać celowi dyrektywy 95/46/WE, sformułowanemu w jej art. 1 ust. 1. Następnie Trybunał stwierdził, że system przetwarzania danych osobowych jest zgodny z prawem Unii, jeśli zawiera wyłącznie dane konieczne do stosowania tych przepisów przez wspomniane organy oraz jeśli jego scentralizowany charakter pozwala na bardziej skuteczne stosowanie tych przepisów w zakresie prawa pobytu obywateli Unii niebędących obywatelami tego państwa członkowskiego.

W każdym razie nie może zostać uznane za konieczne w rozumieniu art. 7 lit. e) dyrektywy 95/46/WE przechowywanie i przetwarzanie w ramach takiego rejestru danych wymieniających dane osoby z nazwiska w celach statystycznych (pkt 52, 66, 68).

Ponadto w odniesieniu do kwestii wykorzystywania danych zawartych w rejestrze do celów zwalczania przestępczości Trybunał orzekł w szczególności, że cel ten odnosi się do ścigania popełnionych zbrodni i występków, niezależnie od przynależności państwowej osób, które się ich dopuściły. Wobec tego w świetle celu zwalczania przestępczości z punktu widzenia państwa członkowskiego sytuacja jego obywateli nie może różnić się od sytuacji obywateli Unii niebędących obywatelami tego państwa członkowskiego, którzy zamieszkują na jego terytorium. W związku z tym różnica w traktowaniu tych obywateli i obywateli Unii wynikająca z systematycznego przetwarzania danych osobowych dotyczących wyłącznie obywateli Unii niebędących obywatelami danego państwa członkowskiego służąca realizacji celu zwalczania przestępczości stanowi dyskryminację zakazaną przez art. 12 akapit pierwszy WE (pkt 78–80).

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

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) wniosły do Tribunal Supremo (Hiszpania) skargę w trybie sądowo-administracyjnym na szereg artykułów dekretu królewskiego 1720/2007, wprowadzającego w życie ustawę organiczną 15/1999 transponującą dyrektywę 95/46/WE.

W szczególności ASNEF i FECEMD twierdziły, że prawo hiszpańskie w celu umożliwienia przetwarzania danych osobowych, w braku zgody osoby której dotyczą dane, dodało warunek, który nie istnieje w dyrektywie 95/46/WE, wymagający, by wspomniane dane figurowały w „powszechnie dostępnych źródłach" wyliczonych w art. 3 lit. j) ustawy organicznej 15/1999. W tym zakresie podniosły, że ustawa ta i dekret królewski 1720/2007 zawężają zakres art. 7 lit. f) dyrektywy 95/46/WE, który poddaje przetwarzanie danych osobowych, w braku zgody osoby której dotyczą dane, warunkowi dotyczącemu wyłącznie uzasadnionych interesów administratora danych lub osoby trzeciej bądź osobom trzecim, którym dane są ujawniane.

W tym zakresie Trybunał przede wszystkim stwierdził, że art. 7 dyrektywy 95/46/WE przewiduje zamknięty i wyczerpujący wykaz przypadków, w których przetwarzanie danych osobowych może zostać uznane za zgodne z prawem w braku zgody osoby, której dane dotyczą. Co za tym idzie, państwa członkowskie nie mogą wprowadzać na podstawie art. 5 wspomnianej dyrektywy nowych kryteriów zgodności z prawem przetwarzania danych osobowych, ani też modyfikować, za pomocą dodatkowych wymogów, zakresu kryteriów przewidzianych we wspomnianym art. 7. Artykuł 5 upoważnia bowiem państwa członkowskie jedynie do określenia, w granicach przepisów zawartych w rozdziale II wspomnianej dyrektywy, a w konsekwencji jej art. 7, bardziej szczegółowych warunków ustalania zgodności z prawem przetwarzania danych osobowych (pkt 30, 32, 33).

W szczególności w celu przewidzianego na mocy art. 7 lit. f) tej dyrektywy ważenia przeciwstawnych praw i interesów występujących w danym przypadku państwa członkowskie mogą ustanowić wytyczne. Mogą one również uwzględnić okoliczność, że powaga naruszenia praw podstawowych osoby, której

wspomniane przetwarzanie dotyczy, może różnić się w zależności od tego, czy sporne dane figurują już w powszechnie dostępnych źródłach (pkt 44, 46).

Jednakże Trybunał stwierdził, że o ile przepisy krajowe wykluczają w odniesieniu do określonych kategorii danych osobowych możliwość ich przetwarzania, określając w stosunku do nich w sposób ostateczny rezultat ważenia przeciwstawnych praw i interesów, tym samym nie dopuszczając do innego rezultatu będącego wynikiem szczególnych okoliczności konkretnego przypadku, nie chodzi tu już o doprecyzowanie w rozumieniu art. 5 dyrektywy 95/46/WE. W konsekwencji Trybunał stwierdził, że art. 7 lit. f) dyrektywy 95/46/WE 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 (pkt 47, 48).

Wyrok z dnia 19 października 2016 r., Breyer (C-582/14, EU:C:2016:779)

W tym wyroku (zob. także część II.2., zatytułowaną „Pojęcie »danych osobowych«") Trybunał wypowiedział się także w kwestii, czy art. 7 lit. f) dyrektywy 95/46/WE stoi na przeszkodzie przepisowi prawa krajowego, zgodnie z którym 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 konkretnej strony.

Trybunał orzekł, że art. 7 lit. f) dyrektywy 95/46/WE stoi na przeszkodzie rozpatrywanym przepisom. Na mocy bowiem tego przepisu przetwarzanie danych osobowych w rozumieniu tego przepisu jest zgodne z prawem, jeśli jest konieczne do realizacji celów wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej lub osób trzecich, którym dane są ujawniane, pod warunkiem, że interesy takie nie przeważają nad interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą. Tymczasem w tym przypadku przepisy niemieckie wykluczały 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. W ten sposób przepisy te w sposób niezgodny z prawem ograniczyły zakres zasady przewidzianej w art. 7 lit. f) dyrektywy 95/46/WE, wykluczając możliwość ważenia celu polegającego na zagwarantowaniu ogólnej funkcjonalności mediów online z interesem lub podstawowymi prawami i wolnościami użytkowników (pkt 62–64, pkt 2 sentencji).

Wyrok z dnia 4 maja 2017 r., Rīgas satiksme (C-13/16, EU:C:2017:336)

Sprawa ta wpisywała się w ramy sporu pomiędzy łotewską policją krajową a Rīgas satiksme, przedsiębiorstwem trolejbusowym miasta Ryga, dotyczącego wniosku o przekazanie danych osobowych osoby odpowiedzialnej za wypadek drogowy. W omawianej sprawie podczas wypadku drogowego kierowca taksówki zatrzymał swój pojazd na poboczu jezdni. W chwili gdy trolejbus należący do Rīgas satiksme przejeżdżał obok tej taksówki, pasażer zajmujący tylne miejsce w taksówce otworzył drzwi, które otarły i uszkodziły karoserię trolejbusu. W celu wytoczenia powództwa cywilnego Rīgas satiksme zwróciło się do policji krajowej, żądając między innymi przekazania danych dotyczących sprawcy wypadku. Policja odmówiła podania numeru dokumentu tożsamości i adresu pasażera oraz dokumentów dotyczących wyjaśnień osób biorących udział w wypadku z tego względu, że dokumenty odnoszące się do postępowania administracyjnego kończącego się nałożeniem sankcji mogą być przekazane wyłącznie stronom tego postępowania, a w odniesieniu do numeru dokumentu tożsamości i adresu, ustawa o ochronie danych osobowych osób fizycznych zakazywała ujawnienia takich informacji dotyczących osób fizycznych.

W tych okolicznościach Augstākās tiesas Administratīvo lietu departaments (sąd najwyższy, wydział spraw administracyjnych, Łotwa) postanowił skierować do Trybunału Sprawiedliwości pytanie, czy art. 7 lit. f) dyrektywy 95/46/WE nakłada obowiązek przekazania danych osobowych osobie trzeciej, aby umożliwić jej dochodzenie odszkodowania przed sądem cywilnym za szkodę wyrządzoną przez osobę objętą ochroną tych danych, oraz czy fakt, że osoba ta jest małoletnia, może mieć wpływ na wykładnię tego przepisu.

Trybunał orzekł, że art. 7 lit. f) dyrektywy 95/46/WE należy interpretować w ten sposób, że nie nakłada on obowiązku przekazania danych osobowych osobie trzeciej, aby umożliwić jej dochodzenie odszkodowania przed sądem cywilnym za szkodę wyrządzoną przez osobę objętą ochroną tych danych. Jednakże wspomniany przepis nie stałby na przeszkodzie takiemu przekazaniu, w sytuacji gdyby miało ono miejsce na podstawie prawa krajowego, przy poszanowaniu określonych w tym przepisie przesłanek (pkt 27, 34 i sentencja).

W tym kontekście Trybunał stwierdził, że z zastrzeżeniem ustaleń, jakich dokona w tym względzie sąd odsyłający, w okolicznościach takich jak rozpatrywane w postępowaniu głównym nie wydaje się uzasadnione odmówienie pokrzywdzonemu przekazania danych osobowych koniecznych do wniesienia powództwa o odszkodowanie przeciwko sprawcy szkody lub, w danym wypadku, przeciwko osobom wykonującym władzę rodzicielską ze względu na to, że sprawca ten jest małoletni (pkt 33).

Wyrok z dnia 27 września 2017 r., Puškár (C-73/16, EU:C:2017:725)

W sporze w postępowaniu głównym Peter Puškár wniósł skargę do Najvyšší súd Slovenskej republiky (sądu najwyższego Republiki Słowackiej), żądając nakazania Finančné riaditel'stvo (dyrekcji ds. podatków i ceł), wszystkim podlegającym jej urzędom skarbowym oraz Kriminálny úrad finančnej správy (urzędowi ds. zwalczania przestępczości finansowej) nieumieszczania jego nazwiska w wykazie osób uznawanych przez dyrekcję ds. podatków i ceł za osoby podstawione, utworzonego przez ten organ w ramach poboru podatków i aktualizowanego przez ten organ oraz urząd ds. zwalczania przestępczości finansowej (zwanym dalej „spornym wykazem"). Poza tym zażądał usunięcia każdej dotyczącej go wzmianki z tych wykazów oraz z systemu informatycznego administracji podatkowej.

W tych okolicznościach Najvyšší súd zwrócił się do Trybunału Sprawiedliwości, w szczególności, z pytaniem, czy uznane w art. 7 karty prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się oraz uznane w jej art. 8 prawo do ochrony danych osobowych można interpretować w ten sposób, że państwo członkowskie nie może bez zgody zainteresowanej osoby tworzyć wykazów danych osobowych do celów administracji podatkowej, co oznacza, że uzyskanie danych osobowych przez organ publiczny w celach zwalczania oszustw podatkowych samo w sobie niesie ze sobą ryzyko naruszenia.

Trybunał stwierdził, że art. 7 lit. e) dyrektywy 95/46/WE nie stoi na przeszkodzie takiemu przetwarzaniu danych osobowych dokonanemu bez zgody zainteresowanych osób przez organy państwa członkowskiego do celów poboru podatków i zwalczania przestępstw podatkowych, jakie miało miejsce w przypadku sporządzenia wykazu będącego przedmiotem sporu w postępowaniu głównym, pod warunkiem, po pierwsze, że na mocy ustawodawstwa krajowego organom tym zostały powierzone zadania wykonywane w interesie publicznym w rozumieniu tego przepisu, że sporządzenie tego wykazu i wpisanie do niego nazwisk konkretnych osób jest rzeczywiście właściwe i konieczne dla osiągnięcia zamierzonych celów i że istnieją wystarczające przesłanki do tego, aby sądzić, że wciągnięcie tych osób do wykazu było uzasadnione, a po drugie, że wszystkie warunki zgodności z prawem tego przetwarzania danych osobowych wynikające z dyrektywy 95/46/WE zostały spełnione (pkt 117, pkt 3 sentencji).

W tym zakresie Trybunał orzekł, że na sądzie odsyłającym spoczywa również obowiązek ustalenia, czy sporządzenie spornego wykazu było konieczne do realizacji zadania wykonywanego w interesie

publicznym, którego dotyczy postępowanie główne, biorąc pod uwagę w szczególności konkretny cel sporządzenia spornego wykazu, skutki prawne uwzględnienia w tym wykazie osób w nim figurujących oraz jawny lub niejawny charakter tego wykazu. Ponadto w świetle zasady proporcjonalności do sądu odsyłającego należy również ustalenie, czy sporządzenie spornego wykazu i wpisanie do niego nazwisk konkretnych osób jest właściwe dla realizacji przyświecających im celów i czy nie istnieją inne, mniej uciążliwe środki dla ich osiągnięcia (pkt 111, 112, 113).

Poza tym Trybunał zauważył, że zamieszczenie nazwiska danej osoby w spornym wykazie może skutkować naruszeniem niektórych praw tej osoby. Wciągnięcie jej do tego wykazu może bowiem zaszkodzić jej dobremu imieniu i negatywnie wpłynąć na jej relacje z organami podatkowymi. Ponadto zamieszczenie w tym wykazie mogłoby naruszyć zasadę domniemania niewinności tej osoby, uznaną w art. 48 ust. 1 karty, oraz zapisaną w art. 16 karty swobodę przedsiębiorczości osób prawnych powiązanych z osobami fizycznymi wpisanymi do spornego wykazu. W konsekwencji tego rodzaju naruszenie może zostać uznane za odpowiednie jedynie wtedy, gdy istnieją dostateczne powody uzasadniające podejrzenie, że dana osoba w sposób pozorny zajmuje stanowiska kierownicze w organach osób prawnych z nią powiązanych i w ten sposób działa ze szkodą dla poboru podatków i zwalczania oszustw podatkowych (pkt 114).

Ponadto Trybunał stwierdził, że jeśli istniałyby powody do ograniczenia na mocy art. 13 dyrektywy 95/46/WE niektórych z praw przewidzianych w art. 6 i 10-12 tej dyrektywy, takich jak prawo do informacji osoby zainteresowanej, to ograniczenie takie powinno być konieczne dla ochrony interesów, o których mowa w ust. 1 wspomnianego art. 13, w szczególności takich jak ważny interes ekonomiczny lub finansowy w dziedzinie podatkowej, oraz powinno być przyjęte w drodze przepisów ustawowych (pkt 116).

III. Przekazywanie danych osobowych do państw trzecich

Wyrok z dnia 6 listopada 2003 r. (w pełnym składzie), Lindqvist (C-101/01, EU:C:2003:596)[19]

W tej sprawie (zob. także część II.3, zatytułowana „Pojęcie »przetwarzania danych osobowych«") sąd odsyłający zmierzał w istocie do ustalenia, czy Bodil Lindqvist dokonywała przekazywania danych do państwa trzeciego w rozumieniu wspomnianej dyrektywy.

Trybunał orzekł, że „przekazywanie danych do państw trzecich" w rozumieniu art. 25 dyrektywy 95/46/WE nie ma miejsca, w przypadku gdy osoba, która znajduje się w jednym z państw członkowskich, zamieszcza na stronie internetowej, przechowywanej przez osobę fizyczną lub prawną będącą administratorem witryny internetowej, na której wspomniana strona może być odwiedzana, i mającą swoją siedzibę w tym samym państwie lub w innym państwie członkowskim, dane osobowe, czyniąc je w ten sposób dostępnymi dla każdego, kto połączy się z Internetem, w tym również dla osób, które znajdują się w państwie trzecim (pkt 71, pkt 4 sentencji).

Jeśli uwzględnić z jednej strony stan rozwoju Internetu w okresie trwania prac nad dyrektywą 95/46/WE i z drugiej strony brak określenia w jej rozdziale IV – który obejmuje wspomniany art. 25, mający na celu zapewnienie kontroli państw członkowskich nad przekazywaniem danych osobowych do państw trzecich i zakazanie tego przekazywania, w przypadku gdy państwa te nie zapewniają odpowiedniego stopnia ochrony – kryteriów mających zastosowanie do korzystania z Internetu, to nie można przypisać prawodawcy wspólnotowemu zamiaru objęcia w przyszłości pojęciem przekazywania danych do państwa

19 Wyrok ten został omówiony w sprawozdaniu rocznym 2003, s. 67.

trzeciego takiego zamieszczenia danych na stronie internetowej, nawet jeżeli stały się one w ten sposób dostępne dla osób znajdujących się w państwach trzecich i posiadających środki techniczne pozwalające na dostęp do nich (pkt 63, 64, 68).

Wyrok z dnia 6 października 2015 r. (wielka izba), Schrems (C-362/14, EU:C:2015:650)[20]

Maximillian Schrems, obywatel austriacki i użytkownik sieci społecznościowej Facebook, wniósł skargę do Data Protection Commissioner (komisarza ds. ochrony danych, Irlandia) w związku z przekazywaniem przez Facebook Ireland do Stanów Zjednoczonych danych osobowych użytkowników i ich przechowywania na serwerach położonych w tym państwie, gdzie były one przedmiotem przetwarzania. Zdaniem M. Schremsa prawo i praktyka Stanów Zjednoczonych nie gwarantowały odpowiedniej ochrony przed działaniami nadzorczymi organów publicznych w stosunku do danych przekazanych do tego państwa. Data Protection Commissioner odmówił rozpatrzenia tej skargi, w szczególności z tego względu, że w decyzji 2000/520/WE[21] Komisja stwierdziła, iż w ramach systemu zwanego „bezpieczną przystanią" (ang. „safe harbour")[22] Stany Zjednoczone zapewniają odpowiedni poziom ochrony przekazywanych danych osobowych.

W tym kontekście High Court (wysoki trybunał, Irlandia) zwrócił się do Trybunału Sprawiedliwości z wnioskiem o wykładnię art. 25 ust. 6 dyrektywy 95/46/WE, na podstawie której Komisja może stwierdzić, że państwo trzecie zapewnia odpowiedni stopień ochrony przekazanych danych oraz, w istocie, z pytaniem dotyczącym ważności decyzji 2000/520/WE, przyjętej przez Komisję na podstawie wspomnianego art. 25 ust. 6 dyrektywy 95/46/WE.

Trybunał stwierdził nieważność decyzji Komisji w całości, podkreślając przede wszystkim, że jej wydanie wymaga prawidłowo uzasadnionego ustalenia przez tę instytucję, że dane państwo trzecie rzeczywiście zapewnia poziom ochrony praw podstawowych merytorycznie równoważny poziomowi gwarantowanemu w unijnym porządku prawnym. Tymczasem, ponieważ Komisja w swojej decyzji 2000/520/WE tego nie uczyniła, art. 1 tej decyzji narusza wymogi ustanowione w art. 25 ust. 6 dyrektywy 95/46/WE w związku z kartą i jest w związku z tym nieważny. W istocie zasady „bezpiecznej przystani" mają zastosowanie wyłącznie do organizacji amerykańskich, które dokonały samocertyfikacji, otrzymujących dane osobowe z Unii, przy czym nie wymaga się, aby organy publiczne Stanów Zjednoczonych zostały zobowiązane do poszanowania tych zasad. Ponadto decyzja 2000/520/WE umożliwia ingerencję w prawa podstawowe osób, których dane osobowe zostały lub mogły zostać przekazane z Unii do Stanów Zjednoczonych, nie zawierając stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w te prawa oraz nie ustalając istnienia skutecznej ochrony prawnej przed ingerencją tego rodzaju (pkt 82, 87–89, 96–98, pkt 2 sentencji).

Poza tym Trybunał stwierdził nieważność art. 3 decyzji 2000/520/WE, ponieważ pozbawia on krajowe organy nadzorcze ich kompetencji wynikających z art. 28 dyrektywy 95/46/WE, w przypadku gdy jednostka przedstawia okoliczności mogące podważyć zgodność z ochroną życia prywatnego oraz wolnościami i prawami podstawowymi osób fizycznych decyzji Komisji stwierdzającej, że państwo trzecie zapewnia odpowiedni stopień ochrony (pkt 102–104). Trybunał stwierdził, że nieważność art. 1 i 3 decyzji 2000/520/WE miała wpływ na ważność tej decyzji w całości (pkt 105, 106).

20 Wyrok ten został omówiony w sprawozdaniu rocznym 2015, s. 53.

21 Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez departament handlu USA (Dz.U. L 215 z 25.8.2000, s. 7).

22 System bezpiecznej przystani obejmuje szereg zasad dotyczących ochrony danych osobowych, do których amerykańskie przedsiębiorstwa mogą przystąpić dobrowolnie.

Jeśli chodzi o brak możliwości uzasadnienia takiej ingerencji Trybunał przede wszystkim zauważył, że uregulowania Unii stanowiące ingerencję w prawa podstawowe gwarantowane w art. 7 i 8 karty muszą zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony ich danych przed ryzykiem nadużyć oraz uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem. Konieczność zapewnienia takich gwarancji ma znaczenie tym większe w przypadku, gdy dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do tych danych (pkt 91).

Ponadto i przede wszystkim ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia były ograniczone do tego, co ściśle niezbędne (pkt 92). W ten sposób uregulowanie umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez określenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu organów publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych, nie ogranicza się do tego, co ściśle niezbędne (pkt 93). W szczególności uregulowanie pozwalające organom publicznym na uzyskanie dostępu w sposób ogólny do treści wiadomości elektronicznych narusza istotę podstawowego prawa do poszanowania życia prywatnego. Co więcej, uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty (pkt 94, 95).

Opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r. (wielka izba) (EU:C:2017:592)

W dniu 26 lipca 2017 r. Trybunał po raz pierwszy orzekł w kwestii zgodności projektu umowy międzynarodowej z Kartą praw podstawowych Unii Europejskiej, a w szczególności z postanowieniami dotyczącymi poszanowania życia prywatnego oraz ochrony danych osobowych.

Unia Europejska i Kanada negocjowały umowę o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera (umowa PNR), która została podpisana w 2014 r. Ponieważ Rada Unii Europejskiej zwróciła się do Parlamentu Europejskiego o jej zatwierdzenie, Parlament postanowił zwrócić się do Trybunału Sprawiedliwości w celu ustalenia, czy przewidywana umowa jest zgodna z prawem Unii.

Przewidywana umowa umożliwiała systematyczne i ciągłe przekazywanie danych PNR wszystkich pasażerów lotniczych organowi kanadyjskiemu w celu ich wykorzystywania i przechowywania, a także ich ewentualnego dalszego przekazania innych organom i innym państwom trzecim w celu zwalczania terroryzmu i poważnej przestępczości międzynarodowej. W tym celu wspomniana umowa przewidywała, między innymi pięcioletni okres przechowywana danych i nakładała szczególne wymagania w zakresie bezpieczeństwa i integralności PNR, takie jak natychmiastowe maskowanie danych szczególnie chronionych, a także przewidywała prawa dostępu do danych, sprostowania i usunięcia oraz możliwość wniesienia administracyjnych lub sądowych środków zaskarżenia.

Dane PNR, o których mowa w przewidywanej umowie, obejmują w szczególności, oprócz nazwiska i informacji kontaktowych pasażera lub pasażerów lotniczych, informacje konieczne do rezerwacji, takie jak przewidywane daty podróży oraz trasy podróży, informacje dotyczące biletów, grup osób zarejestrowanych pod numerem rezerwacji, informacje dotyczące sposobów płatności lub fakturowania, informacje dotyczące bagażów, a także ogólne uwagi odnoszące się do pasażerów.

W opinii Trybunał orzekł, że umowa PNR nie może zostać zawarta w jej ówczesnej formie ze względu na niezgodność kilku jej postanowień z uznanymi przez Unię prawami podstawowymi.

Trybunał stwierdził w pierwszej kolejności, że zarówno przekazywanie danych PNR z Unii właściwemu organowi kanadyjskiemu, jak i wynegocjowane przez Unię z Kanadą uregulowanie przesłanek dotyczących zatrzymywania tych danych, ich wykorzystania, jak również ewentualnego późniejszego przekazania innym organom kanadyjskim, Europolowi, Eurojustowi, organom sądowym lub policyjnym państw członkowskich lub innych państw trzecich, stanowią ingerencję w prawo zagwarantowane w art. 7 karty. Czynności te wyczerpują również znamiona ingerencji w prawo podstawowe do ochrony danych osobowych zagwarantowane w art. 8 karty, gdyż stanowią przetwarzanie danych osobowych (pkt 125, 126).

Ponadto Trybunał podkreślił, że nawet jeżeli niektóre dane PNR, rozpatrywane oddzielnie, nie wydają się ujawniać istotnych informacji o życiu prywatnym danych osób, to jednak, rozpatrywane jako całość, mogą między innymi ujawniać pełną trasę podróży, nawyki turystyczne, relacje między dwoma osobami lub większą ich liczbą, a także informacje o sytuacji finansowej pasażerów lotniczych, ich zwyczajach żywieniowych lub stanie zdrowia, a nawet mogą dostarczać o tych pasażerach informacji szczególnie chronionych, takich jak informacje, o których mowa w art. 2 lit. e) przewidywanej umowy (informacje ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne itp.) (pkt 128).

W tym zakresie Trybunał stwierdził, że chociaż rozpatrywana ingerencja może być uzasadniona dążeniem do realizacji celu interesu ogólnego (zapewnienie bezpieczeństwa publicznego w ramach zwalczania przestępstw terrorystycznych oraz poważnej przestępczości międzynarodowej), szereg postanowień umowy nie jest ograniczony do tego, co ściśle konieczne i nie przewiduje jasnych i precyzyjnych reguł.

W szczególności Trybunał stwierdził, że zważywszy na niebezpieczeństwo przetwarzania danych sprzecznego z zasadą niedyskryminacji przekazywanie do Kanady danych szczególnie chronionych wymagałoby precyzyjnego i szczególnie solidnego uzasadnienia, wywodzonego z powodów innych niż ochrona bezpieczeństwa publicznego przed terroryzmem i poważną przestępczością międzynarodową. Tymczasem w tej sprawie brak tego rodzaju uzasadnienia. Trybunał w związku z powyższym orzekł, że postanowienia umowy dotyczące przekazywania danych szczególnie chronionych do Kanady, a także przekazywanie i zatrzymywanie tych danych są niezgodne z prawami podstawowymi (pkt 165, 232).

W drugiej kolejności Trybunał orzekł, że po opuszczeniu przez pasażerów lotniczych Kanady trwałe przechowywanie danych PNR ogółu pasażerów lotniczych, jakie umożliwia przewidywana umowa, nie jest ograniczone do tego, co ściśle konieczne. Jeżeli bowiem chodzi o pasażerów lotniczych, w odniesieniu do których ryzyka w zakresie terroryzmu i przestępczości międzynarodowej nie zidentyfikowano w chwili ich przybycia do Kanady i aż do opuszczenia przez nich tego państwa, okazuje się, że od chwili ich wyjazdu nie istnieje chociażby pośredni związek między ich danymi PNR a celem przewidywanej umowy, który to związek uzasadniałby zatrzymanie tych danych. Natomiast przechowywanie danych PNR pasażerów lotniczych, w odniesieniu do których zidentyfikowano obiektywne elementy pozwalające na uznanie, że mogliby oni – nawet po opuszczeniu Kanady – stanowić zagrożenie w rozumieniu zwalczania terroryzmu i poważnych przestępstw międzynarodowych, jest dopuszczalne po zakończeniu ich pobytu w tym państwie, nawet przez okres pięciu lat (pkt 205–207, 209).

W trzeciej kolejności Trybunał stwierdził, że uznane w art. 7 Karty praw podstawowych Unii Europejskiej prawo do poszanowania życia prywatnego oznacza, że osoba, której dane dotyczą, może upewnić się, iż te dane osobowe są przetwarzane prawidłowo oraz zgodnie z prawem. Osoba ta, by móc dokonać stosownych sprawdzeń, powinna posiadać prawo dostępu do dotyczących jej danych będących przedmiotem przetwarzania.

W tym zakresie Trybunał podkreślił, że w przewidywanej umowie istotne jest, by pasażerowie lotniczy byli informowani o przekazywaniu ich danych PNR do danego państwa trzeciego oraz o ich wykorzystywaniu od chwili, gdy to udostępnienie nie może zagrozić dochodzeniom prowadzonym przez organy publiczne, o których mowa w przewidywanej umowie. Informowanie takie okazuje się de facto konieczne, by umożliwić pasażerom lotniczym skorzystanie z prawa do domagania się dostępu do dotyczących ich danych oraz ewentualnie ich sprostowania, jak również, zgodnie z art. 47 akapit pierwszy karty, wniesienia skutecznego środka prawnego do sądu.

Tak więc w sytuacjach, w których obecne są obiektywne elementy uzasadniające wykorzystanie danych PNR w celu zwalczania terroryzmu i poważnej przestępczości międzynarodowej i wymagające uprzedniego zezwolenia wydanego przez sąd lub niezależny organ administracyjny, indywidualne informowanie pasażerów lotniczych okazuje się konieczne. Dotyczy to również przypadków, gdy dane PNR pasażerów lotniczych są udostępniane innym organom publicznym lub osobom fizycznym. Jednak takie informowanie powinno się odbywać dopiero od chwili, gdy nie może ono zagrozić dochodzeniom prowadzonym przez organy publiczne, o których mowa w przewidywanej umowie (pkt 219, 220, 223, 224).

IV. Ochrona danych osobowych w Internecie

1. Prawo do sprzeciwu wobec przetwarzania danych osobowych („prawo do bycia zapomnianym")

Wyrok z dnia 13 maja 2014 r. (wielka izba), Google Spain i Google (C-131/12, EU:C:2014:317)

W tym wyroku (zob. także część II.3, zatytułowana „Pojęcie »przetwarzania danych osobowych«") Trybunał wyjaśnił zakres przewidzianych w dyrektywie 95/46/WE praw dostępu i sprzeciwu wobec przetwarzania danych osobowych w Internecie.

I tak orzekając w kwestii zakresu odpowiedzialności operatora wyszukiwarki internetowej, Trybunał w istocie stwierdził, że w celu przestrzegania prawa dostępu i prawa do sprzeciwu, zagwarantowanych w art. 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46/WE, i o ile spełnione są warunki przewidziane w tych artykułach, operator ten jest w określonych okolicznościach zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje. Trybunał wyjaśnił, że taki obowiązek może istnieć także w przypadku, gdy to imię czy nazwisko czy te informacje nie zostały uprzednio czy jednocześnie usunięte z tych stron internetowych i, w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem (pkt 88, pkt 3 sentencji).

Ponadto, odpowiadając na pytanie, czy dyrektywa umożliwia danej osobie domaganie się usunięcia linków do stron internetowych z listy wyników z tego względu, że osoba ta życzy sobie, by znajdujące się tam informacje dotyczące jej osoby zostały „zapomniane" po upływie pewnego czasu, Trybunał najpierw stwierdził, że nawet początkowo zgodne z prawem przetwarzanie prawidłowych danych może wraz z upływem czasu stać się niezgodne z tą dyrektywą, jeśli dane te nie są już potrzebne do realizacji celów, ze względu na które były gromadzone i przetwarzane, w szczególności wówczas, gdy należy uznać je za niewłaściwe, (już) niestosowne czy też nadmierne w stosunku do celów, w jakich są one przetwarzane, czy też ze względu na upływ czasu (pkt 93). Zatem w przypadku gdy wskutek wniosku złożonego przez osobę, której dotyczą dane, stwierdzone zostanie, że zawarcie na liście wyników tych linków jest w aktualnym stanie rzeczy niezgodne z dyrektywą, zawarte na tej liście informacje i linki należy usunąć

(pkt 94). W tym względzie stwierdzenie, iż danej osobie przysługuje prawo, aby dotycząca jej informacja nie była już powiązana z jej imieniem i nazwiskiem poprzez listę wyników wyszukiwania, pozostaje bez związku z tym, czy zawarcie na liście wyników wyszukiwania danej informacji wyrządza szkodę osobie, której dotyczą dane (pkt 96, pkt 4 sentencji).

Wreszcie Trybunał wyjaśnił, że ponieważ osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 karty prawa podstawowe, zażądać, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania, prawa te są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji (pkt 97, pkt 4 sentencji).

2. Przetwarzanie danych osobowych a prawa własności intelektualnej

Wyrok z dnia 29 stycznia 2008 r. (wielka izba), Promusicae (C-275/06, EU:C:2008:54)[23]

Promusicae, niemające celu zarobkowego hiszpańskie stowarzyszenie zrzeszające producentów i wydawców nagrań muzycznych i opracowań audiowizualnych wniosło do sądów hiszpańskich o nakazanie Telefónica de España SAU (spółce prawa handlowego, która w ramach swej działalności świadczy między innymi usługi w zakresie dostępu do Internetu) wskazania tożsamości i adresów określonych osób, na rzecz których świadczy usługi w zakresie dostępu do Internetu i w przypadku których adres IP oraz data i godzina połączenia są znane. Zdaniem Promusicae osoby te korzystały z programu wymiany plików zwanego "peer-to-peer" lub "P2P" (przejrzysty środek pozwalający na wymianę treści, niezależny, zdecentralizowany i wyposażony w zaawansowane funkcje wyszukiwania i pobierania) i umożliwiały, w ramach udostępnionych folderów swoich komputerów osobistych, dostęp do nagrań, do których majątkowe prawa autorskie należą do podmiotów będących członkami Promusicae. Promusicae wniosło więc o przekazanie mu tych informacji w celu wytoczenia następnie powództw cywilnych przeciwko tym osobom.

W tych okolicznościach Juzgado de lo Mercantil no 5 de Madrid (sąd gospodarczy nr 5 w Madrycie, Hiszpania) zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy prawodawstwo Unii w celu zapewnienia skutecznego przestrzegania praw autorskich zobowiązuje państwa członkowskie do ustanowienia obowiązku przekazania danych osobowych w ramach postępowania cywilnego.

Zdaniem Trybunału wspomniany wniosek o wydanie orzeczenia w trybie prejudycjalnym poruszył zagadnienie koniecznego pogodzenia wymogów związanych z ochroną poszczególnych praw podstawowych, a mianowicie, z jednej strony, prawa do poszanowania życia prywatnego, a z drugiej strony, prawa do ochrony własności i skutecznego środka prawnego.

W tym zakresie Trybunał orzekł, że w sytuacji takiej jak będąca przedmiotem postępowania głównego dyrektywy: 2000/31/WE w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego („dyrektywa o handlu

23 Wyrok ten został omówiony w sprawozdaniu rocznym 2008, s. 46.

elektronicznym")[24], 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym[25], 2004/48/WE w sprawie egzekwowania praw własności intelektualnej[26] oraz dyrektywa 2002/58/WE nie zobowiązują państw członkowskich do ustanowienia obowiązku przekazania danych osobowych w celu zapewnienia skutecznej ochrony praw autorskich w ramach postępowania cywilnego. Prawo Unii wymaga jednak, by przy transpozycji tych dyrektyw oparły się one na takiej wykładni tych dyrektyw, która pozwoli na zapewnienie odpowiedniej równowagi między poszczególnymi prawami podstawowymi chronionymi przez wspólnotowy porządek prawny. Ponadto przy przyjmowaniu środków mających na celu transpozycję tych dyrektyw organy i sądy państw członkowskich są zobowiązane nie tylko dokonywać wykładni swojego prawa krajowego w sposób zgodny ze wspomnianymi dyrektywami, lecz również nie opierać się na takiej wykładni tych dyrektyw, która pozostawałaby w konflikcie ze wspomnianymi prawami podstawowymi lub z innymi ogólnymi zasadami prawa wspólnotowego, takimi jak zasada proporcjonalności (pkt 70 i sentencja).

Wyrok z dnia 24 listopada 2011 r., Scarlet Extended (C-70/10, EU:C:2011:771)[27]

Belgijskie zrzeszenie autorów, kompozytorów i wydawców SCRL (SABAM) stwierdziło, że internauci korzystający z usług Scarlet Extended SA, dostawcy dostępu do Internetu (zwanego dalej „Scarlet") pobierają z Internetu, bez zezwolenia i bez uiszczania opłat, utwory zapisane w jej katalogu za pomocą sieci „peer-to-peer". SABAM wystąpiła do sądu krajowego i doprowadziła do wydania, w pierwszej instancji, względem Scarlet nakazu zaprzestania naruszania praw autorskich poprzez uniemożliwienie wszelkich form wysyłania lub otrzymywania przez jej klientów za pośrednictwem programów „peer-to-peer" plików elektronicznych zawierających utwory muzyczne z repertorium SABAM.

Cour d'appel de Bruxelles (sąd apelacyjny w Brukseli, Belgia), do którego Scarlet wniosła apelację, zawiesił postępowanie celem uzyskania od Trybunału Sprawiedliwości w trybie prejudycjalnym odpowiedzi na pytanie, czy taki nakaz jest zgodny z prawem Unii.

Trybunał orzekł, że dyrektywy 95/46/WE, 2000/31/WE, 2001/29/WE, 2002/58/WE i 2004/48/WE, pozostające w związku i interpretowane w świetle wymogów wynikających z ochrony mających zastosowanie praw podstawowych, należy rozumieć w ten sposób, że stoją one na przeszkodzie skierowanemu do Scarlet nakazowi wdrożenia systemu filtrowania wszystkich połączeń elektronicznych przekazywanych za pośrednictwem jego usług, w szczególności przy zastosowaniu programów „peer-to-peer", mającego zastosowanie bez rozróżnienia w stosunku do wszystkich jego klientów, w celach zapobiegawczych, na wyłączny koszt dostawcy i bez ograniczeń w czasie, zdolnego do zidentyfikowania w sieci tego dostawcy przypadków przekazywania plików elektronicznych zawierających utwory muzyczne, kinematograficzne lub audiowizualne, co do których strona powodowa rości sobie prawa własności intelektualnej, celem zablokowania transferu plików, których wymiana narusza prawo autorskie (pkt 54 i sentencja).

Zdaniem Trybunału tego typu nakaz narusza bowiem wprowadzony przez art. 15 ust. 1 dyrektywy 2000/31/WE zakaz nakładania na takiego usługodawcę ogólnego obowiązku nadzorowania oraz wymóg zapewnienia odpowiedniej równowagi między z jednej strony prawem własności intelektualnej, a z drugiej strony wolnością prowadzenia działalności gospodarczej, prawem do ochrony danych osobowych oraz wolnością otrzymywania i przekazywania informacji (pkt 40, 49).

24 Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1).

25 Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L 167 z 22.62001, s. 10).

26 Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności (Dz.U. L 157 z 30.4.2004, s. 45; sprostowanie Dz.U. L 195 z2.6.2004, s. 16);

27 Wyrok ten został omówiony w sprawozdaniu rocznym 2011, s. 37.

W tym kontekście Trybunał orzekł po pierwsze, że nakaz ustanowienia spornego systemu filtrowania pociągałby za sobą konieczność przeprowadzania systematycznej analizy wszelkich treści oraz gromadzenie i identyfikację adresów IP użytkowników, od których pochodzą przesłane w sieci nielegalne treści, przy czym adresy te stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników (pkt 51). Po drugie, istnieje ryzyko, że omawiany nakaz naruszyłby wolność informacji, ponieważ system ten mógłby nie rozróżniać w wystarczającym stopniu treści niezgodnej z prawem i treści zgodnej z prawem, skutkiem czego jego wdrożenie mogłoby doprowadzić do blokady połączeń o treści zgodnej z prawem. Nie budzi bowiem wątpliwości okoliczność, że odpowiedź na pytanie dotyczące zgodności z prawem danego przekazu zależy również od stosowania ustawowych wyjątków od prawa autorskiego, które różnią się od siebie w poszczególnych państwach członkowskich. Ponadto w niektórych państwach członkowskich pewne utwory mogą należeć do domeny publicznej lub zostać bezpłatnie opublikowane w witrynie internetowej przez ich autorów (pkt 52).

W konsekwencji Trybunał stwierdził, że wydając nakaz zobowiązujący Scarlet do wdrożenia spornego systemu filtrowania, wspomniany sąd krajowy nie spełniłby wymogu zapewnienia odpowiedniej równowagi między z jednej strony prawem własności intelektualnej, a z drugiej strony wolnością prowadzenia działalności gospodarczej, prawem do ochrony danych osobowych oraz wolnością otrzymywania i przekazywania informacji (pkt 53).

Wyrok z dnia 19 kwietnia 2012 r., Bonnier Audio i in. (C-461/10, EU:C:2012:219)

Högsta domstolen (sad najwyższy, Szwecja) zwrócił się do Trybunału Sprawiedliwości w trybie prejudycjalnym w celu uzyskania wykładni dyrektyw 2002/58/WE i 2004/48/WE, w ramach sporu pomiędzy Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB i Storyside AB (zwanym dalej „Bonnier Audio i in.") a Perfect Communication Sweden AB (zwanym dalej „ePhone") w przedmiocie sprzeciwu wniesionego przez ePhone'a wobec złożonego przez Bonnier Audio i in. wniosku o nakazanie przekazania danych.

W tym przypadku Bonnier Audio i in. byli wydawcami, którym przysługiwały wyłączne prawa do rozpowszechniania 27 książek w postaci książek audio, ich powielania oraz udostępniania publiczności. Bonnier Audio i in. twierdzą, że ich wyłączne prawa zostały naruszone ze względu na udostępnienie publiczności tych 27 dzieł, bez ich zgody, za pomocą serwera FTP („file transfer protocol" – protokół transferu plików), który umożliwia wymianę plików i transfer danych pomiędzy komputerami za pośrednictwem Internetu. Bonnier Audio i in. zwrócili się zatem do sądów szwedzkich o wydanie nakazu ujawnienia imienia i nazwiska oraz adresu osoby, która jest zarejestrowana jako użytkownik adresu IP, z którego rzekomo przedmiotowe pliki były transferowane.

W tym kontekście Högsta domstolen (sąd najwyższy, Szwecja), do którego została wniesiona skarga kasacyjna, zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy prawo Unii stoi na przeszkodzie stosowaniu przepisu krajowego, opartego na art. 8 dyrektywy 2004/48/WE, na mocy którego w postępowaniu cywilnym można, w celu zidentyfikowania określonego abonenta, nakazać dostawcy usług internetowych ujawnienie uprawnionemu z prawa autorskiego albo jego przedstawicielowi informacji o abonencie, któremu dostawca usług internetowych udostępnił określony adres IP, przy użyciu którego miało zostać popełnione naruszenie. Założono, po pierwsze, że powód żądający wydania nakazu uprawdopodobnił naruszenie konkretnego prawa autorskiego, a po drugie, że wydanie nakazu jest proporcjonalne.

Trybunał najpierw przypomniał, że art. 8 ust. 3 dyrektywy 2004/48/WE w związku z art. 15 ust. 1 dyrektywy 2002/58/WE nie stoi na przeszkodzie ustanowieniu przez państwa członkowskie obowiązku przekazania prywatnym osobom trzecim danych osobowych, tak aby umożliwić im wnoszenie do sądów cywilnych powództw o naruszenie praw autorskich, lecz nie nakłada też na państwa zobowiązania do

ustanowienia takiego obowiązku. Jednakże organy i sądy państw członkowskich są zobowiązane nie tylko dokonywać wykładni swojego prawa krajowego w sposób zgodny z tymi dyrektywami, lecz również nie opierać się na takiej wykładni tych dyrektyw, która pozostawałaby w konflikcie ze wspomnianymi prawami podstawowymi lub z innymi ogólnymi zasadami prawa Unii, takimi jak zasada proporcjonalności (pkt 55, 56).

W tym zakresie Trybunał stwierdził, że przedmiotowe przepisy krajowe wymagają, w szczególności dla wydania nakazu ujawnienia przedmiotowych danych, rzeczywistego uprawdopodobnienia naruszenia prawa własności intelektualnej w odniesieniu do istniejącego dzieła, aby żądane informacje mogły ułatwić dochodzenie w przedmiocie złamania praw autorskich lub naruszenia takich praw oraz aby względy uzasadniające ten nakaz miały wyższą rangę w porównaniu z niedogodnościami albo innymi szkodami, które mogłyby powstać u adresata takiego nakazu, względnie w porównaniu z wszelkim interesem, który się jemu sprzeciwia (pkt 58).

W konsekwencji Trybunał orzekł, że dyrektywy 2002/58/WE i 2004/48/WE nie sprzeciwiają się przepisowi krajowemu, takiemu jak analizowany przepis w postępowaniu głównym, ponieważ przepis ten zezwala sądowi krajowemu, do którego skierowano wniosek o wydanie nakazu ujawnienia danych osobowych, wniesiony przez osobę posiadającą legitymację procesową, na wyważenie przeciwstawnych interesów, stosownie do okoliczności każdego przypadku oraz przy należytym uwzględnieniu wymogów wynikających z zasady proporcjonalności (pkt 61 i sentencja).

V. Krajowe organy nadzorcze

1. Zakres wymogu niezależności

Wyrok z dnia 9 marca 2010 r. (wielka izba), Komisja/Niemcy (C-518/07, EU:C:2010:125)[28]

W swojej skardze Komisja wniosła do Trybunału o stwierdzenie, że Republika Federalna Niemiec, poddając organy sprawujące nadzór nad przetwarzaniem danych osobowych w sektorze niepublicznym w niektórych krajach związkowych kontroli państwowej i dokonując w związku z tym nieprawidłowej implementacji wymogu „całkowitej niezależności" organów odpowiedzialnych za zagwarantowanie ochrony tych danych, uchybiła zobowiązaniom ciążącym na niej na mocy art. 28 ust. 1 akapit drugi dyrektywy 95/46/WE.

Republika Federalna Niemiec twierdziła z kolei, że art. 28 ust. 1 akapit drugi dyrektywy 95/46/WE wymaga niezależności funkcjonalnej organów nadzorczych w tym sensie, że organy te powinny być niezależne od sektora niepublicznego podlegającego ich kontroli i że nie powinny być poddane wpływom z zewnątrz. Tymczasem według niej kontrola państwowa w niemieckich krajach związkowych nie stanowi takiego wpływu zewnętrznego, lecz wewnętrzny mechanizm kontroli w administracji, wprowadzony przez organy należące do tego samego aparatu administracyjnego co organy nadzorcze i zobowiązane jak te ostatnie do wypełniania celów dyrektywy 95/46/WE.

Trybunał orzekł, że przewidziane w dyrektywie 95/46/WE zagwarantowanie niezależności krajowych organów nadzorczych ma na celu zapewnienie skuteczności i pewności kontroli przestrzegania przepisów w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i powinno być interpretowane w świetle tego celu. Niezależność została przyjęta nie celem przyznania tym organom

28 Wyrok ten został omówiony w sprawozdaniu rocznym 2010, s. 34.

i ich pracownikom szczególnego statusu, lecz celem wzmocnienia ochrony osób i instytucji, których dotyczą decyzje tych organów, a zatem przy wykonywaniu swoich obowiązków organy nadzorcze powinny działać w sposób obiektywny i bezstronny (pkt 25).

Trybunał stwierdził, że organy nadzorcze właściwe dla sprawowania nadzoru nad przetwarzaniem danych osobowych w sektorze niepublicznym muszą być niezależne, gdyż pozwala im to wykonywać swoje obowiązki bez wpływów zewnętrznych. Ta niezależność wyklucza nie tylko jakikolwiek wpływ ze strony instytucji kontrolowanych, lecz również jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz, bez względu na to, czy bezpośredni, czy pośredni, który mógłby podważyć wykonywanie przez te organy ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych. Samo tylko zagrożenie możliwością wpływu politycznego organów kontroli państwowej na decyzje organów nadzorczych jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań. Po pierwsze, może mieć bowiem miejsce „przewidywane posłuszeństwo" tych organów w świetle praktyki decyzyjnej organu kontroli państwowej. Po drugie, rola strażników prawa do poszanowania życia prywatnego, jaką wypełniają te organy nadzorcze, wymaga, by ich decyzje, a tym samym one same, pozostawały poza jakimkolwiek podejrzeniem stronniczości. Zdaniem Trybunału nadzór państwa wykonywany nad niemieckimi organami nadzorczymi jest niezgodny z wymogiem niezależności (pkt 30, 36, 37 i sentencja).

Wyrok z dnia 16 października 2012 r. (wielka izba), Komisja/Austria (C-614/10, EU:C:2012:631)

W swej skardze Komisja zwróciła się do Trybunału o stwierdzenie, że nie przyjmując wszelkich przepisów ustawowych, wykonawczych i administracyjnych potrzebnych, aby obowiązujące w Austrii ustawodawstwo spełniało kryterium niezależności w odniesieniu do Datenschutzkommission (komisji ochrony danych, zwanej dalej „DSK"), ustanowionej jako organ nadzorczy w zakresie ochrony danych osobowych, Austria uchybiła zobowiązaniom, jakie ciążą na niej na mocy art. 28 ust. 1 akapit drugi dyrektywy 95/46/WE.

Trybunał stwierdził uchybienie ze strony Austrii, orzekając w istocie, że nie czyni zadość ustanowionemu w dyrektywie 95/46/WE kryterium niezależności organu nadzorczego państwo członkowskie, które ustanawia przepisy, na mocy których wspomniany organ jest urzędnikiem państwowym podlegającym nadzorowi służbowemu, którego urząd jest włączony do służb rządu krajowego i wobec którego szef rządu krajowego posiada bezwarunkowe prawo do uzyskania informacji na temat wszelkich aspektów zarządzania wspomnianym organem (pkt 66 i sentencja).

Trybunał najpierw przypomniał, że zawarte w art. 28 ust. 1 akapit drugi dyrektywy 95/46/WE sformułowanie „w sposób całkowicie niezależny" oznacza, że organy nadzorcze powinny korzystać z niezależności, pozwalającej im na wykonywanie ich zadań bez wpływu z zewnątrz. W tym względzie okoliczność, że taki organ ma niezależność funkcjonalną, ponieważ jego członkowie są niezależni i nie są związani żadnymi instrukcjami w zakresie wykonywanych przez nich funkcji nie wystarcza sama w sobie dla uchronienia rzeczonego organu od wszelkiego wpływu z zewnątrz. Wymagana w tych ramach niezależność ma bowiem na celu wykluczenie nie tylko bezpośredniego wpływu pod postacią instrukcji, lecz również jakiegokolwiek pośredniego wpływu z zewnątrz, mogącego nadawać kierunek decyzjom organu nadzorczego. Ponadto rola strażników prawa do poszanowania życia prywatnego, jaką wypełniają te organy, wymaga, by ich decyzje, a tym samym one same, pozostawały poza jakimkolwiek podejrzeniem stronniczości (pkt 41–43, 52).

Trybunał wyjaśnił, że aby spełniać wymóg niezależności ustanowiony we wspomnianym wyżej przepisie dyrektywy 95/46/WE, krajowy organ nadzorczy nie musi posiadać niezależnej linii budżetowej takiej jak przewidziana w art. 43 ust. 3 rozporządzenia (WE) nr 45/2001. Państwa członkowskie nie mają bowiem obowiązku powtarzania w ich krajowym ustawodawstwie przepisów analogicznych do przepisów rozdziału V rozporządzenia (WE) nr 45/2001 w celu zapewnienia całkowitej niezależności ich organu

(organów) nadzorczego (nadzorczych) i mogą postanowić, że z punktu widzenia prawa budżetowego organ nadzorczy jest zależny od określonego departamentu ministerstwa. Przyznanie potrzebnych takiemu organowi zasobów ludzkich i materialnych nie może jednak uniemożliwiać mu wykonywania jego zadań „w sposób całkowicie niezależny" w rozumieniu art. 28 ust. 1 akapit drugi dyrektywy 95/46/WE (pkt 58).

Wyrok z dnia 8 kwietnia 2014 r. (wielka izba), Komisja/Węgry (C-288/12, EU:C:2014:237)[29]

W tej sprawie Komisja zwróciła się do Trybunału Sprawiedliwości o stwierdzenie, że poprzez skrócenie kadencji organu nadzorczego ochrony danych osobowych Węgry uchybiły zobowiązaniom, jakie na nich ciążą na mocy dyrektywy 95/46/WE.

Trybunał orzekł, że uchybia zobowiązaniom, jakie na nim ciążą na mocy dyrektywy 95/46/WE, państwo członkowskie, które skraca kadencję organu nadzorczego ochrony danych osobowych (pkt 62, pkt 1 sentencji).

W istocie zdaniem Trybunału niezależność, jaką powinny cechować się organy nadzorcze właściwe w zakresie przetwarzania danych osobowych, wyklucza w szczególności jakiekolwiek nakazy i jakikolwiek inny wpływ z zewnątrz – bez względu na jego formę oraz na to, czy jest bezpośredni, czy pośredni – który mógłby zaważyć na decyzjach tych organów i podważyć w ten sposób wykonywanie przez nie ich zadań polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych (pkt 51).

Trybunał poza tym przypomniał, że ponieważ niezależność funkcjonalna nie wystarcza sama w sobie do uchronienia organów nadzorczych od wszelkiego wpływu z zewnątrz, samo tylko zagrożenie możliwością wpływu politycznego organów kontroli państwa na decyzje organów nadzorczych jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań. Gdyby bowiem każdemu państwu członkowskiemu przysługiwało prawo do zakończenia kadencji organu nadzorczego przed jej pierwotnie przewidzianym zakończeniem bez poszanowania zasad i gwarancji uprzednio ustanowionych w tym celu we właściwych przepisach, zagrożenie tego rodzaju skróceniem kadencji ciążące na owym organie podczas wykonywania jego funkcji mogłoby prowadzić do pewnego rodzaju posłuszeństwa względem władzy politycznej, niezgodnego ze wskazanym wymogiem niezależności. Ponadto w tego rodzaju sytuacji nie można uznać, że organ nadzorczy może działać w każdych okolicznościach poza wszelkim podejrzeniem stronniczości (pkt 52–55).

2. Ustalenie prawa właściwego oraz właściwego organu nadzorczego

Wyrok z dnia 1 października 2015 r., Weltimmo (C-230/14, EU:C:2015:639)[30]

Nemzeti Adatvédelmi és Információszabadság Hatóság (krajowy organ ochrony danych i wolności informacji, Węgry) wymierzył grzywnę spółce Weltimmo, zarejestrowanej w Słowacji i prowadzącej strony internetowe z ogłoszeniami o nieruchomościach dotyczącymi nieruchomości położonych na Węgrzech, ze względu na nieusunięcie danych osobowych ogłoszeniodawców z tych stron, pomimo ich żądania w tym zakresie, oraz przekazanie tych danych agencjom ściągania wierzytelności w celu uzyskania zapłaty zaległych faktur. Według węgierskiego organu nadzorczego spółka Weltimmo naruszyła w ten sposób węgierską ustawę transponującą dyrektywę 95/46/WE.

29 Wyrok ten został omówiony w sprawozdaniu rocznym 2014, s. 62.
30 Wyrok ten został omówiony w sprawozdaniu rocznym 2015, s. 55.

Kúria (sąd najwyższy, Węgry), do którego wpłynęła skarga kasacyjna, wyraził wątpliwości co do ustalenia prawa właściwego oraz co do uprawnień węgierskiego organu nadzorczego w świetle art. 4 ust. 1 i art. 28 dyrektywy 95/46/WE. W konsekwencji sąd ten zwrócił się do Trybunału Sprawiedliwości z kilkoma pytaniami prejudycjalnymi.

W odniesieniu do mającego zastosowanie prawa Trybunał orzekł, że art. 4 ust. 1 lit. a) dyrektywy 95/46/WE zezwala na zastosowanie przepisów prawnych dotyczących ochrony danych osobowych państwa członkowskiego różnego od państwa, w którym zarejestrowany jest administrator tych danych, o ile prowadzi on poprzez stabilne rozwiązanie organizacyjne na terytorium tego państwa członkowskiego faktyczną i rzeczywistą działalność, choćby nawet drobną, w której kontekście dokonuje się rozpatrywanego przetwarzania. W celu ustalenia, czy tak jest, sąd odsyłający może w szczególności wziąć pod uwagę fakt, po pierwsze, że działalność administratora danych, w której kontekście ma miejsce to przetwarzanie, polega na prowadzeniu stron internetowych z ogłoszeniami o nieruchomościach dotyczących nieruchomości położonych na terytorium tego państwa członkowskiego i zredagowanych w jego języku, a w związku z tym ta działalność jest w głównej mierze, a nawet w całości nakierowana na to państwo członkowskie. Sąd odsyłający może, po drugie, także uwzględnić fakt, że ten administrator danych ma w tym państwie członkowskim przedstawiciela odpowiedzialnego za ściąganie należności powstałych w wyniku tej działalności oraz za reprezentowanie go w postępowaniu administracyjnym i sądowym dotyczącym omawianych danych. Trybunał natomiast wyjaśnił, że kwestia przynależności państwowej osób, których dotyczy to przetwarzanie danych, nie ma znaczenia (pkt 41, pkt 1 sentencji).

W odniesieniu do właściwości i uprawnień organu nadzorczego rozpatrującego skargi zgodnie z art. 28 ust. 4 dyrektywy 95/46/WE, Trybunał stwierdził, że organ ten może rozpatrzyć te skargi niezależnie od tego, jakie prawo ma zastosowanie, a nawet zanim zostanie ustalone, które prawo krajowe znajduje zastosowanie do spornego przetwarzania (pkt 54). Jednak, jeśli dojdzie on do wniosku, że właściwe jest prawo innego państwa członkowskiego, nie może on nałożyć sankcji poza terytorium państwa członkowskiego, któremu podlega. W takiej sytuacji powinien on, w myśl obowiązku współpracy przewidzianego w art. 28 ust. 6 tej dyrektywy, zwrócić się do organu nadzorczego tego drugiego państwa członkowskiego o stwierdzenie ewentualnego naruszenia tego prawa i o nałożenie sankcji, o ile prawo właściwe na to pozwala, w razie potrzeby w oparciu o przekazane przez niego informacje (pkt 57, 60, pkt 2 sentenci).

3. Uprawnienia krajowych organów nadzorczych

Wyrok z dnia 6 października 2015 r. (wielka izba), Schrems (C-362/14, EU:C:2015:650)

W tej sprawie (zob. także część III, zatytułowana „Przekazywanie danych osobowych do państw trzecich") Trybunał Sprawiedliwości w szczególności orzekł, że krajowe organy nadzorcze są uprawnione do dokonywania kontroli przekazywania danych osobowych do państw trzecich.

W tym zakresie Trybunał najpierw stwierdził, że krajowe organy nadzorcze dysponują szerokim wachlarzem uprawnień, które, wymienione w sposób niewyczerpujący w art. 28 ust. 3 dyrektywy 95/46/WE, stanowią środki niezbędne do wykonywania ich zadań. Organom tym przysługują zatem uprawnienia dochodzeniowe, takie jak prawo do gromadzenia wszelkich informacji potrzebnych do wykonywania ich funkcji nadzorczych, skuteczne uprawnienia interwencyjne, takie jak prawo nakładania czasowego lub ostatecznego zakazu przetwarzania danych, oraz prawo pozywania (pkt 43).

Co się tyczy uprawnień nadzoru w odniesieniu do przekazywania danych osobowych do państw trzecich Trybunał orzekł, że co prawda z art. 28 ust. 1 i 6 dyrektywy 95/46/WE wynika, że uprawnienia krajowych organów nadzorczych dotyczą przetwarzania danych osobowych dokonywanego na terytorium państwa

członkowskiego, do którego te organy należą, a więc nie posiadają one na mocy tego art. 28 kompetencji w odniesieniu do przetwarzania tychże danych dokonywanego na terytorium państwa trzeciego (pkt 44).

Jednak operacja przekazywania danych osobowych z państwa członkowskiego do państwa trzeciego polega sama w sobie na przetwarzaniu danych osobowych na terytorium państwa członkowskiego. W konsekwencji, skoro krajowe organy nadzorcze, zgodnie z art. 8 ust. 3 karty i z art. 28 dyrektywy 95/46/WE, zobowiązane są kontrolować poszanowanie unijnych zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych, każdy z nich jest wyposażony w uprawnienie do zbadania, czy przekazywanie tych danych z państwa członkowskiego, do którego on należy, do państwa trzeciego następuje z poszanowaniem wymogów sformułowanych przez ową dyrektywę (pkt 45, 47).

VI. Terytorialne stosowanie prawodawstwa Unii

Wyrok z dnia 13 maja 2014 r. (wielka izba), Google Spain i Google (C-131/12, EU:C:2014:317)

W tym wyroku [zob. także część II.3., zatytułowana „Pojęcie »przetwarzania danych osobowych«" i część IV.1., zatytułowana „Prawo do sprzeciwu wobec przetwarzania danych osobowych (»prawo do bycia zapomnianym«)"] Trybunał wypowiedział się także w przedmiocie terytorialnego zakresu stosowania dyrektywy 95/46/WE.

Trybunał orzekł zatem, że przetwarzanie danych osobowych ma miejsce w ramach działalności prowadzonej przez zakład administratora danych odpowiedzialnego za to przetwarzanie na terytorium danego państwa członkowskiego w rozumieniu dyrektywy 95/46/WE, jeśli operator wyszukiwarki internetowej, chociaż ma siedzibę w państwie trzecim, ustanawia w państwie członkowskim oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem tej wyszukiwarki, a działalność tego oddziału lub tej spółki zależnej jest skierowana do osób zamieszkujących to państwo członkowskie (pkt 55, 60, pkt 2 sentencji).

W istocie w takich okolicznościach działalność prowadzona przez operatora wyszukiwarki oraz działalność jego zakładu na terenie danego państwa członkowskiego, choć odmienne, to są ze sobą nierozerwalnie powiązane, gdyż działalność związana z powierzchniami reklamowymi stanowi środek służący uczynieniu rozpatrywanej wyszukiwarki internetowej opłacalną pod względem gospodarczym, a wyszukiwarka ta stanowi jednocześnie środek umożliwiający prowadzenie tej działalności (pkt 56).

VII. Prawo publicznego dostępu do dokumentów instytucji Unii Europejskiej a ochrona danych osobowych

Wyrok z dnia 29 czerwca 2010 r. (wielka izba), Komisja/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, spółka utworzona, aby importować niemieckie piwo przeznaczone do spożycia na miejscu w pubach w Zjednoczonym Królestwie, nie mogła sprzedawać swego towaru ze względu na to, że w Zjednoczonym Królestwie wiele podmiotów prowadzących sprzedaż napojów alkoholowych spożywanych na miejscu było związanych umowami na wyłączność kupna, które zobowiązywały je do zaopatrywania się w piwo w określonych browarach.

Na mocy uregulowania brytyjskiego dotyczącego dostawy piwa (zwanego dalej „GBP") brytyjskie browary były zobowiązane do umożliwienia zarządcom pubów kupna piwa pochodzącego z innego browaru, pod warunkiem że piwo będzie poddane fermentacji w beczce. Większość piw produkowanych poza Zjednoczonym Królestwem nie mogła zaś zostać uznana za „poddane fermentacji w beczce" w rozumieniu GBP, a zatem nie wchodziła w zakres stosowania tego przepisu. Stojąc na stanowisku, że GBP stanowi środek o skutku równoważnym z ograniczeniem ilościowym w przywozie, Bavarian Lager złożyła skargę do Komisji.

W toku postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego wszczętego przez Komisję przeciwko Zjednoczonemu Królestwu, przedstawiciele organów wspólnotowych i brytyjskich, a także przedstawiciele związku piwowarów prowadzących działalność na wspólnym rynku (CBMC) uczestniczyli w spotkaniu w dniu 11 października 1996 r. Wobec faktu, że organy brytyjskie uprzedziły Komisję o zmianie rozpatrywanego uregulowania w celu umożliwienia sprzedaży piwa butelkowanego jako piwa pochodzącego z innego źródła, na takich samych warunkach jak piwo beczkowe, Komisja poinformowała Bavarian Lager o zawieszeniu postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.

Bavarian Lager złożyła wniosek zmierzający do uzyskania kompletnego protokołu ze spotkania z października 1996 r., zawierającego nazwiska wszystkich uczestników, który Komisja odrzuciła decyzją z dnia 18 marca 2004 r., powołując się w szczególności na ochronę życia prywatnego tych osób, zagwarantowaną w rozporządzeniu o ochronie danych osobowych.

Bavarian Lager następnie wniosła skargę do Sądu o stwierdzenie nieważności tej decyzji Komisji. Wyrokiem z dnia 8 listopada 2007 r. Sąd stwierdził nieważność decyzji Komisji, uznając w szczególności, że samo zawarcie w wykazie uczestników spotkania nazwisk danych osób, z uwagi na fakt reprezentowania przez nie danego podmiotu, nie stanowi żadnego naruszenia ani nie naraża na niebezpieczeństwo życia prywatnego tych osób. Komisja, wspierana przez Zjednoczone Królestwo i Radę, wniosła wówczas od tego wyroku Sądu odwołanie do Trybunału Sprawiedliwości.

Trybunał najpierw stwierdził, że jeżeli wniosek sporządzony w oparciu o rozporządzenie nr 1049/2001[31] w sprawie dostępu do dokumentów, ma na celu uzyskanie dostępu do dokumentów zawierających dane osobowe, przepisy rozporządzenia (WE) nr 45/2001 znajdują w pełni zastosowanie, w tym również przepis, który nakłada na odbiorcę przekazania danych osobowych obowiązek wykazania konieczności ich ujawnienia, a także przepis, który przyznaje danej osobie możliwość sprzeciwienia się, w dowolnej chwili, ze względu na nadrzędne i uprawnione powody odnoszące się do jego konkretnej sytuacji, przetwarzaniu odnoszących się do niej danych (pkt 63).

Następnie Trybunał stwierdził, że wykaz uczestników spotkania przeprowadzonego w toku postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, znajdujący się w protokole z tego spotkania, zawiera dane osobowe w rozumieniu art. 2 lit. a) rozporządzenia (WE) nr 45/2001, ponieważ na jego podstawie można ustalić tożsamość uczestniczących w tym spotkaniu osób (pkt 70).

Wreszcie Trybunał z powyższego wywiódł, że wymagając, by w przypadku osób, które nie udzieliły wyraźnej zgody na rozpowszechnianie dotyczących ich danych osobowych zawartych w protokole, Bavarian Lager wykazała konieczność przekazania tych danych osobowych, Komisja działała zgodnie z art. 8 lit. b) wspomnianego rozporządzenia (pkt 77).

31 Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

W przypadku bowiem, gdy w ramach wniosku o dostęp do protokołu na podstawie rozporządzenia (WE) nr 1049/2001, nie dostarczono żadnego wyraźnego i uprawnionego uzasadnienia ani żadnego przekonywającego argumentu w celu wykazania konieczności przekazania tych danych osobowych, Komisja nie ma możliwości wyważenia różnych interesów zainteresowanych stron. Nie ma ona też możliwości sprawdzenia, czy istnieje jakikolwiek powód, by zakładać, że to przekazanie mogłoby naruszyć uprawnione interesy danych podmiotów, co nakazuje druga część art. 8 lit. b) rozporządzenia (WE) nr 45/2001 (pkt 78)[32].

Wyrok z dnia 16 lipca 2015 r., ClientEarth i PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

Europejski Urząd do spraw Bezpieczeństwa Żywności (EFSA) powołał grupę roboczą mającą za zadanie opracowanie wytycznych w celu określenia sposobu wdrożenia art. 8 ust. 5 rozporządzenia (WE) nr 1107/2009[33], w rozumieniu którego podmiot składający wniosek o wprowadzenie do obrotu środka ochrony roślin dołącza recenzowane, ogólnie dostępne publikacje naukowe, zgodnie ze wskazaniem EFSA, dotyczące substancji czynnej i jej istotnych metabolitów, poświęcone skutkom ubocznym dla zdrowia, środowiska i gatunków niebędących celem działania.

Po przedłożeniu projektu wytycznych do konsultacji publicznych ClientEarth i Pesticide Action Network Europe (PAN Europe) przedstawiły uwagi na temat tego projektu. W tym kontekście skierowały wspólnie do EFSA wniosek o udzielenie dostępu do kilku dokumentów odnoszących się do przygotowywania projektu wytycznych, w tym uwag biegłych zewnętrznych.

EFSA przyznała ClientEarth i PAN Europe dostęp do między innymi indywidualnych uwag biegłych zewnętrznych w przedmiocie projektu wytycznych. EFSA wskazała jednak, iż ukryła nazwiska wspomnianych biegłych, zgodnie z art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 1049/2001 oraz z przepisami Unii dotyczącymi ochrony danych osobowych, a zwłaszcza rozporządzenia (WE) nr 45/2001. EFSA zaznaczyła w tym względzie, że ujawnienie nazwisk biegłych odpowiadałoby przekazaniu danych osobowych w rozumieniu art. 8 rozporządzenia (WE) nr 45/2001 i że przesłanki ich przekazania przewidziane w tym przepisie nie były w niniejszym przypadku spełnione.

W związku z tym ClientEarth i PAN Europe wniosły do Sądu skargę o stwierdzenie nieważności wydanej przez EFSA decyzji. Ponieważ Sąd oddalił tę skargę, ClientEarth i PAN Europe wniosły odwołanie od wyroku[34] Sądu do Trybunału Sprawiedliwości.

W pierwszej kolejności Trybunał stwierdził, że ponieważ zażądane informacje umożliwiają powiązanie danej uwagi z określonym biegłym, dotyczą one zidentyfikowanej osoby i w konsekwencji stanowią zbiór danych osobowych w rozumieniu art. 2 lit. a) rozporządzenia (WE) nr 45/2001. Ponieważ nie należy mylić pojęcia „danych osobowych" w rozumieniu art. 2 lit. a) rozporządzenia (WE) nr 45/2001 z pojęciem „danych dotyczących życia prywatnego", Trybunał stwierdził poza tym, że zarzut ClientEarth i PAN Europe, iż sporne informacje nie wchodzą w zakres życia prywatnego biegłych będących podmiotami danych, jest bezskuteczny (pkt 29, 32).

Trybunał zbadał w drugiej kolejności argument ClientEarth i PAN Europe dotyczący istnienia klimatu nieufności względem EFSA, często oskarżanej o stronniczość z powodu odwoływania się przez ten urząd do biegłych mających interes prywatny podyktowany ich powiązaniami ze środowiskami przemysłowymi oraz dotyczący konieczności zapewnienia przejrzystości procesu decyzyjnego tego urzędu. Ten argument miał oparcie w badaniu stwierdzającym istnienie związków utrzymywanych przez większość

32 Wyrok ten został omówiony w sprawozdaniu rocznym 2010, s. 14.

33 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1107/2009 z dnia 21 października 2009 r. dotyczące wprowadzania do obrotu środków ochrony roślin i uchylające dyrektywy Rady 79/117/EWG i 91/414/EWG (Dz.U. L 309 z 24.11.2009, s. 1).

34 Wyrok Sądu z dnia 13 września 2013 r., ClientEarth i PAN Europe/EFSA (C-214/11 P, EU:C:2013:483).

biegłych z grupy roboczej EFSA z przemysłowymi grupami nacisku. W tym względzie Trybunał orzekł, że uzyskanie spornej informacji było konieczne w celu sprawdzenia in concreto bezstronności każdego z biegłych przy wykonywaniu ich misji naukowej w służbie EFSA. Trybunał w konsekwencji uchylił wyrok Sądu, stwierdziwszy, że Sąd niesłusznie orzekł, iż wspomniany wyżej argument ClientEarth i PAN Europe nie wystarczał, aby wykazać konieczność przekazania spornych informacji (pkt 57–59).

W trzeciej kolejności, do celów zbadania zgodności z prawem wydanej przez EFSA spornej decyzji, Trybunał zbadał, czy istnieje powód, by zakładać, że przekazanie mogłoby naruszać uprawniony interes danych osób. W tym zakresie stwierdził, że twierdzenie EFSA, iż ujawnienie spornej informacji powodowałoby ryzyko naruszenia życia prywatnego i integralności wspomnianych biegłych, ma charakter ogólny i nie jest w żaden inny sposób poparte jakimkolwiek właściwym w tym przypadku dowodem. Trybunał stwierdził, wręcz przeciwnie, że takie ujawnienie mogło, samo w sobie, pozwolić rozwiać podejrzenia o stronniczość lub ewentualnie zapewnić biegłym będącym podmiotami danych, okazję do podważenia, w razie potrzeby za pomocą dostępnych środków prawnych, zasadności tychże zarzutów stronniczości. W świetle tych okoliczności Trybunał także stwierdził nieważność decyzji EFSA (pkt 69, 73).

* * *

Wyroki opisane w tej broszurze znajdują się w repertorium orzecznictwa w rubrykach 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 i 4.11.07.